arXiv:2602.09290v1 [cs.CC] 10 Feb 2026

通过扩散性改进 GHZ 支持的游戏的并行重复

Yang P. Liu* Shachar Lovett† Kunal Mittal‡

摘要

我们证明，对于任意三人游戏 $\mathcal{G}$，若其查询分布与 GHZ 游戏具有相同的支撑集（即所有满足 $x+y+z=0 \pmod 2$ 的 $x,\ y,\ z \in \{0,1\}$），则其 n 重并行重复的值 $\mathcal{G}$ 以指数速度衰减：

$$\mathrm{val}(\mathcal{G}^{\otimes n}) \leq \exp(-n^c)$$

对于所有充分大的 n，其中 $c>0$ 是一个绝对常数。

我们还证明了 GHZ 游戏并行重复的一个集中界：对于任意常数 $\epsilon>0$，玩家至少赢得 n 个坐标中 $\left(\frac{3}{4}+\epsilon\right)$ 比例的概率至多为 $\exp(-n^c)$，其中 $c=c(\epsilon)>0$ 是一个常数。

在这两种情形下，我们的工作都将此前已知的最佳界限提高了指数级；此前的界限仅为多项式级的小量，即数量级为 $n^{-\Omega(1)}$。我们的关键技术工具是代数扩散性 这一概念，它改编自 Kelley 和 Meka 在 FOCS '23 上关于无三项等差数列集合的突破性工作。

*卡内基梅隆大学计算机科学系。电子邮箱：yangl7@andrew.cmu.edu。

†加州大学圣迭戈分校计算机科学与工程系。电子邮箱：slovett@ucsd.edu。研究工作得到西蒙斯研究员奖（编号929894）和美国国家科学基金会项目（编号CCF-2425349）的资助。

‡纽约大学库朗数学科学研究所计算机科学系。电子邮箱：kunal.mittal@nyu.edu。研究工作得到西蒙斯研究员奖的资助。

目录

1 引言 3 1.1 组织结构 .5

2 概述 6

2.1 一般归纳框架与高层次方法.6 2.2 步骤1：正方形是困难的 .7 2.3 步骤2：分布近似. 8

3 预备知识 9

3.1 概率分布 .9 3.2 GF(2)上的向量空间 .9 3.3 三人游戏与并行重复.10 3.3.1 关于并行重复的一些基本结果 .11 **4 代数S**

扩散性与均匀化 11

4.1 代数扩散性 .11 4.2 均匀化 .12 4.2.1 单个集合的均匀化 .12 4.2.2 两个集合的均匀化 .14 4.2.3 三个集合的均匀化 .14 **5 均匀 Sq**

正方形覆盖 19

5.1 组合扩展性与图计数 .19 5.2 代数扩散性蕴含图计数 .20 5.3 扩展对角乘积集中的正方形 .21 **6 并行重复**

适用于具有 GHZ 查询支持的博弈的并行重复 25

6.1 分散乘积事件下的困难坐标 .25 6.2 一般乘积事件下的困难坐标 .28 **7 集中界** 30 7.1 乘积事件的改进界 .30 7.2 并行重复下随机集合具有困难性.32 7.3 集中界的证明 . 33

一个边缘分布 o f 一个条件分布 38

1 引言

在一个 k 人博弈 $\mathcal{G}$ 中，验证者从分布Q中采样一个问题元组 $(x^{(1)},\dots,x^{(k)})$。然后，对于每个 $j\in\{1,\dots,k\}$，验证者将问题 $x^{(j)}$ 交给玩家 j，玩家返回一个答案 $a^{(j)}$，该答案仅依赖于 $x^{(j)}$。验证者随后根据谓词 $V(x,a)\in\{0,1\}$ 的求值结果判定玩家获胜或失败，该谓词依赖于问题 $x=(x^{(1)},\dots,x^{(k)})$ 和答案 $a=(a^{(1)},\dots,a^{(k)})$。我们将博弈值（记为 $\mathrm{val}(\mathcal{G})$）定义为在所有可能的玩家策略上、相对于分布 Q 的最大获胜概率；形式定义见定义 3.8 与 3.9。

一个自然的问题是：在并行重复 [FRS94] 下，博弈的值会如何变化？ n 重并行重复记作 $\mathcal{G}^{\otimes n}$，它是这样一种博弈：玩家并行进行并尝试赢得该博弈的 n 个独立副本。更确切地说，验证者独立地为 $i=1$、...、n 抽取问题 $(x_i^{(1)},\dots,x_i^{(k)})\sim Q$，并针对每个 $j\in\{1,\dots,k\}$，向玩家 j 发送问题 $(x_1^{(j)},\dots,x_n^{(j)})$，玩家则返回答案 $(a_1^{(j)},\dots,a_n^{(j)})$。若对每个 $i\in\{1,\dots,n\}$，$V((x_i^{(1)},\dots,x_i^{(k)}),(a_i^{(1)},\dots,a_i^{(k)}))=1$，验证者就判定玩家获胜；形式化定义见定义 3.11。

注意，对于任意博弈 $\mathcal{G}$，都有 $\mathrm{val}(\mathcal{G}^{\otimes n})\geq\mathrm{val}(\mathcal{G})^n$，因为玩家可以在每个 n 坐标上重复采用最优策略来达到这一值。尽管人们可能会预期朴素界 $\mathrm{val}(\mathcal{G}^{\otimes n})\leq\mathrm{val}(\mathcal{G})^n$ 同样成立，但事实并非如此 [For89, Fei91, FV02, Raz11]。粗略来说，这一失败是因为玩家不必独立处理该博弈的 n 个副本，而是可以在不同副本之间关联自己的答案。值得注意的是，这一失败与高维欧几里得镶嵌的几何性质密切相关 [FKO07, KORW08, AK09, BM21]。

双人游戏的并行重复已有深入研究。Raz [Raz98] 证明，对于任意值小于 1 的博弈，其 n重并行重复的值会随 n呈指数级衰减。后续研究简化了这一证明，并改进了定量界 [Hol09, BRR+09, Rao11, RR12, DS14, BG15]。这些及相关研究在多个领域带来了若干应用，包括交互式证明理论 [BOGKW88]，PCP 与近似困难性 [FGL+96, ABSS97, ALM+98, AS98, BGS98, Fei98, Hås01, Kho02a, Kho02b, GHS02, DGKR05, DRS05]，量子信息 [CHTW04, BBLV13]，以及通信复杂度 [PRW97, BBCR13,BRWY13]。有关更多详情，请参阅综述 [Raz10] 。

多人博弈的并行重复远未得到充分理解。唯一的一般性界限指出，对于任意满足值小于 1 的博弈 $\mathcal{G}$，都有 $\mathrm{val}(\mathcal{G}^{\otimes n})\leq 1/\alpha(n)$，其中 $\alpha(n)$ 是增长极其缓慢的逆阿克曼函数 [Ver96, FK91, Pol12]。近期研究在理解多人博弈的特殊情形方面取得了重大进展 [DHVY17, HR20, GHM+21, GHM+22, GMRZ22, BKM23, BBK+24, BBK+25, BBK+26]；然而，即使对于三人游戏，这个一般性问题仍远未解决。

证明多人博弈的改进的并行重复具有多种潜在应用。众所周知，针对某一类多人博弈的强平行重复定理意味着非一致图灵机存在超线性下界，而这一直是复杂性理论中的一个开放问题 [MR21]。此外，大答案字母表情形下的并行重复等价于高维极值组合学中的许多问题，例如密度Hales-Jewett问题以及无平方

有限域中的集合 [FV02，HHR16，Mit25]。此外，正如 [DHVY17], 所述，人们有理由相信，对并行重复的理解有所改进，能够帮助我们更好地理解额头编号（NOF）模型中的通信复杂性，而它与电路下界密切相关。

本文关注的是三人 GHZ 博弈 [GHZ89], ，其流程如下：验证者均匀随机地抽取问题 $(x, y, z) \in \{0,1\}^3$，使得 $x+y+z = 0 (\mathrm{mod}\, 2)$，玩家的目标是分别给出答案 $a, b, c \in \{0,1\}$，满足 $a+b+c (\mathrm{mod}\, 2) = x \vee y \vee z$。GHZ 游戏在量子信息论中发挥了奠基性作用，部分原因在于量子策略能够以概率 1 赢得该博弈，而任何经典策略的获胜概率至多为 $3/4$。此外，GHZ 游戏满足自测试性质，即所有达到值 1 的量子策略本质上都相同；这一性质促成了纠缠测试和设备无关密码学等应用 [ŠB20]。

近来有多篇论文讨论了 GHZ 游戏的并行重复问题。Dinur、Harsha、Venkat 和 Yuen [DHVY17]拓展了 Raz 的双人信息论技术 [Raz98]，并证明了满足某种连通性的特定类别多人博弈的并行重复定理；他们指出，GHZ 游戏是一种在某种意义上与这一类博弈相距最远的多人博弈；谈及这一问题的难度时，他们写道

> “我们认为，GHZ 查询分布中存在的强相关性，代表了多人平行重复问题中‘最难的实例’。”

后续研究为 GHZ 游戏的 n 重复建立了多项式衰减界，表明 $\mathrm{val}(\mathrm{GHZ}^{\otimes n}) \leq n^{-\Omega(1)}$ [HR20、GHM+21]。值得注意的是，这些结果适用于任何查询分布 $\mathcal{G}$ 与 GHZ 游戏具有相同支撑集的三人游戏 Q(即，$\{(x, y, z) \in \{0,1\}^3 : x + y + z = 0 \,(\mathrm{mod}\, 2)\}$)。

最近，人们证明了 GHZ 游戏的指数衰减界 [BKM23]，随后又将其推广到满足某种分布假设的所有三人 XOR 游戏[1] [BBK+25]。然而，这些研究严重依赖博弈谓词的 XOR 结构，并借助傅里叶分析和加性组合学中的复杂工具加以利用。例如，对于 GHZ 游戏，他们注意到该谓词对应于群 $\mathbb{Z}/4\mathbb{Z}$上的一个线性方程。因此，这些技术无法推广到缺乏此类 XOR 结构的一般博弈谓词。

在本文中，我们改进了现有的多项式衰减界 [HR20、GHM+21]：我们为所有查询支撑集与 GHZ 游戏相同的博弈建立了拉伸指数界。关键在于，不同于上述关于 XOR 博弈的工作 [BKM23、BBK+25]，我们的结果与答案集和博弈谓词无关——它仅取决于查询分布的支撑集。我们的技术方法也有所不同：我们采用了近期工作中的基于扩散性的论证 [KM23、KLM24和 JLL+25]，将其应用于并行重复的背景下尚属首次。

我们的主要结果如下：

[1]在三方 XOR 游戏中，三位参与者的答案 a、b、c属于某个有限阿贝尔群 H，且谓词具有 $a + b + c = \varphi(x, y, z)$ 的形式，其中函数 φ 将玩家的问题 (x, y, z) 映射到 H 的元素。

定理 1.1（GHZ 查询支持的并行重复）。设 $\mathcal{G}$ 为任意值为 $\mathrm{val}(\mathcal{G}) < 1$ 的三人游戏，其查询分布具有支撑集

$$\left\{(x,y,z) \in \{0,1\}^3 : x+y+z = 0 \pmod 2\right\}.$$

那么，对于所有充分大的 n，[2] 都有

$$\mathrm{val}(\mathcal{G}^{\otimes n}) \leq \exp\left(-n^c\right),$$

其中，$c > 0$ 是一个绝对常数。

我们用关于具有 GHZ 查询分布的博弈的集中界来补充这一结果。据我们所知，先前工作 [BKM23、BBK+24] 中建立的指数衰减界并不能推出这样的集中性。我们证明如下：

定理 1.2（集中界；作为定理 7.1重新表述并证明）。设 $\mathcal{G}$ 是任意一个取值为 $\mathrm{val}(\mathcal{G}) < 1$的三人游戏，其查询分布在集合上均匀分布

$$\left\{(x,y,z) \in \{0,1\}^3 : x+y+z = 0 \pmod 2\right\}.$$

那么，对于每个常数 $\epsilon > 0$，存在 $c = c(\epsilon) > 0$，使得对于所有充分大的n，[3] 玩家在博弈 $\mathcal{G}^{\otimes n}$ 中至少赢得 n 个坐标中val（$\mathcal{G}$）$+\epsilon$ 比例的概率至多为exp（$-n^c$）。

作为直接的推论 因此，我们得到了标准 GHZ 游戏的一个集中界 .

推论 1.3. 对于任意常数 $\epsilon > 0$，存在 $c = c(\epsilon) > 0$，使得玩家在 *GHZ*游戏$^{\otimes n}$ 中至少赢得 $\left(\frac{3}{4}+\epsilon\right) n$ 个坐标的概率至多为 $\exp\left(-n^c\right)$。

对于 GHZ 支撑集上的博弈，若其底层分布并非均匀分布，则建立类似的集中界（如定理 1.2）仍是一个有趣的开放问题。[4]

1.1 组织结构

在第2节，我们概述证明思路。在第3节，我们介绍一些预备知识。在第4节，我们定义一种称为代数扩散性的伪随机性概念，它将在本文中发挥重要作用；我们还将说明如何将任意集合分解为满足这一扩散性条件的各个部分。在第5节，我们证明，任何由代数扩散集构成的对角乘积集合都能被均匀覆盖于正方形。最后，在第6节，我们运用前面各节的结果，证明具有 GHZ 查询支持的博弈满足并行重复性质（定理1.1）。在第7节，我们证明集中界（定理1.2）。

[2]即 $n \geq N$，其中 N 是一个取决于博弈 $\mathcal{G}$的常数。[3]即 $n \geq N$，其中 N 是一个取决于博弈 $\mathcal{G}$ 和参数 ϵ的常数。[4]我们指出，定理 1.2结合类似于引理 3.12的归约（另见脚注 6），已经可以推出以下结论：玩家赢得至少 $1-\beta+\epsilon$ 比例的 n 个坐标的概率至多为 $\exp(-n^{\Omega_\epsilon(1)})$，其中 $\beta = \beta(\mathcal{G}) > 0$ 是一个常数。

2 概述

本节概述主要结果（定理1.1）的证明。

2.1 一般归纳框架与高层次方法

我们首先介绍并行重复的一般归纳框架。我们的证明遵循 Raz 为双人游戏的并行重复所建立的基本设定 [Raz98]。

设 $\mathcal{G}$ 是一个三人游戏，其查询分布 Q 的支撑集为

$$\mathrm{supp}(Q) = \left\{(x,y,z) \in \mathbb{F}_2^3 : x+y+z=0\right\}.^{5}$$

这里，我们将 $\{0,1\}$ 视为有限域 $\mathbb{F}_2$。为进行并行重复，我们不失一般性地假设 Q 是其支撑集上的均匀分布（见引理 3.12）。[6] 现在，考虑博弈 $\mathcal{G}^{\otimes n}$，并考虑该博弈中 3 位玩家的任意策略。对于每个 $i \in [n]$，令 Win_i 表示玩家赢得 i^{th} 坐标的事件。根据链式法则，对于 i_1的任意排列 i_2，……， i_n，我们可以将 $[n]$获胜概率写为

$$\Pr[\mathrm{Win}_1 \wedge \mathrm{Win}_2 \wedge \cdots \wedge \mathrm{Win}_n] = \prod_{k=1}^{n} \Pr[\mathrm{Win}_{i_k} \mid \mathrm{Win}_{i_1} \wedge \cdots \wedge \mathrm{Win}_{i_{k-1}}].$$

为了对其进行界定，我们采用归纳法。假设玩家已经赢得了一组坐标i_1，……， i_k，我们的目标是找出一个困难坐标 $i \in [n]$，使其条件获胜概率至多为 $1-\Omega(1)$。形式化地说，我们希望证明以下条件：[7]

归纳步骤： 对于每个乘积事件 $\mathcal{E} = E \times F \times G \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^n$，其测度为 $\Pr[\mathcal{E}] \geq \alpha$，都存在一个坐标 $i \in [n]$，使得 $\Pr[\mathsf{Win}_i \mid \mathcal{E}] \leq 1 - \Omega(1)$。

证明该条件对 $\alpha = \exp(-n^{\Omega(1)})$ 成立，即可通过上述归纳策略得到 $\mathrm{val}(\mathcal{G}^{\otimes n})$ 的所需界（参见引理 3.13）。

在本概述余下部分中，考虑任意乘积事件 $\mathcal{E} = E \times F \times G \subseteq (\mathbb{F}_2^n)^3$，其测度为 $\Pr[\mathcal{E}] \geq \alpha = \exp(-n^{\Omega(1)})$。我们的目标是找出一个坐标 $i \in [n]$，使得在输入以 $\mathcal{E}$ 为条件时，仍然难以赢得该坐标上的博弈。证明分为两个主要步骤：

1. **识别困难集合：**我们定义了一类称为正方形的集合，使得当输入分布被限制在一个正方形内时，许多坐标都难以赢得。

[5]该框架适用于所有 k 人博弈，但我们将讨论范围限定为使用 GHZ 查询的 3 人博弈。[6]粗略地说，这是因为任意分布 Q 都包含 $\mathrm{supp}(Q)$ 上均匀分布的一个小副本，因此，在分布 Q 下赢得 n 个副本，至少与在均匀分布下赢得 $\Omega(n)$ 个副本同样困难。[7]以事件 $\mathsf{Win}_{i_1} \wedge \cdots \wedge \mathsf{Win}_{i_k}$ 为条件，可能会在玩家的输入之间引入复杂的相关性。然而，该事件由坐标 $i_1, \ldots, i_k$ 上玩家的问题与答案确定性地决定。因此，我们可以不以事件 $\mathsf{Win}_{i_1} \wedge \cdots \wedge \mathsf{Win}_{i_k}$ 为条件，而改为以坐标 $i_1, \ldots, i_k$ 上玩家的典型问题与答案为条件。这样便会在玩家的输入上诱导出一个乘积事件。

2. **分布近似：**我们证明，条件分布 $Q^{\otimes n}|\mathcal{E}$可以用这类正方形分布的凸组合来近似（在 ℓ_1 距离下）。

结合这些步骤可得，对于随机选取的 $i \in [n]$，$\Pr[\mathsf{Win}_i \mid \mathcal{E}] \leq 1 - \Omega(1)$。

2.2 步骤1：正方形是困难的

由于在 $\mathcal{G}^{\otimes n}$ 中，第三位玩家的输入完全由前两位玩家的输入决定（输入 $(x, y, z) \in \mathrm{supp} Q^{\otimes n} \subseteq \mathbb{F}_2^{n3}$ 满足 $z = x + y$），因此我们可以主要通过观察前两位玩家的输入来分析该博弈。乘积事件 $\mathcal{E} = E \times F \times G$ 在前两位玩家上的限制由一个对角积集合描述，定义如下：

定义 2.1（对角积集合）。给定集合 X、Y、$Z \subseteq \mathbb{F}_2^n$，我们定义相应的对角积集合，记为 $S(X, Y, Z)$，其定义为

$$S(X, Y, Z) = \{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : x \in X, y \in Y, x + y \in Z\}.$$

输入采样 $(x, y, z) \sim Q^{\otimes n}|\mathcal{E}$ 与均匀采样 $(x, y) \sim S(E, F, G)$ 并设置 $z = x + y$ 相同。

现在我们定义困难集合，即 $\mathbb{F}_2^n \times \mathbb{F}_2^n$ 中的正方形：

Defi定义 2.2（正方形）。对于 x、y、$w \in \mathbb{F}_2^n$，正方形 $s_{x,y,w} \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^n$ 是 s et

$$s_{x,y,w} = \{(x, y), (x + w, y), (x, y + w), (x + w, y + w)\}.$$

注记 2.3。给定一个正方形 $s \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^n$，假设我们希望将其表示为 $s = s_{x,y,w}$。注意，宽度 w 由正方形 s 唯一确定。如果 $w = 0$，该正方形只包含一个点，此时 (x, y) 可唯一确定。如果 $w \neq 0$，正方形 $s_{x,y,w}$ 有 4 种不同的表示方式，分别为 $s_{x,y,w} = s_{x+w,y,w} = s_{x,y+w,w} = s_{x+w,y+w,w}$。

正方形的关键性质是其局部困难性：考虑一个正方形 $s = s_{x_0,y_0,w}$，以及一个坐标 $i \in [n]$，使得 $w_i \neq 0$（一个非平凡坐标）。[8] 假设三位参与者的输入 (x, y, z) 按如下方式从正方形 s 中采样：令 $(x, y) \sim s$ 均匀随机选取，并令 $z = x + y$。在这种分布下，玩家的任何策略在坐标 i 上获胜的概率都不超过 $\mathrm{val}(\mathcal{G})$。粗略地说，这是因为该分布与基础分布 Q“看起来完全相同”，因此玩家可以将博弈 $\mathcal{G}$ 的单个副本嵌入该分布的坐标 i 中；这一步的形式化细节见引理 6.4。[9]

[8] 当且仅当 s 中的点在该坐标上的取值不恒定时，该坐标才是非平凡的。[9] 我们指出，输入集合 $\{(x, y, x + y) : (x, y) \in s\}$ 由文献 [GHM+21] 首次引入，他们称该集合为 蝴蝶结。此外，正方形对应于 GHZ 查询分布内部的极大禁子图（因为没有任何玩家策略能在正方形的全部四个点上获胜），而 $\mathbb{F}_2^n \times \mathbb{F}_2^n$ 中无正方形集合的最大规模 n 恰好刻画了大答案字母表情形下 GHZ 查询分布的 [麻省理工学院25]-重并行重复的值。

2.3 第 2 步：分布近似

证明的第二步在技术上要求更高：证明分布 $Q^{\otimes n}|\mathcal{E}$ 可以很好地近似为上述平方分布的混合。等价地，我们希望用平方上的均匀分布的凸组合，近似对角积集合$S = S(E,\ F,\ G)$上的均匀分布，记为 U_S。具体来说，我们分析如下生成的分布 μ ：均匀随机采样一个正方形 $s \subseteq S$，再从 s中均匀随机输出一个元素。

注意，先验上甚至无法确定集合 S 是否包含正方形，也无法确定分布 μ 是否有定义。不过，我们运用了代数扩散性这一伪随机性概念。该概念由 Kelley 和 Meka 在关于不含三项等差数列集合的界的突破性工作中提出 [KM23]。他们证明，代数扩散子集在某种意义上表现得像随机子集（参见定义 4.1 和定理4.2）；在我们的设定中，我们证明，若所有的 E、F、G 都具有代数扩散性，则集合 S 包含预期密度的正方形。我们的近似论证分两个阶段进行：

均匀化：给定任意集合 E, F, G，我们将对角积集合$S(E, F, G)$分解为互不相交的分量 $S(E_1, F_1, G_1) \cup S(E_2, F_2, G_2) \cdots \cup S(E_T, F_T, G_T)$（另加一个可忽略的余项），使得每个分量中的集合 E_i, F_i, G_i 都具有代数扩散性。这推广了 [JLL+25] 最近提出的分解技术；该技术仅使三个集合中的两个具有代数扩散性，并据此证明了有限域中无角集合的界。我们通过细致的递归论证将其推广到全部三个集合；更多详情见第 4.2 节。

计数与近似：假设 E、F、G 均为代数扩散，我们证明它们的行为类似于密度相同的随机集合，并且正方形采样分布 μ 在 U_S 距离下 ℓ_1 近似于均匀分布。我们通过对分布的 ℓ_2 范数（碰撞概率） μ建立紧确界来证明这一点。这里的一个关键技术工具是 [FHHK24]，近期提出的一项图计数结果，该结果基于一种称为组合扩展性的伪随机性概念；我们证明了该概念在我们的情形下成立。关于这一步的更多细节，请参见引理5.5 和命题5.6 。

为何采用代数扩散性？我们的工作与先前多项式衰减界 [GHM+21] 的一个关键区别，在于为集合 E, F, G选择了不同的伪随机性性质。先前的工作采用傅里叶均匀性（针对线性测试的伪随机性）这一概念，并在密度 $\alpha = \Pr[\mathcal{E}]$ 至少为多项式级，即数量级为 $n^{-O(1)}$时，得到相应的界。采用代数扩散性使我们能够突破这一障碍，即使密度 $\alpha =\exp(-n^{\Omega(1)})$ 小到指数级时也能得到相应的界。然而，这一改进带来了显著的技术代价。在傅里叶均匀性的框架下，分解和近似步骤都是标准的；而在代数扩散性的框架下确立这些步骤，则构成了本文的主要技术贡献。

3 预备知识

令 $\mathbb{N}=\{1,2,\ldots\}$ 表示自然数集合。对于 $n\in\mathbb{N}$，我们用 $[n]$ 表示集合 $\{1,2,\ldots,n\}$。

3.1 概率分布

设 P 为一个分布（定义在底层有限集 Ω 上，通常可从上下文中明确）。我们用 $\mathrm{supp}(P)=\{\omega\in\Omega:\ P[\omega]>0\}$ 表示分布 P 的支撑集。对于满足 $P[E]>0$ 的事件 $E\subseteq\Omega$，我们用 $P|E$ 表示在 E条件下的条件概率分布P。

对于定义在集合 Ω 上的分布 P 和 Q，它们之间的 ℓ_1-距离定义为

$$\|P-Q\|_1=\sum_{\omega\in\Omega}|P[\omega]-Q[\omega]|.$$

我们陈述一个关于独立随机变量之和的有用尾界 s:

事实 3.1（Chernoff界，参见 [MU05] 以供参考）。设 X_1，.....，$X_n\in\{0,1\}$ 为相互独立且均值为 μ 的随机变量，并设 $X=\sum_{i=1}^n X_i$。那么，对于所有 $\delta\in(0,\ 1)$，

$$\Pr\left[X\le(1-\delta)\mu n\right]\le e^{-\frac{\delta^2\mu n}{2}},$$

$$\Pr\left[X\ge(1+\delta)\mu n\right]\le e^{-\frac{\delta^2\mu n}{3}}.$$

我们还陈述另一个有用的引理:

引理3.2. 设 $t,n\in\mathbb{N}$，$t<n$。设 μ 为 $[n]$上的均匀分布，ν 为 $[n-t]$上的均匀分布。那么，$\|\mu-\nu\|_1=2t/n$。

证明。我们有 $\|\mu-\nu\|_1=\sum_{i=1}^{n-t}\left(\frac{1}{n-t}-\frac{1}{n}\right)+\sum_{i=n-t+1}^{n}\frac{1}{n}=\frac{2t}{n}$。 □

3.2 GF(2)上的向量空间

设 $\mathcal{V}$ 是 $\mathbb{F}_2$上的有限维向量空间，并赋予均匀测度；通常我们会有 $\mathcal{V}=\mathbb{F}_2^n$，其中某个 $n\in\mathbb{N}$。

定义3.3 (内积)。对于函数 $f,g:\ \mathcal{V}\to\mathbb{R}$，定义它们的内积为

$$\langle f,g\rangle=\mathop{\mathbb{E}}_{x\sim\mathcal{V}}[f(x)g(x)],$$

其中，$x\sim\mathcal{V}$ 表示从 $\mathcal{V}$中均匀选取 x。

定义 3.4（L^p 范数）。对于 $f:\ \mathcal{V}\to\mathbb{R}$ 和 $p\ge1$，我们定义

$$\|f\|_p=\mathbb{E}[f^p]^{1/p}.$$

定义 3.5（卷积）。对于 f、g：$\mathcal{V} \to \mathbb{R}$，我们将它们的卷积定义为

$$(f * g)(x) = \mathop{\mathbb{E}}_{y \sim \mathcal{V}}[f(y)g(x+y)].$$

我们观察到以下简单事实：

事实 3.6. 对于函数 f、g、h：$\mathcal{V} \to \mathbb{R}$，

$$\langle f * g, h\rangle = \langle f * h, g\rangle = \langle g * h, f\rangle = \mathop{\mathbb{E}}_{x,y \sim \mathcal{V}}[f(x)g(y)h(x+y)].$$

定义 3.7（密度函数）。对于非空集合 $A \subseteq \mathcal{V}$，我们将其密度函数定义为

$$\varphi_A = \frac{\mathbb{1}_A}{\mathbb{E}\left[\mathbb{1}_A\right]} = \frac{\mathbb{1}_A}{|A| / |\mathcal{V}|}.$$

注意 $\mathbb{E}[\varphi_A] = 1$。

3.3 三人游戏与并行重复

我们概述有关多人博弈的一些基本定义。我们将把重点限定于三人游戏。

定义 3.8（三人博弈）。一个三人博弈 $\mathcal{G}$ 是一个元组 $\mathcal{G} = (\mathcal{X} \times \mathcal{Y} \times \mathcal{Z},\ \mathcal{A} \times \mathcal{B} \times \mathcal{C},\ Q,\ V_{pred})$，其中问题集 $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ 和答案集 $\mathcal{A}, \mathcal{B}, \mathcal{C}$ 都是有限集，Q 是定义在 $\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ 上的概率分布，而 $V_{pred} : (\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}) \times (\mathcal{A} \times \mathcal{B} \times \mathcal{C}) \to \{0, 1\}$ 是一个谓词。

博弈 $\mathcal{G}$ 按以下方式进行：验证者采样问题 $(X, Y, Z) \sim Q$；然后，验证者将 X 发送给玩家 1，将 Y 发送给玩家 2，并将 Z 发送给玩家 3，玩家分别以答案 $A \in \mathcal{A}$，$B \in \mathcal{B}$，$C \in \mathcal{C}$ 作答。最后，当且仅当 $V_{pred}((X, Y, Z), (A, B, C)) = 1$ 时，验证者才宣布玩家获胜。

定义 3.9（博弈值）。设 $\mathcal{G} = (\mathcal{X} \times \mathcal{Y} \times \mathcal{Z},\ \mathcal{A} \times \mathcal{B} \times \mathcal{C},\ Q, V_{pred})$ 是一个三人游戏。博弈 $\mathcal{G}$ 的值，记为 $\mathrm{val}(\mathcal{G})$，定义如下

$$\mathrm{val}(\mathcal{G}) = \max_{f,g,h} \Pr_{(X,Y,Z) \sim Q}\left[V_{pred}\left((X, Y, Z), (f(X), g(Y), h(Z))\right) = 1\right],$$

其中最大值取遍所有玩家策略 f：$\mathcal{X} \to \mathcal{A}$，$g$：$\mathcal{Y} \to \mathcal{B}$，$h$：$\mathcal{Z} \to \mathcal{C}$。

事实 3.10。即使允许玩家使用公共随机性和私有随机性，博弈值也不会改变，因为总存在一组固定的随机字符串，使其构成最优策略。

接下来，我们定义三人游戏的并行重复，即 n 个独立的博弈并行进行。

定义 *3.11*（并行重复）。设 $\mathcal{G} = (\mathcal{X} \times \mathcal{Y} \times \mathcal{Z},\ \mathcal{A} \times \mathcal{B} \times \mathcal{C},\ Q, V_{pred})$ 是一个三人游戏。我们将其 n 重重复定义为 $\mathcal{G}^{\otimes n} = (\mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n,\ \mathcal{A}^n \times \mathcal{B}^n \times \mathcal{C}^n,\ Q^{\otimes n}, V_{pred}^{\otimes n})$。分布 $Q^{\otimes n}$ 是分布 Q 的 n 重乘积，即对于每个 $x \in \mathcal{X}^n, y \in \mathcal{Y}^n, z \in \mathcal{Z}^n$，都有 $Q^{\otimes n}[(x, y, z)] = \prod_{i=1}^{n} Q[(x_i, y_i, z_i)]$。谓词 $V_{pred}^{\otimes n}$ 定义为 $V_{pred}^{\otimes n}((x, y, z), (a, b, c)) = \bigwedge_{i=1}^{n} V_{pred}((x_i, y_i, z_i), (a_i, b_i, c_i))$。

3.3.1 并行重复的一些基本结果

我们陈述一个引理，出自 [FV02], ，该引理表明，只需在游戏的分布在其支撑集上均匀分布的情况下证明并行重复：

引理 *3.12*（[*GHM*+22，引理 *3.*14]）。设 $\mathcal{G} = (\mathcal{X} \times \mathcal{Y} \times \mathcal{Z},\ \mathcal{A} \times \mathcal{B} \times \mathcal{C},\ Q, V_{pred})$ 是一个三人游戏，满足 $val(\mathcal{G}) < 1$。设 $\mathcal{G} = (\mathcal{X} \times \mathcal{Y} \times \mathcal{Z},\ \mathcal{A} \times \mathcal{B} \times \mathcal{C},\ U, V_{pred})$，其中 U 是 $supp(Q)$ 上的均匀分布。那么，$val(\mathcal{G}) < 1$，并且存在一个常数$c = c(\mathcal{G}) > 0$，使得对每个充分大的 $n \in \mathbb{N}$，

$$\mathrm{val}(\mathcal{G}^{\otimes n}) \leq 2 \cdot \mathrm{val}(\tilde{\mathcal{G}}^{\otimes \lfloor cn \rfloor}).$$

我们陈述一个来自 [Raz98]的归纳式并行重复判据：

引理 *3.13*（[*BBK*+26，引理 *B.*1]）。设 $\mathcal{G} = (\mathcal{X} \times \mathcal{Y} \times \mathcal{Z},\ \mathcal{A} \times \mathcal{B} \times \mathcal{C},\ Q, V_{pred})$ 是一个三人博弈，并考虑其 n 重复 $\mathcal{G}^{\otimes n} = (\mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n,\ \mathcal{A}^n \times \mathcal{B}^n \times \mathcal{C}^n,\ Q^{\otimes n}, V_{pred}^{\otimes n})$，其中 $n \in \mathbb{N}$ 充分大。固定该博弈中三位玩家的最优策略，并对每个 $i \in [n]$，令 Win_i 表示该策略赢得博弈第 i^{th} 个坐标的事件。

设 $\epsilon > 0$ 为常数，且 $\alpha \in (0, 1]$，$\alpha \geq 2^{-n}$ 满足以下条件：对于每个乘积事件 $E \times F \times G \subseteq \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$，若 $\Pr_{Q^{\otimes n}}[E \times F \times G] \geq \alpha$，则存在一个坐标 $i \in [n]$，使得 $\Pr[\mathrm{Win}_i \mid E \times F \times G] \leq 1 - \epsilon$。

那么，对于某个常数 $c = c(\mathcal{G})$，有 $\mathrm{val}(\mathcal{G}^{\otimes n}) \leq \alpha^c$。

4 代数扩散性与均匀化

本节概述一种称为代数扩散性的伪随机性概念。我们还将展示如何将任意集合分解为满足此扩散性定义的若干部分。

4.1 代数扩散性

定义 4.1 (代数扩散性)。设 $\mathcal{V} \subseteq \mathbb{F}_2^n$ 为一个仿射子空间。若子集 $A \subseteq \mathcal{V}$ 满足：对于所有满足 维数$(\mathcal{V}') \geq$ 维数$(\mathcal{V}) - r$ 的仿射子空间 $\mathcal{V}' \subseteq \mathcal{V}$，均有

$$\frac{|A \cap \mathcal{V}'|}{|\mathcal{V}'|} \leq (1 + \epsilon) \cdot \frac{|A|}{|\mathcal{V}|}.$$

我们陈述一个关于扩散子集的有用结果。

定理 4.2。令 $d \geq 1, \epsilon \in (0, 1/4)$。那么，存在一个充分大的整数 $r = d^8 \epsilon^{-O(1)}$，以及一个充分小的 $\delta = \Omega(\epsilon)$，使得以下结论成立：设 $A, B, C \subseteq \mathbb{F}_2^n$ 是大小均至少为 $2^{-d} \cdot |\mathbb{F}_2^n|$ 的集合。那么，

(i) ([KM23，命题 2。16]) 如果 A、B、C 中至少有两个是 $(r,\ \delta)$-代数扩散的，

$$|\langle \varphi_A * \varphi_B,\ \varphi_C\rangle - 1| \le \epsilon.$$[10]

(ii) ([KM23，命题 4.10]) 如果 A、B、C 中至少有一个是(r,δ)-代数扩散的，

$$\langle \varphi_A * \varphi_B,\ \varphi_C\rangle \le 1+\epsilon.$$

4.2 均匀化

本节将介绍一种过程，它以任意集合 $X \subseteq \mathbb{F}_2^n$ 为输入，并将其近似分解为若干代数扩散的分量。更一般地，我们为三个集合 X、Y、Z 找到一种与对角乘积相容的同时分解：

命题 4.3。 设 $r \in \mathbb{N}$, $\epsilon,\eta \in (0,1/10)$，且 $X,Y,Z \subseteq \mathcal{V}$ 是线性子空间 $\mathcal{V} \subseteq \mathbb{F}_2^n$ 的元素。定义 $\alpha = |S(X,Y,Z)|/|\mathcal{V}|^2$。那么，存在 $C_\eta = (1/\eta)^{O(1)} \ge 1$（仅依赖于 η）、一个整数 $T \in \mathbb{N}$，并且对每个 $i \in [T]$，存在一个线性子空间 $\mathcal{V}_i \subseteq \mathcal{V}$、点 $x_i, y_i \in \mathcal{V}/\mathcal{V}_i$ 以及子集 $X_i \subseteq x_i + \mathcal{V}_i$，$Y_i \subseteq y_i + \mathcal{V}_i$，$Z_i \subseteq x_i + y_i + \mathcal{V}_i$，使得：

1. $\dim(\mathcal{V}_i) \ge \dim(\mathcal{V}) - r\epsilon^{-3}\log_2(4/\alpha)^{C_\eta}$ 对所有 $i \in [T]$。
2. S（X_1、Y_1、Z_1）……，S（X_T、Y_T、Z_T）是 S（X、Y、Z）的不相交子集，满足 t

$$\left|S(X,Y,Z) \setminus \cup_{i=1}^T S(X_i,Y_i,Z_i)\right| \le \eta\,|S(X,Y,Z)|\,.$$

   对角积集合的定义与定义 2.1 中相同。

3. 对所有 $i \in [T]$，有 $|X_i|$、$|Y_i|$、$|Z_i| \ge 2^{-(\log_2(4/\alpha))^{C_\eta}} \cdot |\mathcal{V}_i|$，并且 X_i、Y_i、Z_i 在 $x_i + \mathcal{V}_i$、$y_i + \mathcal{V}_i$、$x_i + y_i + \mathcal{V}_i$ 中分别是（r、ϵ）-代数扩散的。

上述命题的证明基于 [JLL+25，第 5 节，3]，但不同之处在于，我们致力于使全部 3 个集合都具有扩散性（而不仅仅是 2 个）。因此，与他们针对两个集合的版本相比，我们对参数 η 的依赖性较弱；不过，这在我们的情形中无关紧要，因为我们仅将其用于常数 η。在接下来的小节中，我们将首先展示如何分解一个集合，然后是两个集合，最后是三个集合。

4.2.1 单个集合的均匀化

我们首先说明如何将单个集合 X 分解为分散分量。在此之前，我们证明任意大集合都包含一个分散集。

引理 4.4（分散子集的存在性）。设 $r \in \mathbb{N}$、$\epsilon \in (0,\ 1)$，并设 $X \subseteq \mathcal{V}$ 为一个线性子空间 $\mathcal{V} \subseteq \mathbb{F}_2^n$。定义 $\alpha_X = |X|/|\mathcal{V}|$。则存在一个仿射子空间 $\mathcal{V}' \subseteq \mathcal{V}$，使得：

[10]例如，如果两者 A、B 都是代数扩散的，则有 $|\langle \varphi_A * \varphi_B,\ \varphi_C\rangle - 1| \le 2\,\|\varphi_A * \varphi_B - 1\|_d \le \epsilon$，其中第一个不等式由 Hölder 不等式得出，第二个不等式由 [KM23，命题 2。16]。

1. 维数($\mathcal{V}'$) $\geq$ 维数($\mathcal{V}$) $- r\epsilon^{-1}\log_2(1/\alpha_X)$。

集合 $X' = X \cap \mathcal{V}'$ 满足 $\frac{|X'|}{|\mathcal{V}'|} \geq \alpha_X$，且 X' 在 $\mathcal{V}'$ 中是 (r,ϵ)-代数扩散的。

证明。我们迭代进行。令 $\mathcal{V}^{(0)} = \mathcal{V}$；对于 $t = 0, 1, 2, \ldots\ldots$，我们按如下步骤操作：若 $X \cap \mathcal{V}^{(t)}$ 在 $\mathcal{V}^{(t)}$ 中是 (r, ϵ)-代数扩散的，则停止；否则，存在某个子空间 $\mathcal{V}^{(t+1)} \subseteq \mathcal{V}^{(t)}$，使得 $\dim(\mathcal{V}^{(t+1)}) \geq \dim(\mathcal{V}^{(t)}) - r$，并且

$$\frac{\left|X \cap \mathcal{V}^{(t+1)}\right|}{|\mathcal{V}^{(t+1)}|} > (1+\epsilon) \cdot \frac{\left|X \cap \mathcal{V}^{(t)}\right|}{|\mathcal{V}^{(t)}|}.$$

如果直到第 t 步我们仍未停止，则有 $\dim(\mathcal{V}^{(t)}) \geq \dim(\mathcal{V}) - rt$，并且

$$\frac{\left|X \cap \mathcal{V}^{(t+1)}\right|}{|\mathcal{V}^{(t+1)}|} \geq (1+\epsilon)^t \alpha_X \geq 2^{\epsilon t}\alpha_X.$$

Sin由于该密度不能超过 1，因此我们必定会在某个 $t \leq \epsilon^{-1}\log_2(1/\alpha$ 时停止 $_X)$. □

利用上述 引理，我们说明如何将单个集合分解为分散分量 .

引理 4.5 (单个集合的均匀化)。设 $r \in \mathbb{N}$, $\epsilon, \eta \in (0,1)$。设 $X \subseteq \mathcal{V}$ 是一个线性子空间 $\mathcal{V} \subseteq \mathbb{F}_2^n$。那么，存在 $T \in \mathbb{N}$，并且对每个 $i \in [T]$，存在一个仿射子空间 $\mathcal{V}_i \subseteq \mathcal{V}$和一个子集 $X_i \subseteq \mathcal{V}_i$，使得：

1. $\dim(\mathcal{V}_i) \geq \dim(\mathcal{V}) - r\epsilon^{-1}\log_2(1/\eta)$ *for all* $i \in [T]$.
2. $X_1, \ldots, X_T$是 X 的两两不相交子集，且满足 $\left|X \setminus \cup_{i\in[T]} X_i\right| \leq \eta\,|\mathcal{V}|$。
3. 对所有 $i \in [T]$, $|X_i| \geq \eta\,|\mathcal{V}_i|$， X_i 在 $\mathcal{V}_i$内是(r,ϵ)-代数扩散的。

证明。我们通过以下算法迭代进行：设 $X^{(1)} = X$, $\mathcal{V}^{(1)} = \mathcal{V}$。在任意时刻 t，若 $\left|X^{(t)}\right| \leq \eta\,|\mathcal{V}|$，则停止。否则，若 $\left|X^{(t)}\right| \geq \eta\,|\mathcal{V}|$，由引理 4.4 可找到一个仿射子空间 $\mathcal{V}_t \subseteq \mathcal{V}$，其维数为 $\dim(\mathcal{V}_t) \geq \dim(\mathcal{V}) - r\epsilon^{-1}\log_2(1/\eta)$，使得$X_t := X^{(t)} \cap \mathcal{V}_t$ 满足 $|X_t| \geq \eta\,|\mathcal{V}_t|$，且 X_t 在 $\mathcal{V}_t$内是(r,ϵ)-代数扩散的。然后，我们定义 $X^{(t+1)} = X^{(t)} \setminus X_t$。

最后，假设我们在第 $T+1$ 步停止。那么，我们可以将 X 写成不交并 $X = X^{(T+1)} \cup X_1 \cup X_2 \cup \cdots \cup X_T$，其中 $\left|X^{(T+1)}\right| \leq \eta\,|\mathcal{V}|$。 □

备注 4.6。注意

1. 必须有 $T \leq 2^{(1+r/\epsilon)\log_2(1/\eta)}$，因为对于所有 $i \in [T]$,

$$\frac{|X_i|}{|\mathcal{V}|} = \frac{|X_i|}{|\mathcal{V}_i|} \cdot \frac{|\mathcal{V}_i|}{|\mathcal{V}|} \geq \eta \cdot 2^{-r\log_2(1/\eta)/\epsilon} = 2^{-(1+r/\epsilon)\log_2(1/\eta)},$$

以及 $\sum_{i=1}^{T} |X_i| \leq |X| \leq |\mathcal{V}|$。

2. 考虑 $\eta = \eta' \cdot \frac{|X|}{|\mathcal{V}|}$ 有助于获得集合 X 的乘法近似。

4.2.2 两个集合的均匀化

接下来，我们陈述一个关于将两个集合 X， Y 的乘积 $X \times Y$ 分解为分散分量的引理。

引理 *4.7*（两个集合的均匀化，[JLL+25，引理 5.9]）。设 $r \in \mathbb{N}, \epsilon, \eta \in (0, 1/10)$，并设 $X, Y \subseteq \mathcal{V}$ 对于一个线性子空间 $\mathcal{V} \subseteq \mathbb{F}_2^n$。定义 $\alpha_{XY} = |X|\,|Y|\,/|\mathcal{V}|^2$。那么，存在 $T \in \mathbb{N}$，且对于每个 $i \in [T]$，存在一个线性子空间 $\mathcal{V}_i \subseteq \mathcal{V}$、点 $x_i, y_i \in \mathcal{V}/\mathcal{V}_i$ 以及子集 $X_i \subseteq x_i + \mathcal{V}_i$，$Y_i \subseteq y_i + V_i$，使得：

1. $\dim(\mathcal{V}_i) \geq \dim(\mathcal{V}) - O\left(r\epsilon^{-2}\log_2(1/\alpha_{XY})^2 \log_2(1/\eta) + r\epsilon^{-2}\log_2(1/\eta)^5\right)$ *for all* $i \in [T]$.
2. $X_1 \times Y_1, \ldots, X_T \times Y_T$ 是 $X \times Y$ 的互不相交子集，使得

$$\left|(X \times Y) \setminus \cup_{i\in[T]}(X_i \times Y_i)\right| \leq \eta\,|X \times Y|$$

3. 对所有 $i \in [T]$，我们有 $|X_i \times Y_i| \geq \kappa \cdot |\mathcal{V}_i|^2$，其中 $\kappa \geq 2^{-O(\log_2(1/\eta)^2)} \cdot \alpha_{XY}$，且 X_i，Y_i 分别在 $x_i + \mathcal{V}_i, y_i + \mathcal{V}_i$ 内(r, ϵ)代数扩散。

4.2.3 三个集合的均匀化

我们将证明命题 4.3 ，并展示如何将三个集合分解为与对角乘积相容的分散分量。首先，我们陈述一个关于对角乘积 $S(X, Y, Z)$大小的简单事实。结合定理 4.2 ，当 X, Y, Z 中至少一个或两个是分散的时，我们可以控制这个大小。

事实 4.8。设 $X, Y, Z \subseteq \mathcal{V}$ 是线性子空间 $\mathcal{V} \subseteq \mathbb{F}_2^n$，且设 $\alpha_X = |X|\,/|\mathcal{V}|$，$\alpha_Y = |Y|\,/|\mathcal{V}|$，$\alpha_Z = |Z|\,/|\mathcal{V}|$。则，$|S(X, Y, Z)| = \alpha_X\alpha_Y\alpha_Z \cdot \langle \varphi_X * \varphi_Y, \varphi_Z \rangle$.

首先，我们给出一个关于 $S(X, Y, Z)$ 的单轮划分结果：

引理 4.9。设 $\eta \in (0, 1/50)$，并设 $X, Y, Z \subseteq \mathcal{V}$ 为线性子空间 $\mathcal{V} \subseteq \mathbb{F}_2^n$。定义$\alpha = |S(X, Y, Z)|\,/\,|\mathcal{V}|^2$。那么，存在一个整数 $r' = O(\log_2(1/(\eta\alpha))^{16})$以及常数$\epsilon' = \Omega(1)$，使得以下结论成立：

设 $r \in \mathbb{N}$, $\epsilon \in (0, 1/10)$ 满足 $r \geq r'$, $\epsilon \leq \epsilon'$。那么，存在 $T \in \mathbb{N}$ 、一个集合$\mathcal{G} \subseteq [T]$，并且对于每个 $i \in [T]$，都有一个线性子空间 $\mathcal{V}_i \subseteq \mathcal{V}$、点 $x_i, y_i \in \mathcal{V}/\mathcal{V}_i$ 以及子集$X_i \subseteq x_i + \mathcal{V}_i, Y_i \subseteq y_i + \mathcal{V}_i$，$Z_i \subseteq x_i + y_i + \mathcal{V}_i$，使得

1. 维数$(\mathcal{V}_i)$ $\geq$ 维数$(\mathcal{V})$ $- O\left(r\epsilon^{-3}\log_2(1/(\eta\alpha))^6\right)$ 对于所有 $i \in [T]$。
2. $S(X_1, Y_1, Z_1) \ldots, S(X_T, Y_T, Z_T)$ 是 $S(X, Y, Z)$ 的互不相交子集，使得

$$\left|S(X, Y, Z) \setminus \cup_{i=1}^{T} S(X_i, Y_i, Z_i)\right| \leq 4\eta\,|S(X, Y, Z)|\,.$$

3. $|S(X_i, Y_i, Z_i)| \geq 2^{-O(\log_2(1/(\eta\alpha))^2)} \cdot |\mathcal{V}_i|^2$ 对所有 $i \in [T]$成立。
4. 对于所有 $i \in \mathcal{G}$，集合 X_i、Y_i、Z_i 分别在 $x_i + \mathcal{V}_i$、$y_i + \mathcal{V}_i$、$x_i + y_i + \mathcal{V}_i$ 内是 $(r,\ \epsilon)$-代数扩散的。

5. $\sum_{i\in\mathcal{G}} |S(X_i, Y_i, Z_i)| \geq \frac{1}{10} \cdot |S(X, Y, Z)|$.

证明。令 $\kappa = 2^{-O(\log_2(1/(\eta\alpha))^2)} \cdot \alpha_{XY} \geq 2^{-O(\log_2(1/(\eta\alpha))^2)}$ 如引理 4.7 中第三项所述，并取参数 $\eta\alpha$；不妨设 $\kappa \leq \eta\alpha/2$。令 $r' = O(\log_2(1/\kappa)^8)$ $\epsilon' = \Omega(1)$ 如定理 4.2 所述，其中密度为 $\kappa/2$，误差为 $1/10$（即 $d \leftarrow \log_2(2/\kappa)$ 和 $\epsilon \leftarrow 1/10$）。

令 $r_0 = r + \lceil r\epsilon^{-1}\log_2(1/(\eta\alpha))\rceil$。将引理 4.7 应用于 $X \times Y$，取参数 $r_0, \epsilon/10, \eta\alpha$，我们可以找到 $T \in \mathbb{N}$，并且对于每个 $t \in [T]$，都有一个维数为 dim($\mathcal{V}_t \geq \mathcal{V} - O(r_0\epsilon^{-2} \log_2(1/\eta\alpha)^5)$ $x_t\ y_t \in \mathcal{V}/\mathcal{V}_t$ $X_t \subseteq x_t +$) 的线性子空间 $\mathcal{V}_t$，点 $x_t + \mathcal{V}_t$, $\mathcal{V}_t$ $Y_t \subseteq y_t + \mathcal{V}_t$ $|X_t|\,|Y_t| / |\mathcal{V}_t|^2 \geq \kappa$ X_t Y_t r_0 $\epsilon/10$ 以及大小为 $X \times Y$ 的子集 ，使得 $x_t + \mathcal{V}_t$ 中的 $y_t + \mathcal{V}_t$ 分别为 (,)-代数扩散的。此外，我们有 $X_1 \times Y_1$, ..., $X_T \times Y_T$ 是 $X \times Y$ 的互不相交子集，其中 $XY = (X \times Y) \setminus \cup_{t\in[T]}(X_t \times Y_t)$ 满足 $|XY| \leq \eta\alpha\,|X \times Y|$。特别地， $S(X_1, Y_1, Z)$ ....., $S(X_T, Y_T, Z)$ 也是 $S(X, Y, Z)$ 的互不相交子集。

现在，考虑任意一个 $t \in [T]$。注意到 $S(X_t, Y_t, Z) = S(X_t, Y_t, Z_t)$，其中 $Z_t = Z \cap (x_t + t_t + \mathcal{V}_t)$。我们现在进一步分解 $S(X_t, Y_t, Z_t)$，以使第三个集合扩散。对 Z_t,[11] 应用引理 4.5，并取参数 $r, \epsilon, \eta\alpha$，我们可以找到 $T_t \in \mathbb{N}$；对于每个 $t' \in [T_t]$，都有一个线性子空间 $\mathcal{V}_{t,t'} \subseteq \mathcal{V}_t$，其维数 $\dim(\mathcal{V}_{t,t'}) \geq \dim(\mathcal{V}_t) - r\epsilon^{-1}\log_2(1/(\eta\alpha))$，一个点 $z_{t,t'} \in \mathcal{V}_t/\mathcal{V}_{t,t'}$，以及一个大小为 $|Z_{t,t'}| \geq \eta\alpha\,|\mathcal{V}_{t,t'}|$ 的子集 $Z_{t,t'} \subseteq x_t + y_t + z_{t,t'} + \mathcal{V}_{t,t'}$，它是 $\tilde{(}r, \epsilon)$-代数扩散的。此外，我们可以将 Z_t 写成不交并 $Z_t = Z_{t,1} \cup \cdots \cup Z_{t,T_t} \cup Z_t$, $\tilde{}$ ，其中 $|Z_t| \leq \eta\alpha\,|\mathcal{V}_t|$。

注意，对于所有 $t \in [T]$、 $t' \in [T_t]$，我们有 $S(X_t, Y_t, Z_{t,t'}) = \cup_{z\in\mathcal{V}_t/\mathcal{V}_{t,t'}} S(X_{t,t',z}, Y_{t,t',z}, Z_{t,t'})$，其中 $X_{t,t',z} = X_t \cap (x_t + z + \mathcal{V}_{t,t'})$ $Y_{t,t',z} = Y_t \cap (y_t + z + z_{t,t'} + \mathcal{V}_{t,t'})$；回忆一下 $Z_{t,t'} \subseteq x_t + y_t + z_{t,t'} + \mathcal{V}_{t,t'}$。

最后，我们将引理陈述中的集合 X_i, Y_i, Z_i 定义为所有满足以下条件的 $X_{t,t',z}, Y_{t,t',z}, Z_{t,t'}$，其中 $t \in [T], t' \in [T_t], z \in \mathcal{V}_t/\mathcal{V}_{t,t'}$

$$|S(X_{t,t',z}, Y_{t,t',z}, Z_{t,t'})| \geq \eta^2\alpha^2\kappa \cdot |\mathcal{V}_{t,t'}|^2 .$$

此外，我们定义 $\mathcal{G}$ 包含所有满足以下条件的 $X_{t,t',z}, Y_{t,t',z}, Z_{t,t'}$

$$\frac{|X_{t,t',z}|}{|\mathcal{V}_{t,t'}|} \geq (1 - 4\epsilon/10) \cdot \frac{|X_t|}{|\mathcal{V}_t|}, \quad \frac{|Y_{t,t',z}|}{|\mathcal{V}_{t,t'}|} \geq (1 - 4\epsilon/10) \cdot \frac{|Y_t|}{|\mathcal{V}_t|}.$$

我们将在稍后的部分（下方最后一项中）证明，集合 $\mathcal{G}$ 中的片段也满足条件 $|S(X_{t,t',z}, Y_{t,t',z}, Z_{t,t'})| \geq \eta^2\alpha^2\kappa \cdot |\mathcal{V}_{t,t'}|^2$。现在，我们验证引理陈述中的每个结论：

1. 对所有 t, t'，我们有

$$\begin{aligned}\dim(\mathcal{V}_{t,t'}) &\geq \dim(\mathcal{V}_t) - r\epsilon^{-1}\log_2(1/(\eta\alpha)) \\ &\geq \dim(\mathcal{V}) - O\left(r_0\epsilon^{-2}\log_2(1/(\eta\alpha))^5\right) \\ &\geq \dim(\mathcal{V}) - O\left(r\epsilon^{-3}\log_2(1/(\eta\alpha))^6\right).\end{aligned}$$

[11] 形式化地，我们将集合 Z_t 平移，使其位于线性子空间 $\mathcal{V}_t$ 中，然后应用引理并平移回去。

2. 根据构造，集合 $S(X_i, Y_i, Z_i)$ 是 $S(X, Y, Z)$ 的互不相交子集。令 $\mathcal{I}$ 表示所有满足 $|S(X_t, _{t'}, _z, Y_{t,t',z}, Z_{t,t'})| < \eta^2\alpha^2\kappa \cdot |\mathcal{V}_{t,t'}|^2$ 的 (t, t', z)。那么，量 $|S(X, Y, Z)| - \sum_i |S(X_i, Y_i, Z_i)|$ 等于

$$|\widetilde{XY} \cap \{(x, y) : x + y \in Z\}| + \sum_t |S(X_t, Y_t, \tilde{Z}_t)| + \sum_{(t,t',z)\in\mathcal{I}} |S(X_{t,t',z}, Y_{t,t',z}, Z_{t,t'})| .$$

我们逐一对这些项进行界定。

(a) 第一项至多为 $|\widetilde{XY}| \le \eta\alpha |X| |Y| \le \eta\alpha |\mathcal{V}|^2$。

(b) 对任意 $t \in [T]$，都有 X_t, Y_t 是 $(r_0, \epsilon/10)$-代数扩散的，因此 $\tilde{}$ 也是 (r, ϵ)-代数扩散的。因此，根据定理 4.2，我们有 $|S(X_t, Y_t, Z_t)| \le 1.1 \cdot |X_t| |Y_t| \cdot \eta\alpha$。这里我们用到了 X_t, Y_t 的密度至少为 κ，并且在此计算中，我们可以假设 Z_t 的密度至少为 κ（至多为 $\tilde{}$，即 $\eta\alpha/2$），只需向 Z_t 中添加更多元素即可。因此，第二项至多为

$$\sum_{t\in[T]} |S(X_t, Y_t, \tilde{Z}_t)| \le 1.1 \cdot \eta\alpha \cdot \sum_{t\in[T]} |X_t| |Y_t| \le 1.1 \cdot \eta\alpha \cdot |X| |Y| \le 1.1 \cdot \eta\alpha |\mathcal{V}|^2 .$$

(c) 第三项至多为

$$\begin{aligned}
\sum_{(t,t',z)\in\mathcal{I}} |S(X_{t,t',z}, Y_{t,t',z}, Z_{t,t'})| &\le \sum_{(t,t',z)\in\mathcal{I}} \eta^2\alpha^2\kappa \cdot |\mathcal{V}_{t,t'}|^2 \le \sum_{\substack{t,t' \\ z\in\mathcal{V}_t/\mathcal{V}_{t,t'}}} \eta^2\alpha^2\kappa \cdot |\mathcal{V}_{t,t'}|^2 \\
&= \sum_{t,t'} \eta\alpha\kappa \cdot (\eta\alpha |\mathcal{V}_{t,t'}|) \cdot |\mathcal{V}_t| \le \sum_{t,t'} \eta\alpha\kappa \cdot |Z_{t,t'}| \cdot |\mathcal{V}_t| \\
&\le \sum_t \eta\alpha \cdot \left(\kappa |\mathcal{V}_t|^2\right) \le \sum_t \eta\alpha \cdot |X_t| |Y_t| \le \eta\alpha |\mathcal{V}|^2 .
\end{aligned}$$

综合起来，我们得到界 $3.1 \cdot \eta\alpha |\mathcal{V}|^2 \le 4\eta |S(X, Y, Z)|$。

3. 根据构造，我们有 $|S(X_i, Y_i, Z_i)| \ge \eta^2\alpha^2\kappa |\mathcal{V}_i|^2 \ge 2^{-O(\log_2(1/(\eta\alpha))^2)} \cdot |\mathcal{V}_i|^2$。

4. 每个 $Z_{t,t'}$ 在 $x_t + y_t + z_{t,t'} + \mathcal{V}_{t,t'}$ 内都是 (r, ϵ)-代数扩散的。
现在，考虑任意满足 $|X_{t,\ _{t'}\ z}| \ge (1 - 4\epsilon/10) \cdot \frac{|X_t|}{|\mathcal{V}_t|}$ 的 $X_{t,t',z}$。我们证明它在 $x_t + z + \mathcal{V}_{t,t'}$ 内是 (r, ϵ)-代数扩散的。为此，令 $\mathcal{W} \subseteq x_t + z + \mathcal{V}_{t,t'}$ 为任意满足 $\dim(\mathcal{W}) \ge \dim(\mathcal{V}_{t,t'}) - r \ge \dim(\mathcal{V}_t) - r_0$ 的仿射子空间。那么，由于 X_t 在 $x_t + \mathcal{V}_t$ 内是 $(r_0, \epsilon/10)$-代数扩散的，我们得到

$$\frac{|X_{t,t',z} \cap \mathcal{W}|}{|\mathcal{W}|} = \frac{|X_t \cap \mathcal{W}|}{|\mathcal{W}|} \le \left(1 + \frac{\epsilon}{10}\right) \cdot \frac{|X_t|}{|\mathcal{V}_t|} \le \frac{\left(1 + \frac{\epsilon}{10}\right)}{\left(1 - \frac{4\epsilon}{10}\right)} \cdot \frac{|X_{t,t',z}|}{|\mathcal{V}_{t,t'}|} \le (1 + \epsilon) \cdot \frac{|X_{t,t',z}|}{|\mathcal{V}_{t,t'}|}.$$

类似的论证表明，$Y_{t,t',z}$ 在 $y_t + z + z_{t,t'} + \mathcal{V}_{t,t'}$ 内是 (r, ϵ)-代数扩散的，假设 $|Y_{t,\ _{t'}\ z}| \ge (1 - 4\epsilon/10) \cdot \frac{|Y_t|}{|\mathcal{V}_t|}$。

5. 考虑 $\mathcal{G}$中的任意片段$X_{t,t',z}$,$Y_{t,t',z}$,$Z_{t,t'}$ 。它满足

$$\frac{|X_{t,t',z}|}{|\mathcal{V}_{t,t'}|} \geq (1-4\epsilon/10)\cdot\frac{|X_t|}{|\mathcal{V}_t|} \geq \frac{\kappa}{2}, \quad \frac{|Y_{t,t',z}|}{|\mathcal{V}_{t,t'}|} \geq (1-4\epsilon/10)\cdot\frac{|Y_t|}{|\mathcal{V}_t|} \geq \frac{\kappa}{2}, \quad \frac{|Z_{t,t'}|}{|\mathcal{V}_{t,t'}|} \geq \eta\alpha \geq \frac{\kappa}{2}.$$

由于这三者都是$(r、\ \epsilon)$-代数扩散的，且有 $r \geq r'、\ \epsilon \leq \epsilon'$，根据定理4.2，

$$\begin{aligned}
|S(X_{t,t',z}, Y_{t,t',z}, Z_{t,t'})| &\geq \frac{9}{10}\cdot\frac{|X_{t,t',z}|}{|\mathcal{V}_{t,t'}|}\cdot\frac{|Y_{t,t',z}|}{|\mathcal{V}_{t,t'}|}\cdot\frac{|Z_{t,t'}|}{|\mathcal{V}_{t,t'}|}\cdot|\mathcal{V}_{t,t'}|^2 \\
&\geq \frac{9}{10}\cdot\left(1-\frac{4\epsilon}{10}\right)^2\cdot\frac{|X_t|\,|Y_t|}{|\mathcal{V}_t|^2}\cdot\frac{|Z_{t,t'}|}{|\mathcal{V}_{t,t'}|}\cdot|\mathcal{V}_{t,t'}|^2 \\
&\geq \frac{1}{2}\cdot\frac{|X_t|\,|Y_t|}{|\mathcal{V}_t|^2}\cdot|Z_{t,t'}|\,|\mathcal{V}_{t,t'}|\,. \qquad (1)
\end{aligned}$$

特别地，上式至少为$1/2\cdot\kappa\cdot\eta\alpha\,|\mathcal{V}_{t、\ t'}|^2 \geq \eta^2\alpha^2\kappa\cdot|\mathcal{V}_{t、\ t'}|^2$，这表明 $\mathcal{G}$ 中的片段是未被丢弃的片段 $X_i、\ Y_i、\ Z_i$ 的子集。

现在，固定任意 $t \in [T]、\ t' \in [T_t]$。我们证明

$$\Pr_{z\sim\mathcal{V}_t/\mathcal{V}_{t,t'}}\left[\frac{|X_{t,t',z}|}{|\mathcal{V}_{t,t'}|} \geq (1-4\epsilon/10)\cdot\frac{|X_t|}{|\mathcal{V}_t|}\right] \geq 4/5.$$

为此，令 p 表示左侧的概率。注意，对于每个$z \in \mathcal{V}_t/\mathcal{V}_{t、\ t'}$，由于 X_t 在 $x_t+\mathcal{V}_t$ 内是$(r_0、\ \epsilon/10)$-代数扩散的，我们有上界$|X_{t、\quad t'\ z}|_{、,t'}| \leq (1+\epsilon/10)\cdot\frac{|X_t|}{|\mathcal{V}_t|}$。这意味着

$$\frac{|X_t|}{|\mathcal{V}_t|} = \mathop{\mathbb{E}}_{z\sim\mathcal{V}_t/\mathcal{V}_{t,t'}}\left[\frac{|X_{t,t',z}|}{|\mathcal{V}_{t,t'}|}\right] \leq (1-p)\cdot(1-4\epsilon/10)\cdot\frac{|X_t|}{|\mathcal{V}_t|} + p\cdot(1+\epsilon/10)\cdot\frac{|X_t|}{|\mathcal{V}_t|},$$

从而得到 $p \geq 4/5$。

因此，对于任意 $t \in [T]$，$t' \in [T_t]$，根据上述结果，并对 $Y_{t,\ t',\ z}$ 使用类似的界，

$$\Pr_{z\sim\mathcal{V}_t/\mathcal{V}_{t,t'}}\left[\frac{|X_{t,t',z}|}{|\mathcal{V}_{t,t'}|} \geq (1-4\epsilon/10)\cdot\frac{|X_t|}{|\mathcal{V}_t|}, \quad \frac{|Y_{t,t',z}|}{|\mathcal{V}_{t,t'}|} \geq (1-4\epsilon/10)\cdot\frac{|Y_t|}{|\mathcal{V}_t|}\right] \geq 3/5.$$

结合前面的界（方程 1），得到

$$\begin{aligned}
\sum_{i\in\mathcal{G}}|S(X_i,Y_i,Z_i)| &\geq \sum_{t\in[T],t'\in[T_t]}\frac{1}{2}\cdot\frac{|X_t|\,|Y_t|}{|\mathcal{V}_t|^2}\cdot|Z_{t,t'}|\,|\mathcal{V}_{t,t'}|\cdot\left(\frac{3}{5}\cdot\frac{|\mathcal{V}_t|}{|\mathcal{V}_{t,t'}|}\right) \\
&= \sum_{t\in[T],t'\in[T_t]}\frac{3}{10}\cdot\frac{|X_t|\,|Y_t|}{|\mathcal{V}_t|}\cdot|Z_{t,t'}| \\
&\geq \sum_{t\in[T]}\frac{3}{10}\cdot\frac{|X_t|\,|Y_t|}{|\mathcal{V}_t|}\cdot(|Z_t|-\eta\alpha\,|\mathcal{V}_t|) \\
&= \sum_{t\in[T]}\frac{3}{10}\cdot\frac{|X_t|\,|Y_t|\,|Z_t|}{|\mathcal{V}_t|} - \eta\alpha\sum_{t\in[T]}|X_t|\,|Y_t| \\
&\geq \sum_{t\in[T]}\frac{3}{10}\cdot\frac{|X_t|\,|Y_t|\,|Z_t|}{|\mathcal{V}_t|}\cdot\mathbb{1}\left[|Z_t| \geq \eta\alpha\,|\mathcal{V}_t|\right] - \eta\alpha\,|\mathcal{V}|^2\,.
\end{aligned}$$

现在，由于 X_t， Y_t 分别在 $(r_0,\ \epsilon/10)$-代数扩散于 $x_t+\mathcal{V}_t$， $y_t+\mathcal{V}_t$ 根据 r'、ϵ'的选取以及定理 4.2，我们有 $|S(X_t,\ Y_t,\ Z_t)| \le 1.1 \cdot \frac{|X_t||Y_t||Z_t|}{|\mathcal{V}_t|}$ 只要 $|Z_t| \ge \eta\alpha\,|\mathcal{V}_t| \ge \kappa|\mathcal{V}_t|$。因此，

$$\begin{aligned}
\sum_{i\in\mathcal{G}} |S(X_i,Y_i,Z_i)| &\ge \sum_{t\in[T]} \frac{3}{10}\cdot\frac{1}{1.1}\cdot|S(X_t,Y_t,Z_t)|\cdot\mathbb{1}\left[|Z_t|\ge\eta\alpha\,|\mathcal{V}_t|\right]-\eta\alpha\,|\mathcal{V}|^2\\
&\ge 0.25\cdot\sum_{t\in[T]}|S(X_t,Y_t,Z_t)| - \sum_{t\in[T]}|S(X_t,Y_t,Z_t)|\cdot\mathbb{1}\left[|Z_t|<\eta\alpha\,|\mathcal{V}_t|\right]-\eta\alpha\,|\mathcal{V}|^2\\
&\ge 0.25\cdot|S(X,Y,Z)| - \eta\alpha\,|\mathcal{V}|^2 - 1.1\cdot\sum_{t\in[T]}|X_t|\,|Y_t|\,\eta\alpha-\eta\alpha\,|\mathcal{V}|^2.\\
&\ge 0.25\cdot|S(X,Y,Z)|-3.1\eta\alpha\,|\mathcal{V}|^2\\
&= (0.25-3.1\eta)\cdot|S(X,Y,Z)| \ge 0.1\cdot|S(X,Y,Z)|.
\end{aligned}$$

对于中间项 $|S(X_t,\ Y_t,\ Z_t)|\cdot\mathbb{1}\left[|Z_t|<\eta\alpha\right]$，我们用到了 X_t、Y_t 分别在 $x_t+\mathcal{V}_t$、$y_t+\mathcal{V}_t$ 内是（r_0、$\epsilon/10$）-代数扩散这一事实；此外，为了计算上界，我们还假设 $|Z_t|/|\mathcal{V}_t| \ge \kappa$，这可以通过向 Z_t 中添加更多元素得到。 □

我们写出上述引理的一个更简单版本，并去掉对 r、ϵ 的假设：

推论 4.10。 设 $r\in\mathbb{N}, \epsilon,\eta\in(1/10)$，且 $X,Y,Z\subseteq\mathcal{V}$ 属于线性子空间 $\mathcal{V}\subseteq\mathbb{F}_2^n$。定义 $\alpha=|S(X,Y,Z)|/|\mathcal{V}|^2$。那么，存在 $T\in\mathbb{N}$、一个集合 $\mathcal{G}\subseteq[T]$，并且对每个 $i\in[T]$，存在一个线性子空间 $\mathcal{V}_i\subseteq\mathcal{V}$、点 $x_i,y_i\in\mathcal{V}/\mathcal{V}_i$ 以及子集 $X_i\subseteq x_i+\mathcal{V}_i, Y_i\subseteq y_i+\mathcal{V}_i, Z_i\subseteq x_i+y_i+\mathcal{V}_i$，使得

1. $\dim(\mathcal{V}_i)\ge\dim(\mathcal{V})-O\left(r\epsilon^{-3}\log_2(1/(\eta\alpha))^6+\epsilon^{-3}\log_2(1/(\eta\alpha))^{22}\right)$ *for all* $i\in[T]$.
2. $S(X_1,Y_1,Z_1)\ldots,S(X_T,Y_T,Z_T)$ 是 $S(X,Y,Z)$ 的两两不相交子集，且
$$\left|S(X,Y,Z)\setminus\cup_{i=1}^T S(X_i,Y_i,Z_i)\right| \le \eta\,|S(X,Y,Z)|.$$
3. $|S(X_i,Y_i,Z_i)|\ge 2^{-O(\log_2(1/(\eta\alpha))^2)}\cdot|\mathcal{V}_i|^2$ 对所有 $i\in[T]$ 均成立。
4. 对所有 $i\in\mathcal{G}$，集合 X_i,Y_i,Z_i 分别在 $x_i+\mathcal{V}_i, y_i+\mathcal{V}_i, x_i+y_i+\mathcal{V}_i$ 内是(r,ϵ)-代数扩散的。
5. $\sum_{i\in\mathcal{G}}|S(X_i,Y_i,Z_i)|\ge\frac{1}{10}\cdot|S(X,Y,Z)|$.

证明。 代入参数 $\eta/5$，应用引理4.9 可得 $r'=O(\log_2(1/(\eta\alpha))^{16})$，并且$\epsilon'=\Omega(1)$。然后，使用参数 $r_0=r+r'$ 和 $\epsilon_0=\epsilon\cdot\epsilon'$应用该引理，并注意到，任何一个 (r_0,ϵ_0)-代数扩散的集合也都是 (r,ϵ)-代数扩散的。 □

最后，我们完成本节的主要结果：

命题 4.3 的证明。给定集合 X、Y、$Z \subseteq \mathcal{V}$，我们执行以下递归过程：令 $T \in \mathbb{N}$、$\mathcal{G} \subseteq [T]$ 以及子集 $X_i \subseteq x_i + \mathcal{V}_i$、$Y_i \subseteq y_i + \mathcal{V}_i$、$Z_i \subseteq x_i + y_i + \mathcal{V}_i$ 如推论 4.10 中所述，参数为 r、$\frac{\epsilon}{10}$、$\frac{\eta^2}{100}$。现在，对每个 $i \in [T] \setminus \mathcal{G}$，我们使用参数 ~~$r$~~、$\frac{\epsilon}{10}$、$\frac{\eta^2}{100}$，在 X_i、Y_i、Z_i [12] 上递归调用推论 4.10。当递归深度达到 $L = \lceil 20 \log_2(1/\eta) \rceil$ 时，我们终止递归，~~—~~ 并丢弃此时剩余的所有片段。

注意，对于任意 X_i，Y_i，Z_i，若它们属于某个线性子空间 $\mathcal{V}_i \subseteq \mathcal{V}$的仿射平移，且算法在某个时刻看到了它们但没有将其丢弃，则有

$$\frac{|S(X_i, Y_i, Z_i)|}{|\mathcal{V}_i|^2} \geq 2^{-(\log_2(4/\alpha))^{\mathrm{poly}(1/\eta)}}.$$

根据推论4.10，测度在单步中从 β 降至 $2^{-O(\log_2(1/(\eta\beta))^2)}$，而步数为 $L = O(\log_2(1/\eta))$。由此，我们验证命题陈述中的各项结论：

1. 每一步中，维数最多减少 $r\epsilon^{-3}\log_2(4/\alpha)^{\mathrm{poly}(1/\eta)}$，步数为 $L = O(\log_2(1/\eta))$。

2. 片段之间互不相交是由构造保证的。
   在每个递归层中，被丢弃的片段总规模至多为 $\frac{\eta^2}{100} \cdot |S(X, Y, Z)|$。~~—~~
   此外，在任意一层中，继续递归处理的片段总规模至多为上一层片段总规模的 $9/10$ 倍；特别地，第 L 层的片段总规模至多为$(9/10)^L \cdot |S(X, Y, Z)| \leq \eta^2 |S(X, Y, Z)|$。因此，被丢弃的片段总比例至多为

$$\frac{\eta^2}{100} \cdot 21 \log_2(1/\eta) + \eta^2 \leq \eta.$$

3. 关于 X_i、Y_i、Z_i 的大小界如上所述，其扩散性由推论4.10得出。 □

5 均匀平方覆盖

本节中，我们证明，任何由代数扩展集（见定义*2.1*）组成的对角乘积集合（见定义2.1）都可由正方形（见定义4.1）均匀覆盖（见定义2.2）。在第5.1节中，我们介绍一个对本文有用的组合扩展性概念；在第5.2节中，我们证明代数扩展集满足该定义（以一种特定方式）；最后，在第5.3节中，我们证明命题5.6，即我们的正方形覆盖结果。

5.1 组合扩展性与图计数

我们陈述 [KLM24]中的一些有用定义：

[12]形式上，我们将这些集合平移，使它们都位于线性子空间 $\mathcal{V}_i$ 中，然后应用推论，再平移回去。

定义 5.1 (组合扩展性**)**。 设 X, Y 为有限集，且令 $f\colon X \times Y \to \{0,1\}$。若对于满足 $|S \times T| \geq 2^{-r} |X \times Y|$的每个 $S \subseteq X$, $T \subseteq Y$，都有

$$\mathop{\mathbb{E}}_{(x,y)\sim S\times T}[f(x,y)] \leq (1+\epsilon)\,\mathbb{E}[f],$$

其中 $\mathbb{E}[f] = \mathbb{E}_{(x,y)\sim X\times Y}[f(x、y)]$。

定义 5.2 （下有界左边缘）。设 X、Y 为有限集，并设 $f\colon X\times Y \to \{0,1\}$。如果 f 具有（r、ϵ）下有界左边缘，则称其具有

$$\Pr_{x\sim X}\left[\mathop{\mathbb{E}}_{y\sim Y}[f(x,y)] \leq (1-\epsilon)\cdot\mathbb{E}[f]\right] \leq 2^{-r}.$$

我们给出一个关于扩展集中的图计数的结果：

定理 5.3 （[FHHK24，定理 2。1]）。对于任意 $k \in \mathbb{N}$, $\epsilon \in$ （0，1），存在充分小的 $\gamma = \gamma(\epsilon, k) > 0$，以及充分大的 $C = C(\epsilon, k) \in \mathbb{N}$，使得以下结论成立：

设 $H =$（$[k]$、E）为有向图，其中（i、j）$\in E$蕴含 $i < j$。设 X_1、.....、X_k为有限集；设 $d \geq 1$，并且对于每个（i、j）$\in E$，令 $f_{ij}\colon X_i \times X_j \to \{0,1\}$ 为满足以下条件的函数：

1. $\mathbb{E}[f_{ij}] \geq 2^{-d}$，2. f_{ij} 是(Cd^2, γ)-组合扩散的，并且3. f_{ij} 具有(Cd, γ)-下有界左边缘。

于是，成立：

$$\left|\mathop{\mathbb{E}}_{x_1\sim X_1,\ldots,x_k\sim X_k}\left[\prod_{(i,j)\in E} f_{ij}(x_i,x_j)\right] - \prod_{(i,j)\in E}\mathbb{E}[f_{ij}]\right| \leq \epsilon\cdot\prod_{(i,j)\in E}\mathbb{E}[f_{ij}].$$

5.2 代数扩散性蕴含图计数

我们证明，与代数扩散集合对应的某个函数既是组合扩散的，又具有下有界左边缘。

引理5.4。 设 $d, r \geq 1, \epsilon \in (0, 1/4)$。那么，存在一个充分大的整数 $s = (r^8 + d^8)\cdot\epsilon^{-O(1)}$，以及一个充分小的 $\delta = \Omega(\epsilon)$，使得下述结论成立：

设 $X, Y, Z \subseteq \mathbb{F}_2^n$是密度至少为 2^{-d}的子集，并且 Y, Z是(s, δ)-代数扩散的。那么，函数 $f\colon X\times Y \to \{0,1\}$，定义为 $f(x,y) = \mathbb{1}[x+y \in Z]$，满足：

1. $|\mathbb{E}[f] - \alpha_Z| \leq \epsilon\cdot\alpha_Z$，其中 $\alpha_Z = |Z|/2^n$，
2. f 是(r, ϵ)-组合扩散的，并且

3. f 具有(r,ϵ)-下有界左边缘。

证明。 令 s,δ满足定理 4.2 的条件，其中参数为 $r+d,\epsilon/4$。首先，我们有

$$\mathbb{E}[f]=\Pr_{x\sim X,y\sim Y}[x+y\in Z]=\langle\varphi_X*\varphi_Y,\mathbb{1}_Z\rangle=\alpha_Z\cdot\langle\varphi_X*\varphi_Y,\varphi_Z\rangle.$$

因此，根据定理 4.2(i)，可得

$$|\mathbb{E}[f]-\alpha_Z|\le\frac{\epsilon}{4}\cdot\alpha_Z.$$

接下来，我们证明组合扩展性。令 $S\subseteq X,\ T\subseteq Y$满足 $|S\times T|\ge 2^{-r}|X\times Y|$。我们可以写成

$$\mathop{\mathbb{E}}_{(x,y)\sim S\times T}[f(x,y)]=\alpha_Z\cdot\langle\varphi_S*\varphi_T,\varphi_Z\rangle.$$

由于 $|X|\ge 2^{-d}\cdot 2^n$，我们有 $|S|\cdot|Y|\ge|S\times T|\ge 2^{-r}\cdot|X\times Y|\ge 2^{-r}\cdot 2^{n-d}\cdot|Y|$，因此 $|S|\ge 2^{-(r+d)}\cdot 2^n$。类似地， $|T|\ge 2^{-(r+d)}\cdot 2^n$，因此根据定理 4.2(ii)，可得

$$\mathop{\mathbb{E}}_{(x,y)\sim S\times T}[f(x,y)]\le\left(1+\frac{\epsilon}{4}\right)\alpha_Z\le\left(1+\frac{\epsilon}{4}\right)\cdot\left(1-\frac{\epsilon}{4}\right)^{-1}\mathbb{E}[f]\le(1+\epsilon)\cdot\mathbb{E}[f].$$

最后，我们证明下有界左边缘。定义 $A\subseteq X$ 如下

$$A=\left\{x\in X:\mathop{\mathbb{E}}_{y\sim Y}[f(x,y)]\le(1-\epsilon)\cdot\mathbb{E}[f]\right\}.$$

反设 $|A|>2^{-r}|X|$；那么， $|A|\ge 2^{-(r+d)}\cdot 2^n$。根据 A 的定义，我们有

$$\mathop{\mathbb{E}}_{x\sim A,y\sim Y}[f(x,y)]\le(1-\epsilon)\,\mathbb{E}[f].$$

另一方面，根据定理 4.2(i)，我们有

$$\mathop{\mathbb{E}}_{x\sim A,y\sim Y}[f(x,y)]=\alpha_Z\cdot\langle\varphi_A*\varphi_Y,\varphi_Z\rangle\ge\left(1-\frac{\epsilon}{4}\right)\alpha_Z\ge\left(1-\frac{\epsilon}{4}\right)\cdot\left(1+\frac{\epsilon}{4}\right)^{-1}\mathbb{E}[f]>(1-\epsilon)\,\mathbb{E}[f],$$

which is a contradiction. □

5.3 扩散对角积集中的正方形

在本小节中，我们证明正方形覆盖结果。首先证明以下计数引理：

引理 5.5。 设 $\epsilon\in(0,1/4)$ 是一个常数，且设 $d\ge 1$。那么，存在一个充分大的整数 $r=O_\epsilon(d^{16})$ 以及一个充分小的 $\delta=\delta(\epsilon)>0$，使得以下结论成立：

设 $X,Y,Z\subseteq\mathbb{F}_2^n$ 的密度均至少为 2^{-d}，且 X,Y,Z 全部都是 (r,δ)-代数扩散的。设 $S=S(X,Y,Z)$ 如定义 *2.1* 所示，并设 $\Gamma:\mathbb{F}_2^n\times\mathbb{F}_2^n\to\mathbb{R}$ 是将 (x,y) 映射到 S 中包含 (x,y) 的正方形的归一化数量的函数（见定义 *2.2*），即

$$\Gamma(x,y)=\mathop{\mathbb{E}}_{w\sim\mathbb{F}_2^n}\left[\mathbb{1}\left[s_{x,y,w}\subseteq S\right]\right].$$

定义 $\alpha_X=\mathbb{E}[\mathbb{1}_X]$、 $\alpha_Y=\mathbb{E}[\mathbb{1}_Y]$、 $\alpha_Z=\mathbb{E}[\mathbb{1}_Z]$。则有

1. $||S| \cdot 2^{-2n} - \alpha_X\alpha_Y\alpha_Z| \le \epsilon \cdot \alpha_X\alpha_Y\alpha_Z$。
2. $|\|\Gamma\|_1 - \alpha_X^2\alpha_Y^2\alpha_Z^2| \le \epsilon \cdot \alpha_X^2\alpha_Y^2\alpha_Z^2$。
3. $\left|\|\Gamma\|_2^2 - \alpha_X^3\alpha_Y^3\alpha_Z^3\right| \le \epsilon \cdot \alpha_X^3\alpha_Y^3\alpha_Z^3$。

证明。设 $f\colon X \times Y \to \{0,1\}$, $g\colon Y \times Z \to \{0,1\}$, $h\colon X \times Z \to \{0,1\}$ 由下式给出

$$f(x,y) = \mathbb{1}[x+y \in Z], \quad g(y,z) = \mathbb{1}[y+z \in X], \quad h(x,z) = \mathbb{1}[x+z \in Y].$$

设 $\gamma = \gamma(\frac{\epsilon}{10}, 4) \le \frac{\epsilon}{10}$, $C = C(\frac{\epsilon}{10}, 4)$ 如定理 5.3 中所述。于是，根据引理5.4以及参数 (r,δ) 的选取，我们可以假设 f（g, h 也类似）满足 $|\mathbb{E}[f] - \alpha_Z| \le \gamma\alpha_Z \le \frac{\epsilon}{10}\alpha_Z$，且 f 是 (Cd^2, γ)-组合扩散的，而 f 具有 (Cd, γ)-下有界左边缘。

首先，注意到

$$|S| \cdot 2^{-2n} = \mathop{\mathbb{E}}_{x,y\sim\mathbb{F}_2^n}[\mathbb{1}[x \in X, y \in Y, x+y \in Z]] = \alpha_X\alpha_Y \Pr_{x\sim X, y\sim Y}[x+y \in Z] = \alpha_X\alpha_Y\,\mathbb{E}[f].$$

由此可得结果，因为 $|\mathbb{E}[f] - \alpha_Z| \le \gamma\alpha_Z \le \frac{\epsilon}{10}\alpha_Z$。

接下来，我们注意到

$$\begin{aligned}
\|\Gamma\|_1 &= \mathop{\mathbb{E}}_{x,y,w\sim\mathbb{F}_2^n}[\mathbb{1}[s_{x,y,w} \subseteq S]] \\
&= \mathop{\mathbb{E}}_{x,y,w\sim\mathbb{F}_2^n}[\mathbb{1}_X(x)\mathbb{1}_X(x+w)\mathbb{1}_Y(y)\mathbb{1}_Y(y+w)\mathbb{1}_Z(x+y)\mathbb{1}_Z(x+y+w)] \\
&= \mathop{\mathbb{E}}_{x,y,z\sim\mathbb{F}_2^n}[\mathbb{1}_X(x)\mathbb{1}_X(y+z)\mathbb{1}_Y(y)\mathbb{1}_Y(x+z)\mathbb{1}_Z(x+y)\mathbb{1}_Z(z)] \quad (\text{replace } w = x+y+z) \\
&= \alpha_X\alpha_Y\alpha_Z \mathop{\mathbb{E}}_{x\sim X, y\sim Y, z\sim Z}[f(x,y)g(y,z)h(x,z)].
\end{aligned}$$

现在，根据定理 5.3（取有向图 $\{(1,2),(1,3),(2,3)\}$，其中 $1,2,3$ 分别标记为X, Y, Z），我们得到

$$\begin{aligned}
(1-\epsilon)\cdot\alpha_X\alpha_Y\alpha_Z &\le \left(1-\frac{\epsilon}{10}\right)^4 \cdot \alpha_X\alpha_Y\alpha_Z \\
&\le \left(1-\frac{\epsilon}{10}\right)\cdot \mathbb{E}[f]\,\mathbb{E}[g]\,\mathbb{E}[h] \\
&\le \mathop{\mathbb{E}}_{x\sim X, y\sim Y, z\sim Z}[f(x,y)g(y,z)h(x,z)] \\
&\le \left(1+\frac{\epsilon}{10}\right)\cdot \mathbb{E}[f]\,\mathbb{E}[g]\,\mathbb{E}[h] \\
&\le \left(1+\frac{\epsilon}{10}\right)^4 \cdot \alpha_X\alpha_Y\alpha_Z \le (1+\epsilon)\cdot\alpha_X\alpha_Y\alpha_Z,
\end{aligned}$$

因此

$$\left|\|\Gamma\|_1 - \alpha_X^2\alpha_Y^2\alpha_Z^2\right| \le \epsilon \cdot \alpha_X^2\alpha_Y^2\alpha_Z^2.$$

最后，我们可以写成

$$\begin{aligned}\|\Gamma\|_2^2 &= \mathop{\mathbb{E}}_{x,y,w,w'\sim\mathbb{F}_2^n}\left[\mathbb{1}\left[s_{x,y,w}\subseteq S, s_{x,y,w'}\subseteq S\right]\right]\\ &= \mathop{\mathbb{E}}_{x,y,z,z'\sim\mathbb{F}_2^n}\left[\mathbb{1}\left[s_{x,y,x+y+z}\subseteq S, s_{x,y,x+y+z'}\subseteq S\right]\right] \quad (\text{replace } w=x+y+z, w'=x+y+z')\\ &= \mathop{\mathbb{E}}_{x,y,z,z'\sim\mathbb{F}_2^n}\left[\mathbb{1}_X(x)\mathbb{1}_X(y+z)\mathbb{1}_X(y+z')\mathbb{1}_Y(y)\mathbb{1}_Y(x+z)\mathbb{1}_Y(x+z')\mathbb{1}_Z(x+y)\mathbb{1}_Z(z)\mathbb{1}_Z(z')\right]\\ &= \alpha_X\alpha_Y\alpha_Z^2 \mathop{\mathbb{E}}_{x\sim X,y\sim Y,z,z'\sim Z}\left[f(x,y)g(y,z)g(y,z')h(x,z)h(x,z')\right].\end{aligned}$$

现在，由定理 5.3（取有向图 {(1, 2), (1, 3), (1, 4), (2, 3), (2, 4)}，其中 1、2、3、4 分别标记为 X、Y、Z、Z），可得

$$\begin{aligned}(1-\epsilon)\cdot\alpha_X^2\alpha_Y^2\alpha_Z &\le \left(1-\frac{\epsilon}{10}\right)^6\cdot\alpha_X^2\alpha_Y^2\alpha_Z\\ &\le \left(1-\frac{\epsilon}{10}\right)\cdot\mathbb{E}[f]\,\mathbb{E}[g]^2\,\mathbb{E}[h]^2\\ &\le \mathop{\mathbb{E}}_{x\sim X,y\sim Y,z,z'\sim Z}\left[f(x,y)g(y,z)g(y,z')h(x,z)h(x,z')\right]\\ &\le \left(1+\frac{\epsilon}{10}\right)\cdot\mathbb{E}[f]\,\mathbb{E}[g]^2\,\mathbb{E}[h]^2\\ &\le \left(1+\frac{\epsilon}{10}\right)^6\cdot\alpha_X^2\alpha_Y^2\alpha_Z \le (1+\epsilon)\cdot\alpha_X^2\alpha_Y^2\alpha_Z,\end{aligned}$$

因此

$$\left|\|\Gamma\|_2^2-\alpha_X^3\alpha_Y^3\alpha_Z^3\right|\le\epsilon\cdot\alpha_X^3\alpha_Y^3\alpha_Z^3. \qquad \square$$

有了以上结果，我们可以证明本节的主要结论了。

命题 5.6。设 $\epsilon\in(0,1/4)$ 为一个常数，且 $d\ge 1$。那么，存在一个充分大的整数 $r=O_\epsilon(d^{16})$ 和一个充分小的 $\delta=\delta(\epsilon)>0$，使得下述结论成立：

设 X、Y、$Z\subseteq\mathbb{F}_2^n$的密度均至少为 2^{-d}，且 X、Y、Z均为 (r,δ)-代数扩散的。设 $S=S(X,Y,Z)$ 如定义 *2.1*所述，并令 $\mathcal{T}$表示 S 中的所有正方形的集合（见定义*2.2*）；形式化地，

$$\mathcal{T}=\left\{(x,y,w)\in(\mathbb{F}_2^n)^3 : s_{x,y,w}\subseteq S\right\}.$$

定义 $\alpha_X=\mathbb{E}[\mathbb{1}_X]$, $\alpha_Y=\mathbb{E}[\mathbb{1}_Y]$, $\alpha_Z=\mathbb{E}[\mathbb{1}_Z]$。那么，成立：

1. $\left||S|\cdot 2^{-2n}-\alpha_X\alpha_Y\alpha_Z\right|\le\epsilon\cdot\alpha_X\alpha_Y\alpha_Z$。
2. $\left||\mathcal{T}|\cdot 2^{-3n}-\alpha_X^2\alpha_Y^2\alpha_Z^2\right|\le\epsilon\cdot\alpha_X^2\alpha_Y^2\alpha_Z^2$。
3. 令 μ 为 S 上按如下方式得到的分布：在 S 中均匀随机选取一个随机方形，即均匀随机选取 $(x,y,w)\sim\mathcal{T}$；然后，从集合 $s_{x,\ y,\ w}$ 中均匀随机输出一个元素。成立：

$$\|\mu-U_S\|_1\le\epsilon,$$

其中 U_S 表示 S上的均匀分布。

证明。令 $(r,\ \delta)$ 满足引理 5.5 在参数 d 和 $\epsilon^2/5:=\gamma$下成立，并令 Γ为引理 5.5陈述中的函数。根据引理 5.5，可直接得到

$$\left||S|\cdot 2^{-2n}-\alpha_X\alpha_Y\alpha_Z\right|\le\gamma\cdot\alpha_X\alpha_Y\alpha_Z\le\epsilon\cdot\alpha_X\alpha_Y\alpha_Z.$$

现在，注意到

$$|\mathcal{T}|=\sum_{x,y,w\in\mathbb{F}_2^n}\mathbb{1}\left[s_{x,y,w}\subseteq S\right]=2^{3n}\left\|\Gamma\right\|_1,$$

因此由引理5.5,

$$\left||\mathcal{T}|\cdot 2^{-3n}-\alpha_X^2\alpha_Y^2\alpha_Z^2\right|\le\gamma\cdot\alpha_X^2\alpha_Y^2\alpha_Z^2\le\epsilon\cdot\alpha_X^2\alpha_Y^2\alpha_Z^2.$$

最后，我们回顾备注 2.3：每个正方形 $s_{x,\ y,\ w}\subseteq S$ 满足 $w\neq 0$的对象在 $\mathcal{T}$中恰好出现 4 次，因为 $s_{x,\ y,\ w}=s_{x+w,\ y,\ w}=s_{x,\ y+w,\ w}=s_{x+w,\ y+w,\ w}$。此外，当 $w=0$时，我们有$s_{x,\ y,\ 0}=\{(x,\ y)\}$。因此，对于任意 $(x,\ y)\in S$,

$$\mu[(x,y)]=\frac{1}{|\mathcal{T}|}\cdot\left(\sum_{w\in\mathbb{F}_2^n,w\neq 0}4\cdot\mathbb{1}\left[s_{x,y,w}\subseteq S\right]\cdot\frac{1}{4}+\mathbb{1}\left[s_{x,y,0}\subseteq S\right]\cdot 1\right)=\frac{\Gamma(x,y)\cdot 2^n}{|\mathcal{T}|}.\tag{2}$$

因此，我们可以计算 μ 的 ℓ_2-范数，得到

$$\begin{aligned}\|\mu\|_2^2&=\sum_{(x,y)\in S}\mu[(x,y)]^2\\&=\frac{2^{2n}}{|\mathcal{T}|^2}\cdot\sum_{(x,y)\in S}\Gamma(x,y)^2\\&=\frac{2^{2n}}{|\mathcal{T}|^2}\cdot\sum_{x,y\in\mathbb{F}_2^n}\Gamma(x,y)^2&&(\text{as }\Gamma(x,y)=0\text{ for }(x,y)\notin S)\\&=\frac{2^{4n}}{|\mathcal{T}|^2}\cdot\|\Gamma\|_2^2.\end{aligned}$$

现在，由引理5.5，我们得到

$$\|\mu\|_2^2\le\frac{2^{4n}}{|\mathcal{T}|^2}\cdot(1+\gamma)\cdot\alpha_X^3\alpha_Y^3\alpha_Z^3,$$

因此，

$$\begin{aligned}\|\mu\|_2^2\cdot|S|&\le 2^{4n}\cdot(1+\gamma)\cdot\alpha_X^3\alpha_Y^3\alpha_Z^3\cdot\frac{|S|}{|\mathcal{T}|^2}\\&\le 2^{4n}\cdot(1+\gamma)\cdot\alpha_X^3\alpha_Y^3\alpha_Z^3\cdot\frac{(1+\gamma)\cdot\alpha_X\alpha_Y\alpha_Z\cdot 2^{2n}}{(1-\gamma)^2\cdot\alpha_X^4\alpha_Y^4\alpha_Z^4\cdot 2^{6n}}\\&=\frac{(1+\gamma)^2}{(1-\gamma)^2}\le 1+5\gamma.&&(\text{as }\gamma\le 0.1)\end{aligned}$$

最后，根据柯西-施瓦茨不等式，我们得到

$$\|\mu-U_S\|_1\le\left(|S|\cdot\|\mu-U_S\|_2^2\right)^{1/2}=\left(|S|\cdot\left(\|\mu\|_2^2-\frac{1}{|S|}\right)\right)^{1/2}\le\sqrt{5\gamma}=\epsilon.\qquad\square$$

6 支持 GHZ 查询的博弈的并行重复

本节旨在证明定理 1.1。根据引理 3.12，只需考虑 Q 是 $\mathrm{supp}(Q)$上的均匀分布这一情形。我们证明如下结论：

定理 6.1。 设 $\mathcal{G} = (\mathcal{X} \times \mathcal{Y} \times \mathcal{Z},\ \mathcal{A} \times \mathcal{B} \times \mathcal{C},\ Q, V_{pred})$ 是任意一个带有$\mathcal{X} = \mathcal{Y} = \mathcal{Z} = \mathbb{F}_2$的三人游戏，且 Q 是.....上的均匀分布

$$\mathrm{supp}(Q) = \left\{(x, y, z) \in \mathbb{F}_2^3 : x + y + z = 0\right\},$$

并且满足 $\mathrm{值}(\mathcal{G}) < 1$。那么，对于所有充分大的 n,[2] ，都有

$$\mathrm{val}(\mathcal{G}^{\otimes n}) \leq \exp\left(-n^c\right),$$

其中 $c > 0$ 是一个绝对常数。

本节余下部分将用于证明上述定理。为此，我们固定一个满足定理陈述条件的三人游戏 $\mathcal{G}$；特别地，必须有 $\mathrm{val}(\mathcal{G}) \leq 3/4$。

证明的主要步骤是证明， $\mathcal{G}^{\otimes n}$ 当玩家的输入以测度充分大的乘积事件为条件时，存在一个困难坐标。我们分两部分完成这一证明：首先，在第6.1节中，我们假设乘积事件中的三个集合在4.1子空间的定义中所述的意义下，在某个较大的 $\mathbb{F}_2^n$子空间中充分分散，并在此假设下证明该结论；然后，在第6.2节中，我们使用均匀化策略证明一般乘积事件的情形。

6.1 扩散乘积事件下的困难坐标

考虑博弈 $\mathcal{G}^{\otimes n} = (\mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n,\ \mathcal{A}^n \times \mathcal{B}^n \times \mathcal{C}^n,\ Q^{\otimes n},\ V_{pred}^{\otimes n})$，其中 $n \in \mathbb{N}$ 足够大。固定该博弈中 3 位玩家的任意策略，对于每个 $i \in [n]$，令 $\mathrm{Win}_i \subseteq \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$ 表示该策略赢得博弈第 i^{th} 个坐标的事件。

引理 6.2。 对于任意 $1 \leq d \leq o(n)$，以及常数 $\epsilon \in (0,\ 1/4)$，存在一个（足够大的）整数 $r = O_\epsilon(d^{16})$，以及一个（足够小的）常数 $0 < \delta = \delta(\epsilon) < 1$，使得以下结论成立：

设 $\mathcal{V} \subseteq \mathbb{F}_2^n$是一个维数为 $\dim(\mathcal{V}) \geq n - o(n)$ 的线性子空间，并设 E、F、$G \subseteq \mathcal{V}$满足：它们各自都在 $(r,\ \delta)$-代数扩散于 $\mathcal{V}$ （见定义 *4.1*），且各自的密度 $\frac{|E|}{|\mathcal{V}|}$、$\frac{|F|}{|\mathcal{V}|}$、$\frac{|G|}{|\mathcal{V}|} \geq 2^{-d}$。那么，

$$\mathop{\mathbb{E}}_{i \sim [n]} \left[\Pr_{Q^{\otimes n}} \left[\mathrm{Win}_i \mid E \times F \times G \right] \right] \leq \frac{1}{2} + \frac{\mathrm{val}(\mathcal{G})}{2} + \epsilon.$$

本小节余下部分将用于证明引理 6.2。我们固定某个 $1 \leq d \leq o(n)$，以及常数 $\epsilon \in (0, 1/4)$，并令 $r = O_\epsilon(d^{16})$ $\delta = \delta(\epsilon) > 0$ 使命题 5.6 在参数 $d, \frac{\epsilon}{2}$ 下成立。令 $\mathcal{V} \subseteq \mathbb{F}_2^n$ 为一个线性子空间，属于

维数 $\dim(\mathcal{V}) \geq n - o(n)$，并令 E，F，$G \subseteq \mathcal{V}$ 均在 $\mathcal{V}$ 内代数扩散，参数为 $(r,\ \delta)$，且每个密度 $\alpha_E = \frac{|E|}{|\mathcal{V}|}$，$\alpha_F = \frac{|F|}{|\mathcal{V}|}$，$\alpha_G = \frac{|G|}{|\mathcal{V}|}$ 均至少为 2^{-d}。

我们先证明一个引理，说明正方形的用途。该引理指出，对于博弈 $\mathcal{G}^{\otimes n}$，不存在能在正方形的非平凡坐标上获胜的策略。

定义 6.3 (非平凡坐标)。给定一个正方形 $s = s_{x,\ y,\ w} \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^n$，如定义 2.2所述，我们将其非平凡坐标集合定义为

$$\mathcal{I}_s = \{i \in [n] : w_i \neq 0\}.$$

这是良定义的，因为 w 由正方形 s 唯一确定（参见备注 2.3）。

引理 6.4。设 s 是一个正方形，且 $i \in \mathcal{I}_s$ 是 s 中的一个非平凡坐标。那么，

$$\Pr_{(x,y)\sim s}\left[(x, y, x+y) \in \mathrm{Win}_i\right] \leq \mathrm{val}(\mathcal{G}) < 1.$$

证明。设 x_0、y_0、$w \in \mathbb{F}_2^n$ 满足 $s = s_{x_0,\ y_0,\ w}$，且 $w_i \neq 0$。不妨假设 $(x_0)_i = 0$（必要时将 x_0 替换为 $x_0 + w$），同理也可假设 $(y_0)_i = 0$。定义这些点$x_1 = x_0 + w$、$y_1 = y_0 + w$、$z_0 = x_0 + y_0$、$z_1 = z_0 + w$。另外，定义

$$\begin{aligned}\tilde{s} &= \{(x, y, x+y) : (x, y) \in s\} \\ &= \{(x_0, y_0, z_0), (x_0, y_1, z_1), (x_1, y_0, z_1), (x_1, y_1, z_0)\} \\ &= \{(x_\alpha, y_\beta, z_\gamma) : (\alpha, \beta, \gamma) \in \mathrm{supp}(Q)\}\end{aligned}$$

注意，$\tilde{s} \subseteq \mathrm{supp}(Q)^n$ 以及 $\tilde{s}$ 中的所有点都是博弈 $\mathcal{G}^{\otimes n}$ 中玩家的有效输入。此外，对于每个 $(\alpha, \beta, \gamma) \in \mathrm{supp}(Q)$，这些输入满足 $(x_\alpha, y_\beta, z_\gamma)_i = (\alpha, \beta, \gamma)$。

注意，对于 $(x, y) \sim s$，$(x, y, x+y)$ 的分布就是 $\tilde{s}$ 中 4 个点上的均匀分布。因此，只需证明，对于 $\mathcal{G}^{\otimes n}$ 中的坐标，不存在策略 $f : \mathbb{F}_2^n \to \mathcal{A}$，$g : \mathbb{F}_2^n \to \mathcal{B}$，$h : \mathbb{F}_2^n \to \mathcal{C}$ 能在超过 $\mathrm{val}(\mathcal{G})$ 比例的点 $\tilde{s}$ 上获胜。为此，考虑任意这样的函数 f, g, h。利用这些函数，我们按如下方式为基础博弈 $\mathcal{G}$ 构造一种策略：

1. 验证者选择 $(\alpha, \beta, \gamma) \sim Q$，并分别将它们交给三位参与者。
2. 玩家 1 输出 $f(x_\alpha)$，玩家 2 输出 $g(y_\beta)$，玩家 3 输出 $h(z_\gamma)$。

对于任意输入 $(\alpha,\ \beta,\ \gamma) \in \mathrm{supp}(Q)$，如前所见，向量 $(x_\alpha,\ y_\beta,\ z_\gamma)$ 的 i^{th} 坐标 $\in \tilde{s}$ 等于 $(\alpha,\ \beta,\ \gamma)$。因此，上述策略赢得博弈$\mathcal{G}$的概率，等于集合 $\tilde{s}$ 中使 f，g，h 在 $\mathcal{G}^{\otimes n}$ 的 i^{th} 坐标上获胜的点所占比例。根据博弈值的定义，该比例至多为 $\mathrm{val}(\mathcal{G})$。 □

接下来，我们证明 E，F，$G \subseteq \mathcal{V}$ 的扩散性保证 $S = S(E,\ F,\ G)$（见定义 2.1）被正方形均匀覆盖。为此，令 $\mathcal{T}$ 表示包含于 S 的所有正方形构成的集合；形式化地说，

$$\mathcal{T} = \left\{(x, y, w) \in \mathcal{V}^3 : s_{x,y,w} \subseteq S\right\}.$$

令 U_S 表示 S 上的均匀分布。另外，令 μ 表示在 S 上按如下方式得到的分布：在 S 中随机选取一个正方形，即均匀随机选取 $(x,\ y,\ w) \sim \mathcal{T}$；然后，从集合 $s_{x,\ y,\ w}$ 中均匀随机输出一个元素。

引理 6.5。我们有

1. $\left|\frac{|S|}{|\mathcal{V}|^2} - \alpha_E\alpha_F\alpha_G\right| \le \frac{\epsilon}{2}\cdot\alpha_E\alpha_F\alpha_G$.
2. $\left|\frac{|\mathcal{T}|}{|\mathcal{V}|^3} - \alpha_E^2\alpha_F^2\alpha_G^2\right| \le \frac{\epsilon}{2}\cdot\alpha_E^2\alpha_F^2\alpha_G^2$.
3. $\|\mu - U_S\|_1 \le \frac{\epsilon}{2}$.

证明。这可直接由命题 5.6 得出，该命题是相对于 $\mathcal{V}\cong\mathbb{F}_2^{\dim(\mathcal{V})}$ 应用的。注意，正方形的定义是 坐标无关的，因此该命题适用。 □

在完成引理 6.2 的证明之前，我们先证明，在 $S=S(E,\ F,\ G)$ 中的随机方形包含许多非平凡坐标。

引理 6.6。令 $(x,y,w)\sim\mathcal{T}$，并令 $s=s_{x,\ y,\ w}$。那么，

$$\mathbb{E}\,|\mathcal{I}_s| \ge \frac{n}{2}\cdot(1-o(1)).$$

证明。对于任意 $0<\theta<1$，我们有

$$\begin{aligned}
\Pr\left[|\mathcal{I}_s| \le (1-\theta)\cdot\frac{n}{2}\right] &= \Pr_{(x,y,w)\sim\mathcal{T}}\left[|\{i : w_i\neq 0\}| \le (1-\theta)\cdot n/2\right] \\
&= \frac{1}{|\mathcal{T}|}\sum_{(x,y,w)\in\mathcal{T}} \mathbb{1}\left[|\{i : w_i\neq 0\}| \le (1-\theta)\cdot n/2\right] \\
&\le \frac{1}{|\mathcal{T}|}\sum_{x,y,w\in\mathbb{F}_2^n} \mathbb{1}\left[|\{i : w_i\neq 0\}| \le (1-\theta)\cdot n/2\right] \\
&= \frac{2^{3n}}{|\mathcal{T}|}\Pr_{w\sim\mathbb{F}_2^n}\left[|\{i : w_i\neq 0\}| \le (1-\theta)\cdot n/2\right].
\end{aligned}$$

根据事实 3.1，我们有，$\Pr_{w\sim\mathbb{F}_2^n}\left[|\{i:\ w_i\neq 0\}| \le (1-\theta)\cdot n/2\right] \le 2^{-\theta^2 n/4}$；根据引理 6.5，我们有

$$\frac{|\mathcal{T}|}{2^{3n}} \ge \frac{|\mathcal{V}|^3}{2^{3n}}\cdot(1-\epsilon/2)\cdot\alpha_E^2\alpha_F^2\alpha_G^2 \ge 2^{-3\cdot(n-\dim(\mathcal{V}))}\cdot\frac{1}{2}\cdot 2^{-6d} \ge 2^{-\kappa n},$$

对于某个 $\kappa=o(1)$。综合以上结果，我们得到

$$\Pr\left[|\mathcal{I}_s| \le (1-\theta)\cdot\frac{n}{2}\right] \le 2^{\kappa n}\cdot 2^{-\theta^2 n/4} = 2^{-(\theta^2-4\kappa)n/4}.$$

现在，我们选择 $\theta=\max\{3\sqrt{\kappa}, n^{-0.1}\}\le o(1)$，因此上述概率为 $o(1)$。于是，

$$\mathbb{E}\,|\mathcal{I}_s| \ge \frac{n}{2}\cdot(1-\theta)\cdot(1-o(1)) \ge \frac{n}{2}\cdot(1-o(1)).$$ □

最后，我们完成证明。

引理的证明 6.2。对于任意 $i \in [n]$，以及 $S = S(E,F,G)$，我们可以写成

$$\begin{aligned}\Pr_{Q^{\otimes n}}[\mathrm{Win}_i \mid E \times F \times G] &= \Pr_{x,y\sim\mathbb{F}_2^n}[(x,y,x+y) \in \mathrm{Win}_i \mid (x,y,x+y) \in E \times F \times G] \\ &= \Pr_{x,y\sim\mathbb{F}_2^n}[(x,y,x+y) \in \mathrm{Win}_i \mid (x,y) \in S] \\ &= \Pr_{(x,y)\sim S}[(x,y,x+y) \in \mathrm{Win}_i].\end{aligned}$$

根据引理 6.5，这可以界定为

$$\Pr_{Q^{\otimes n}}[\mathrm{Win}_i \mid E \times F \times G] \le \mathop{\mathbb{E}}_{(x_0,y_0,w)\sim\mathcal{T}} \mathop{\mathbb{E}}_{(x,y)\sim s_{x_0,y_0,w}} [\mathbb{1}[(x,y,x+y) \in \mathrm{Win}_i]] + \frac{\epsilon}{2}. \tag{3}$$

注意，对于固定的正方形 $(x_0,\ y_0,\ w) \in \mathcal{T}$，$s = s_{x_0,\ y_0,\ w}$，由引理 6.4，我们可以界定

$$\mathop{\mathbb{E}}_{(x,y)\sim s_{x_0,y_0,w}} [\mathbb{1}[(x,y,x+y) \in \mathrm{Win}_i]] \le 1 - (1-\mathrm{val}(\mathcal{G})) \cdot \mathbb{1}[i \in \mathcal{I}_s].$$

将此代入上式，并对 $i \sim [n]$ 取期望，我们得到

$$\begin{aligned}\mathop{\mathbb{E}}_{i\sim[n]}\left[\Pr_{Q^{\otimes n}}[\mathrm{Win}_i \mid E \times F \times G]\right] &\le \mathop{\mathbb{E}}_{i\sim[n]} \mathop{\mathbb{E}}_{(x_0,y_0,w)\sim\mathcal{T}} \left[1 - (1-\mathrm{val}(\mathcal{G})) \cdot \mathbb{1}\left[i \in \mathcal{I}_{s_{x_0,y_0,w}}\right]\right] + \frac{\epsilon}{2} \\ &= 1 - \frac{(1-\mathrm{val}(\mathcal{G}))}{n} \mathop{\mathbb{E}}_{(x_0,y_0,w)\sim\mathcal{T}} |\mathcal{I}_{s_{x_0,y_0,w}}| + \frac{\epsilon}{2}. \\ &\le 1 - (1-\mathrm{val}(\mathcal{G})) \cdot \frac{1}{2} \cdot (1-o(1)) + \frac{\epsilon}{2} \qquad \text{(by Lemma 6.6)} \\ &\le \frac{1}{2} + \frac{\mathrm{val}(\mathcal{G})}{2} + \frac{\epsilon}{2} + o(1) \le \frac{1}{2} + \frac{\mathrm{val}(\mathcal{G})}{2} + \epsilon. \qquad \square\end{aligned}$$

6.2 一般乘积事件下的困难坐标

现在，我们考虑一般乘积事件。考虑博弈 $\mathcal{G}^{\otimes n} = (\mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n,\ \mathcal{A}^n \times \mathcal{B}^n \times \mathcal{C}^n,\ Q^{\otimes n},\ V_{pred}^{\otimes n})$，其中 $n \in \mathbb{N}$ 足够大。固定该博弈中 3 位玩家的任意策略，对于每个 $i \in [n]$，令 $\mathsf{Win}_i \subseteq \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$ 表示该策略赢得博弈第 i^{th} 个坐标的事件。我们证明：

引理 6.7。 对于任意常数 $\epsilon \in (0, 1/4)$，存在一个常数 $c = c(\epsilon) > 0$，使得以下结论成立：对于任意集合 $E, F, G \subseteq \mathbb{F}_2^n$，若满足 $\Pr_{Q^{\otimes n}}[E \times F \times G] \ge 2^{-n^c}$，则有

$$\mathop{\mathbb{E}}_{i\sim[n]}\left[\Pr_{Q^{\otimes n}}[\mathrm{Win}_i \mid E \times F \times G]\right] \le \frac{1}{2} + \frac{\mathrm{val}(\mathcal{G})}{2} + \epsilon.$$

证明。设 $d = n^{1/20}$，并设 $r = O_\epsilon(d^{16}) \in \mathbb{N}$ 和常数 $0 < \delta = \delta(\epsilon) < 1/10$ 满足引理 6.2 的引理陈述，其中参数为 d、$\epsilon/2$。

设 $\eta = \epsilon/3$，并设 $C = C_\eta$ 为命题 4.3 中的常数。设 $d_0 = d^{1/C} = n^{1/(20C)}$，并设 E、F、$G \subseteq \mathbb{F}_2^n$ 使得 $\alpha = \Pr_{Q^{\otimes n}}[E \times F \times G] \ge 4 \cdot 2^{-d_0}$。注意到，对于 $c(\epsilon) = 1/(40C)$，引理陈述仍然成立。

令 $S = S(E,F,G)$ 如定义 2.1 所述；它满足 $|S| = 2^{2n}\alpha$。现在，根据命题 4.3（参数为 r、δ、η，空间为 $\mathbb{F}_2^n$），我们可找到一个整数 $T \in \mathbb{N}$，并且对每个 $t \in [T]$，找到一个线性子空间 $\mathcal{V}_t \subseteq \mathbb{F}_2^n$、点 e_t、$f_t \in \mathbb{F}_2^n$ 以及子集 $E_t \subseteq e_t + \mathcal{V}_t$、$F_t \subseteq f_t + \mathcal{V}_t$、$G_t \subseteq e_t + f_t + \mathcal{V}_t$，使得：

1. 对所有 $t \in [T]$，都有维数$(\mathcal{V}_t) \geq n - r\delta^{-3}\log_2(4/\alpha)^C = n - O(d^{17}) \geq n - o(n)$。

2. $S(E_1, F_1, G_1)$ ……，$S(E_T, F_T, G_T)$ 是 S 的互不相交子集，使得

$$\left|S \setminus \cup_{t=1}^{T} S(E_t, F_t, G_t)\right| \leq \eta |S| = \eta\alpha \cdot 2^{2n}.$$

3. 对所有 $t \in [T]$，我们有 $|E_t|$，$|F_t|$，$|G_t| \geq 2^{-\log_2(4/\alpha)^C} |\mathcal{V}_t| \geq 2^{-d} |\mathcal{V}_t|$，且 E_t，F_t，G_t 分别在 $e_t + \mathcal{V}_t$，$f_t + \mathcal{V}_t$，$e + f_t + \mathcal{V}_t$ 中是 (r, δ)-代数扩散的。

现在，对于任意 $i \in [n]$，我们可以写成

$$\begin{aligned}
\Pr_{Q^{\otimes n}}[\mathrm{Win}_i \mid E \times F \times G] &= \alpha^{-1} \cdot \Pr_{Q^{\otimes n}}[\mathrm{Win}_i \cap E \times F \times G] \\
&= \alpha^{-1} \cdot \Pr_{x,y \sim \mathbb{F}_2^n}[(x, y, x+y) \in \mathrm{Win}_i \cap (x, y) \in S(E, F, G)] \\
&\leq \eta + \sum_{t=1}^{T} \alpha^{-1} \cdot \Pr_{x,y \sim \mathbb{F}_2^n}[(x, y, x+y) \in \mathrm{Win}_i \cap (x, y) \in S(E_t, F_t, G_t)] \\
&= \eta + \sum_{t=1}^{T} \alpha^{-1} \cdot \Pr_{Q^{\otimes n}}[\mathrm{Win}_i \cap E_t \times F_t \times G_t] \\
&= \eta + \sum_{t=1}^{T} \alpha^{-1} \cdot \Pr_{Q^{\otimes n}}[\mathrm{Win}_i \mid E_t \times F_t \times G_t] \cdot \frac{|S(E_t, F_t, G_t)|}{2^{2n}}.
\end{aligned}$$

此外，根据引理 6.2，对每个 $t \in [T]$，都有

$$\mathop{\mathbb{E}}_{i \sim [n]}\left[\Pr_{Q^{\otimes n}}[\mathrm{Win}_i \mid E_t \times F_t \times G_t]\right] \leq \frac{1 + \mathrm{val}(\mathcal{G}) + \epsilon}{2}.$$

这里注意，当输入是在给定 $E_t \times F_t \times G_t$ 的条件下抽取时，三位参与者可以分别将其平移 e_t，f_t，$e_t + f_t \in \mathbb{F}_2^n$；此时，每位玩家的输入都落在线性子空间 $\mathcal{V}_t$ 的扩散子集中，因此引理适用。最后，结合上述两个方程，并回想 $\eta = \epsilon/3$，得到

$$\begin{aligned}
\mathop{\mathbb{E}}_{i \sim [n]}\left[\Pr_{Q^{\otimes n}}[\mathrm{Win}_i \mid E \times F \times G]\right] &\leq \eta + \sum_{t=1}^{T} \alpha^{-1} \cdot \mathop{\mathbb{E}}_{i \sim [n]}\left[\Pr_{Q^{\otimes n}}[\mathrm{Win}_i \mid E_t \times F_t \times G_t]\right] \cdot \frac{|S(E_t, F_t, G_t)|}{2^{2n}} \\
&\leq \eta + \sum_{t=1}^{T} \alpha^{-1} \cdot \left(\frac{1 + \mathrm{val}(\mathcal{G}) + \epsilon}{2}\right) \cdot \frac{|S(E_t, F_t, G_t)|}{2^{2n}} \\
&= \eta + \alpha^{-1} \cdot \left(\frac{1 + \mathrm{val}(\mathcal{G}) + \epsilon}{2}\right) \cdot \frac{\sum_{t=1}^{T} |S(E_t, F_t, G_t)|}{2^{2n}} \\
&\leq \eta + \alpha^{-1} \cdot \left(\frac{1 + \mathrm{val}(\mathcal{G}) + \epsilon}{2}\right) \cdot \frac{|S|}{2^{2n}} = \eta + \frac{1 + \mathrm{val}(\mathcal{G}) + \epsilon}{2} \\
&\leq \frac{1}{2} + \frac{\mathrm{val}(\mathcal{G})}{2} + \epsilon.
\end{aligned}$$

□

有了上述结果，我们主定理的证明便显而易见：

定理 *6.1*的证明。 将引理 3.13 与引理 6.7结合起来，并采用参数取值 $\epsilon = 0.1$，回顾一下 $\mathrm{val}(\mathcal{G}) \leq 3/4$。 □

定理证明 *1.1*。 该定理由定理6.1和引理3.12。 □

7 一个集中界

我们还证明了 GHZ 游戏的集中界：

定理 7.1. 设 $\mathcal{G} = (\mathcal{X} \times \mathcal{Y} \times \mathcal{Z},\ \mathcal{A} \times \mathcal{B} \times \mathcal{C},\ Q, V_{pred})$ 为任意一个三人游戏，具有 $\mathcal{X} = \mathcal{Y} = \mathcal{Z} = \mathbb{F}_2$，且 Q 为均匀分布，定义在

$$\mathrm{supp}(Q) = \left\{(x, y, z) \in \mathbb{F}_2^3 : x + y + z = 0\right\},$$

并且使得 值$(\mathcal{G})$ < 1。那么，对于每个常数 $\epsilon \in (0, 1/4)$，都存在一个常数$c = c(\epsilon) > 0$，使得对于所有充分大的 n，以下结论成立：[3]

考虑博弈 $\mathcal{G}^{\otimes n}$，并考虑该博弈中 *3* 名玩家的任意策略。那么，如果 Z 表示玩家获胜的坐标数量，则有

$$\Pr\left[Z \geq (\mathrm{val}(\mathcal{G}) + \epsilon) \cdot n\right] \leq \exp\left(-n^c\right).$$

本节余下部分将用于证明上述定理。为此，我们固定一个满足定理陈述的博弈 $\mathcal{G}$ 。考虑博弈 $\mathcal{G}^{\otimes n}$ =$(\mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n,\ \mathcal{A}^n \times \mathcal{B}^n \times \mathcal{C}^n,\ Q^{\otimes n},\ V_{pred}^{\otimes n})$，其中 $n \in \mathbb{N}$ 足够大。此外，固定此博弈中 3 位玩家的任意策略，并对每个 $i \in [n]$，令 $\mathsf{Win}_i \subseteq \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$ 表示该策略赢得博弈中 i^{th} 个坐标的事件。对每个 $S \subseteq [n]$，我们用 Win_S 表示事件 $\wedge_{i \in S} \mathsf{Win}_i$。

7.1 乘积事件的改进后的界

我们证明的第一步是证明引理 6.7 的一个改进版本，其中不会损失一个“2 倍因子”。我们证明如下结果：

引理 7.2。 对于任意常数 $\epsilon \in (0,\ 1/4)$，存在 $c = c(\epsilon) > 0$，使得以下结论成立：对于任意集合 E、F、$G \subseteq \mathbb{F}_2^n$，若 $\Pr_{Q^{\otimes n}}[E \times F \times G] \geq 2^{-n^c}$，则有

$$\mathop{\mathbb{E}}_{i \sim [n]} \left[\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_i \mid E \times F \times G\right]\right] \leq \mathrm{val}(\mathcal{G}) + \epsilon.$$

上述引理的证明完全沿用第6节中的证明，因此我们只说明如何改进。我们注意到，界中唯一损失因子 2 的地方是在引理 6.2的证明中；如果证明了引理 6.2的改进版本，那么利用均匀化的引理 6.7的证明便可照常成立。现在，在引理 6.2中，我们以完全相同的方式推导，直到公式 (3)，该公式表示（对 $i \sim [n]$取期望后）

$$\mathop{\mathbb{E}}_{i \sim [n]} \left[\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_i \mid E \times F \times G\right]\right] \leq \mathop{\mathbb{E}}_{i \sim [n]} \mathop{\mathbb{E}}_{(x_0, y_0, w) \sim \mathcal{T}} \mathop{\mathbb{E}}_{(x,y) \sim s_{x_0, y_0, w}} \left[\mathbb{1}\left[(x, y, x + y) \in \mathrm{Win}_i\right]\right] + \frac{\epsilon}{2}.$$

现在出现因子 2 损失，是因为当 $(x_0, y_0, w) \sim \mathcal{T}$时，事件 $w_i = 1$ 发生的概率约为 1/2（见引理 6.6），而只有在该事件发生时，我们才能应用引理 6.4 。为了改进这个界，我们将用一个已经对事件 $w_i = 1$进行条件化的分布来替代原分布，然后再应用引理 6.4；这需要证明引理 6.6的一个更强版本，即上述陈述中的 (x, y) 的分布，即使在以 $w_i = 1$为条件对正方形进行采样时，也保持不变。形式化地，我们证明：

引理 7.3。 回忆一下，在 S 上按如下方式得到的分布 μ：选择 $(x_0, y_0, w) \sim \mathcal{T}$，并令 $(x, y) \sim s_{x_0, y_0, w}$。对于任意 $i \in [n]$，按如下方式定义分布 ν_i：在给定 $w_i = 1$的条件下选择$(x_0, y_0, w) \sim \mathcal{T}$，并令 $(x, y) \sim s_{x_0, y_0, w}$。那么，我们有

$$\mathop{\mathbb{E}}_{i \sim [n]} \|\mu - \nu_i\|_1 \leq o(1).$$

证明中，我们需要以下技术性引理，其证明推迟到附录 A。

引理 7.4。 设 $\mathcal{T} \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2^n$是任意一个大小至少为 $2^{3n - o(n)}$的集合。令$(X, Y, W) \sim \mathcal{T}$为均匀随机选取。则，

$$\mathop{\mathbb{E}}_{i \sim [n]} \left\| P_{X,Y|W_i=1} - P_{X,Y} \right\|_1 \leq o(1).$$

这里，$P_{X,\ Y}$表示(X, Y)的边缘分布，而 $P_{X,\ Y|W_i=1}$ 表示在事件 $W_i = 1$的条件下(X, Y) 的边缘分布。

引理 7.3 的证明。首先，注意到分布 μ 与以下分布相同：选取 $(x_0, y_0, w) \sim \mathcal{T}$，并输出 (x_0, y_0)。这可由公式 (2) 得出：本质上，这是由注记 2.3 推出的，因为在 $\mathcal{T}$ 中，每个带有 $w \neq 0$ 的正方形都会出现 4 次，而选定正方形后，该正方形中的每个点被选中的概率为 $1/4$；此外，每个带有 $w = 0$ 的正方形只出现一次，但选定这样的正方形后，其中的点以概率 1 被选中。类似地，对于每个 $i \in [n]$，分布 ν_i 与以下分布相同：选取 $(x_0, y_0, w) \sim \mathcal{T} \mid w_i = 1$，并输出 (x_0, y_0)。

现在，注意到根据引理 6.5，我们有

$$|\mathcal{T}| \geq |\mathcal{V}|^3 \cdot (1 - \epsilon/2) \cdot \alpha_E^2 \alpha_F^2 \alpha_G^2 \geq 2^{3n - (3(n - \dim(\mathcal{V})) + 1 + 6d)} \geq 2^{3n - o(n)}.$$

由引理 7.4，即可得到该结果。 □

最后，我们完成改进后的界的证明：

引理 7.2 的证明。 如前所述，只需改进引理6.2，并且我们有

$$\mathop{\mathbb{E}}_{i \sim [n]} \left[\Pr_{Q^{\otimes n}} [\mathrm{Win}_i \mid E \times F \times G] \right] \leq \mathop{\mathbb{E}}_{i \sim [n]} \mathop{\mathbb{E}}_{(x_0, y_0, w) \sim \mathcal{T}} \mathop{\mathbb{E}}_{(x, y) \sim s_{x_0, y_0, w}} [\mathbb{1}[(x, y, x + y) \in \mathrm{Win}_i]] + \frac{\epsilon}{2}.$$

根据引理 7.3 和引理 6.4，上述值至多为

$$\begin{aligned} \mathop{\mathbb{E}}_{i \sim [n]} \mathop{\mathbb{E}}_{(x_0, y_0, w) \sim \mathcal{T} | w_i = 1} \mathop{\mathbb{E}}_{(x, y) \sim s_{x_0, y_0, w}} [\mathbb{1}[(x, y, x + y) \in \mathrm{Win}_i]] + \frac{\epsilon}{2} + o(1) &\leq \mathrm{val}(\mathcal{G}) + \frac{\epsilon}{2} + o(1) \\ &\leq \mathrm{val}(\mathcal{G}) + \epsilon. \end{aligned}$$

□

7.2 并行重复下随机集合是困难的

我们通过采用与引理 3.13的证明类似的论证，证明定理 6.1的一个加强版本。

引理 7.5。 对于每个常数 $\epsilon \in (0, 1/4)$，都存在 $c = c(\epsilon) > 0$，使得对于每个整数 $1 \le t \le n^c$，均有

$$\mathop{\mathbb{E}}_{|S|=t}\left[\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_S\right]\right] \le 2 \cdot (\mathrm{val}(\mathcal{G}) + \epsilon)^t,$$

其中 $\mathbb{E}_{|S|=t}$ 表示 期望取自大小为 t 的均匀选取子集 $S \subseteq [n]$.

证明。 令 $\epsilon \in (0, 1/4)$ 为任意常数，并令 $0 < c \le 1$ 如引理 7.2 中关于参数 $\epsilon/2$的定义。我们证明该引理对常数 $c/2$成立。

更正式地说，通过对 t 使用归纳法，我们证明对于每个 $1 \le t \le \lfloor n^{c/2} \rfloor$,

$$\mathop{\mathbb{E}}_{|S|=t}\left[\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_S\right]\right] \le (\mathrm{val}(\mathcal{G}) + \epsilon)^t + t \cdot 2^{-n^c/2} \le 2 \cdot (\mathrm{val}(\mathcal{G}) + \epsilon)^t.$$

注意，第二个不等式成立，因为我们可以假设 $\mathrm{val}(\mathcal{G}) \ge 1/4$ （否则 $\mathrm{val}(\mathcal{G}) = 0$，此时无需证明），在这种情况下， $t \cdot 2^{-n^c/2} \le (1/4)^{n^{c/2}} \le (1/4)^t \le (\mathrm{val}(\mathcal{G}) + \epsilon)^t$。

基本情形 $t = 1$ 显然成立，因为对于每个 $i \in [n]$, $\Pr_{Q^{\otimes n}}[\mathrm{Win}_i] \le \mathrm{val}(\mathcal{G})$。对于归纳步骤，任取 $1 \le t < \lfloor n^{c/2} \rfloor$，并假设 $\mathbb{E}_{|T|=t}\left[\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_T\right]\right] \le (\mathrm{val}(\mathcal{G}) + \epsilon)^t + t \cdot 2^{-n^c/2}$。于是，我们有

$$\begin{aligned}
\mathop{\mathbb{E}}_{|S|=t+1}\left[\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_S\right]\right] &= \mathop{\mathbb{E}}_{|T|=t}\mathop{\mathbb{E}}_{i\sim[n]\setminus T}\left[\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_T \wedge \mathrm{Win}_i\right]\right] \\
&= \mathop{\mathbb{E}}_{|T|=t}\left[\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_T\right] \cdot \mathop{\mathbb{E}}_{i\sim[n]\setminus T}\left[\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_i \mid \mathrm{Win}_T\right]\right]\right].
\end{aligned}$$

考虑到上述表达式，我们固定任意一个大小为 t 的集合 $T \subseteq [n]$ ，并计算 $\mathbb{E}_{i\sim[n]\setminus T}[\Pr[\mathrm{Win}_i \mid \mathrm{Win}_T]]$ 的上界。令 $R \in (\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \times \mathcal{A} \times \mathcal{B} \times \mathcal{C})^T$ 为随机变量，它由集合 T 所给坐标上的玩家的问题与答案构成；注意，该随机变量至多取 $(8|\mathcal{A}||\mathcal{B}||\mathcal{C}|)^t \le 2^{O(t)}$ 个可能值。此外，注意事件 Win_T 是 R 的确定性函数。令 $\mathcal{R}$ 为随机变量 R 所有满足事件 Win_T 的取值 r 构成的集合，并令 $\mathcal{R}' \subseteq \mathcal{R}$ 为所有满足 $\Pr_{Q^{\otimes n}}[R = r] \ge 2^{-n^c}$ 的 $r \in \mathcal{R}$ 构成的集合。注意，根据引理 7.2，对于每个 $r \in \mathcal{R}'$,

$$\mathop{\mathbb{E}}_{i\sim[n]}\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_i \mid R = r\right] \le \mathrm{val}(\mathcal{G}) + \frac{\epsilon}{2},$$

因为事件 $R = r$ 是相对于三位参与者的乘积事件。

因此，我们得到

$$\begin{aligned}
\mathop{\mathbb{E}}_{i\sim[n]\setminus T}\left[\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_i \mid \mathrm{Win}_T\right]\right] &\le \mathop{\mathbb{E}}_{i\sim[n]}\left[\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_i \mid \mathrm{Win}_T\right]\right] + \frac{2t}{n} \qquad \text{(Lemma 3.2)} \\
&= \sum_{r\in\mathcal{R}} \frac{\mathbb{E}_{i\sim[n]}\left[\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_i \mid R=r\right]\right]\cdot \Pr_{Q^{\otimes n}}[R=r]}{\Pr_{Q^{\otimes n}}[\mathrm{Win}_T]} + o(1) \\
&\le \sum_{r\in\mathcal{R}'} \left(\mathrm{val}(\mathcal{G}) + \frac{\epsilon}{2}\right)\cdot \frac{\Pr_{Q^{\otimes n}}[R=r]}{\Pr_{Q^{\otimes n}}[\mathrm{Win}_T]} + \sum_{r\in\mathcal{R}\setminus\mathcal{R}'} \frac{1\cdot 2^{-n^c}}{\Pr_{Q^{\otimes n}}[\mathrm{Win}_T]} + o(1) \\
&\le \left(\mathrm{val}(\mathcal{G}) + \frac{\epsilon}{2}\right) + \frac{(8|\mathcal{A}||\mathcal{B}||\mathcal{C}|)^t\cdot 2^{-n^c}}{\Pr_{Q^{\otimes n}}[\mathrm{Win}_T]} + o(1) \\
&\le \mathrm{val}(\mathcal{G}) + \epsilon + \frac{2^{O(n^{c/2})-n^c}}{\Pr_{Q^{\otimes n}}[\mathrm{Win}_T]} \le \mathrm{val}(\mathcal{G}) + \epsilon + \frac{2^{-n^c/2}}{\Pr_{Q^{\otimes n}}[\mathrm{Win}_T]}.
\end{aligned}$$

C结合以上结果，并使用归纳假设，我们得到

$$\begin{aligned}
\mathop{\mathbb{E}}_{|S|=t+1}\left[\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_S\right]\right] &= \mathop{\mathbb{E}}_{|T|=t}\left[\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_T\right]\cdot\left(\mathrm{val}(\mathcal{G}) + \epsilon + \frac{2^{-n^c/2}}{\Pr_{Q^{\otimes n}}[\mathrm{Win}_T]}\right)\right]. \\
&\le \mathop{\mathbb{E}}_{|T|=t}\left[\Pr_{Q^{\otimes n}}\left[\mathrm{Win}_T\right]\right]\cdot(\mathrm{val}(\mathcal{G}) + \epsilon) + 2^{-n^c/2}. \\
&\le \left((\mathrm{val}(\mathcal{G}) + \epsilon)^t + t\cdot 2^{-n^c/2}\right)\cdot(\mathrm{val}(\mathcal{G}) + \epsilon) + 2^{-n^c/2} \\
&\le (\mathrm{val}(\mathcal{G}) + \epsilon)^{t+1} + (t+1)\cdot 2^{-n^c/2}. \qquad \square
\end{aligned}$$

7.3 集中界的证明

最后，我们使用标准论证完成集中界的证明 [Rao11]:

定理的证明 *7.1*。 取任意常数 $\epsilon\in(0,1/4)$，令 $0<c<1$ 如引理 7.5中所述，参数为 $\epsilon/2$，并令 $t=\lfloor n^c\rfloor$。

令 Z 为一个随机变量，表示玩家赢得的坐标数。每当 $Z\ge(\mathrm{val}(\mathcal{G})+\epsilon)\cdot n$ 时，我们从玩家赢得的坐标中选取一个大小为 t 的均匀随机子集 S。注意，对于任意固定的大小为 t 的子集 $T\subseteq[n]$，S 等于 T 的概率至多为 $\binom{(\mathrm{val}(\mathcal{G})+\epsilon)\cdot n}{t}^{-1}$。因此，我们有

$$\begin{aligned}
\Pr\left[Z\ge(\mathrm{val}(\mathcal{G})+\epsilon)\cdot n\right] &\le \sum_{T\subseteq[n],|T|=t}\Pr[S=T]\cdot\Pr[\mathrm{Win}_T] \\
&\le \sum_{T\subseteq[n],|T|=t}\binom{(\mathrm{val}(\mathcal{G})+\epsilon)\cdot n}{t}^{-1}\cdot\Pr[\mathrm{Win}_T].
\end{aligned}$$

现在，利用引理 7.5，我们得到

$$\begin{aligned}
\Pr\left[Z \geq (\mathrm{val}(\mathcal{G})+\epsilon)\cdot n\right] &\leq \binom{n}{t}\cdot\binom{(\mathrm{val}(\mathcal{G})+\epsilon)\cdot n}{t}^{-1}\cdot 2\cdot(\mathrm{val}(\mathcal{G})+\epsilon/2)^t \\
&\leq \left(\frac{n}{(\mathrm{val}(\mathcal{G})+\epsilon)\cdot n - t}\right)^t \cdot 2\cdot(\mathrm{val}(\mathcal{G})+\epsilon/2)^t \\
&\leq 2\cdot\left(\frac{\mathrm{val}(\mathcal{G})+\epsilon/2}{\mathrm{val}(\mathcal{G})+\epsilon-o(1)}\right)^t \\
&= 2\cdot\left(1-\frac{\epsilon/2-o(1)}{\mathrm{val}(\mathcal{G})+\epsilon-o(1)}\right)^t \leq 2\cdot(1-\epsilon/4)^t \\
&\leq 2^{1-\epsilon t/4} \leq 2^{-n^{c/2}}. \qquad \square
\end{aligned}$$

参考文献

[ABSS97] Sanjeev Arora、László Babai、Jacques Stern 和 Z. Sweedyk。格、码和线性方程组中近似最优解的困难性。《J. Comput. System Sci.》，54(2, part 2):317–331，1997。（亦发表于 FOCS 1993）。3[AK09] Noga Alon 和 Bo'az Klartag。通过 Cheeger 不等式构造经济的环面脊。《J. Topol. Anal.》，1(2):101–111，2009。3[ALM+98] Sanjeev Arora、Carsten Lund、Rajeev Motwani、Madhu Sudan 和 Mario Szegedy。证明验证与近似问题的困难性。《ACM学报》，45(3):501–555，1998。3[AS98] Sanjeev Arora 和 Shmuel Safra。证明的概率检验：NP 的一种新刻画。《ACM学报》，45(1):70–122，1998。3[BBCR13] Boaz Barak、Mark Braverman、Xi Chen 和 Anup Rao。如何压缩交互式通信。SIAM J. Comput.，42(3):1327–1363，2013。（亦发表于 STOC 2010）。3[BBK+24] Amey Bhangale、Mark Braverman、Subhash Khot、Yang P. Liu 和 Dor Minzer。 k玩家投影游戏的并行重复。载于 APPROX-RANDOM，第 54 号文章，16 页，2024。3，5[BBK+25] Amey Bhangale、Mark Braverman、Subhash Khot、Yang Liu 和 Dor Minzer。三方 XOR 游戏的并行重复。载于 STOC，第 104–110 页，2025。3，4[BBK+26] Amey Bhangale、Mark Braverman、Subhash Khot、Yang P. Liu、Dor Minzer 和 Kunal Mittal。通过 CSP 逆定理研究平行重复的解析方法。载于 STOC，2026。（即将发表）。3，11

[BBLV13] Jop Briët、Harry Buhrman、Troy Lee 和 Thomas Vidick。XOR 博弈中的多方纠缠。Quantum Inf. Comput., 13(3-4):334–360, 2013。3[BG15] Mark Braverman 和 Ankit Garg。一般博弈的小值并行重复。载于 STOC，第 335–340 页，2015。3[BGS98] Mihir Bellare、Oded Goldreich 和 Madhu Sudan。自由比特、PCP 与不可近似性——迈向紧确结果。SIAM J. Comput., 27(3):804–915, 1998。（亦见 FOCS 1995）。3[BKM23] Mark Braverman、Subhash Khot 和 Dor Minzer。GHZ 游戏的并行重复：指数衰减。载于 FOCS，第 1337–1341 页，2023。3, 4, 5[BM21] Mark Braverman 和 Dor Minzer。利用置换对称体对欧几里得空间进行最优铺砌。载于 CCC，第 5 号文章，48 页，2021。3[BOGKW88] Michael Ben-Or、Shafi Goldwasser、Joe Kilian 和 Avi Wigderson。多证明者交互式证明：如何去除难解性假设。载于 STOC，第 113–131 页，1988。3[BRR+09] Boaz Barak、Anup Rao、Ran Raz、Ricky Rosen 和 Ronen Shaltiel。自由投影博弈的强并行重复定理。载于 APPROX-RANDOM，第 352–365 页，2009。3[BRWY13] Mark Braverman、Anup Rao、Omri Weinstein 和 Amir Yehudayoff。通信复杂度中的直积。载于 FOCS，第 746–755 页，2013。3[CHTW04] Richard Cleve、Peter Høyer、Benjamin Toner 和 John Watrous。非局域策略的后果与局限。载于 CCC，第 236–249 页，2004。3[CT06] Thomas M. Cover 和 Joy A. Thomas。信息论基础。Wiley-Interscience，第二版，2006。38[DGKR05] Irit Dinur、Venkatesan Guruswami、Subhash Khot 和 Oded Regev。一种新的多层 PCP 与超图顶点覆盖的困难性。SIAM J. Comput., 34(5):1129–1146, 2005。（亦见 STOC 2003）。3[DHVY17] Irit Dinur、Prahladh Harsha、Rakesh Venkat 和 Henry Yuen。扩张博弈的多人平行重复。载于 ITCS，第 37 号文章，16 页，2017。3, 4[DRS05] Irit Dinur、Oded Regev 和 Clifford Smyth。3-一致超图着色的困难性。Combinatorica, 25(5):519–535, 2005。3[DS14] Irit Dinur 和 David Steurer。平行重复的解析方法。载于 STOC，第 624–633 页，2014。3

[Fei91] Uriel Feige。单轮证明系统中两个证明者的成功概率。载于复杂性理论结构会议，第 116–123 页，1991。3[Fei98] Uriel Feige。用于近似集合覆盖的 $\ln n$ 阈值。《ACM学报》, 45(4):634–652, 1998。（亦见 STOC 1996）。3[FGL+96] Uriel Feige、Shafi Goldwasser、Laszlo Lovász、Shmuel Safra 和 Mario Szegedy。交互式证明与团近似的困难性。《ACM学报》, 43(2):268–292, 1996。3[FHHK24] Yuval Filmus、Hamed Hatami、Kaave Hosseini 和 Esty Kelman。二元系统中的稀疏图计数与 Kelley-Meka界。载于 FOCS，第 1559–1578 页，2024。8, 20[FK91] H. Furstenberg 和 Y. Katznelson。Hales-Jewett定理的密度版本。《分析数学杂志》, 57:64–119, 1991。3[FKO07] Uriel Feige、Guy Kindler 和 Ryan O'Donnell。理解平行重复需要理解泡沫。载于 CCC，第 179–192 页，2007。3[For89] Lance Fortnow。交互式证明系统的复杂性理论方面。博士论文，麻省理工学院，1989。3[FRS94] Lance Fortnow、John Rompel 和 Michael Sipser。关于多证明者交互协议的能力。Theoret. Comput. Sci., 134(2):545–557, 1994。3[FV02] Uriel Feige 和 Oleg Verbitsky。通过并行重复进行错误缩减——一项否定性结果。Combinatorica, 22(4):461–478, 2002。3, 4, 11[GHM+21] Uma Girish、Justin Holmgren、Kunal Mittal、Ran Raz 和 Wei Zhan。GHZ 游戏的并行重复：一个更简单的证明。载于 APPROX-RANDOM，第 62:1–62:19 页，2021。3, 4, 7, 8[GHM+22] Uma Girish、Justin Holmgren、Kunal Mittal、Ran Raz 和 Wei Zhan。二元字母表上的所有三人游戏的并行重复。载于 STOC，第 998–1009 页，2022。3, 11[GHS02] Venkatesan Guruswami、Johan Håstad 和 Madhu Sudan。超图近似着色的困难性。SIAM J. Comput., 31(6):1663–1686, 2002。（亦见 FOCS 2000）。3[GHZ89] Daniel M. Greenberger、Michael A. Horne 和 Anton Zeilinger。超越贝尔定理。载于《贝尔定理、量子理论与宇宙观》，第 69–72 页。施普林格荷兰，1989。4[GMRZ22] Uma Girish、Kunal Mittal、Ran Raz 和 Wei Zhan。二元输入下所有三人游戏的并行重复多项式界。载于 APPROX-RANDOM，第 6:1–6:17 页，2022。3

[Hås01] Johan Håstad。一些最优不可近似性结果。《ACM学报》，48(4):798–859，2001。（亦发表于 STOC 1997）。3[HHR16] Jan Hązła、Thomas Holenstein 和 Anup Rao。并行重复与密度 Hales-Jewett 定理的禁子图界。CoRR，abs/1604.05757，2016。见 http://arxiv.org/abs/1604.05757。4[Hol09] Thomas Holenstein。并行重复：简化与无信号情形。《计算理论》，5:141–172，2009。（亦发表于 STOC 2007）。3[HR20] Justin Holmgren 和 Ran Raz。GHZ 游戏的并行重复定理。CoRR，abs/2008.05059，2020。见 https://arxiv.org/abs/ 2008.05059。3，4[JLL+25] Michael Jaber、Yang P. Liu、Shachar Lovett、Anthony Ostuni 和 Mehtaab Sawhney。角定理的拟多项式界。载于计算机科学基础研讨会，2025。4，8，12，14[Kho02a] Subhash Khot。近似超图着色的困难性结果。载于 STOC，第351–359页，2002。3[Kho02b] Subhash Khot。为可3着色的3一致超图着色的困难性结果。载于计算机科学基础研讨会，第23–32页，2002。3[KLM24] Zander Kelley、Shachar Lovett 和 Raghu Meka。随机与确定性额头数字通信之间的显式分离。载于 STOC，第1299–1310页，2024。4，19[KM23] Zander Kelley 和 Raghu Meka。3 项等差数列的强界。载于计算机科学基础研讨会，第933–973页，2023。4，8，12[KORW08] Guy Kindler、Ryan O’Donnell、Anup Rao 和 Avi Wigderson。高维球面立方体与舍入。载于计算机科学基础研讨会，第189–198页，2008。3[Mit25] Kunal Mittal。多人平行重复与高维极值组合学等价，2025。见 https://arxiv.org/abs/2510.24910。4，7[MR21] Kunal Mittal 和 Ran Raz。块刚性：强多人平行重复蕴含图灵机的超线性下界。载于 ITCS，第71号文章，15页，2021。3[MU05] Michael Mitzenmacher 和 Eli Upfal。概率与计算。剑桥大学出版社，剑桥，2005。随机化算法与概率分析。9[Pol12] D. H. J. Polymath。密度 Hales-Jewett 定理的新证明。《数学年刊》（第2辑），175(3):1283–1327，2012。3

[PRW97] Itzhak Parnafes、Ran Raz 和 Avi Wigderson。直接乘积结果与最大公约数问题：新旧通信模型中的研究。载于 STOC，第363–372页，1997。3[Rao11] Anup Rao。投影游戏中的并行重复与一个集中界。SIAM J. Comput.，40(6):1871–1891，2011。（亦发表于 STOC 2008）。3，33[Raz98] Ran Raz。一个并行重复定理。SIAM J. Comput.，27(3):763–803，1998。（亦发表于 STOC 1995）。3，4，6，11[Raz10] Ran Raz。双验证者游戏的并行重复。载于 CCC，第3–6页，2010。3[Raz11] Ran Raz。强并行重复的一个反例。SIAM J. Comput.，40(3):771–777，2011。（亦发表于计算机科学基础研讨会 2008）。3[RR12] Ran Raz 和 Ricky Rosen。扩张图上投影游戏的强并行重复定理。载于 CCC，第247–257页，2012。3[ŠB20] Ivan Šupić 和 Joseph Bowles。量子系统的自检：综述。Quantum，4:337，2020。4[Ver96] Oleg Verbitsky。迈向并行重复猜想。Theoret. Comput. Sci.，157(2):277–282，1996。3

条件分布的边缘分布

本节将证明引理 7.4。证明中会用到一些基础的信息论知识，读者可参阅 [CT06] ，其中对信息论有出色的介绍。回顾一下，对于一个取值于有限集 X 上的随机变量 Ω，其熵定义为

$$H(X) = -\sum_{x\in\Omega} \Pr[X = x] \cdot \log_2(\Pr[X = x]).$$

我们有以下简单事实：

引理 A.1. 设 $X \in \{0,1\}$ 是一个二值随机变量。那么，

$$\left|\Pr[X = 1] - \frac{1}{2}\right|^2 \le 1 - H(X).$$

证明。设 $\delta = \left|\Pr[X = 1] - \frac{1}{2}\right|$。引理陈述等价于以下不等式

$$\delta^2 \le 1 - H(X) = 1 + \left(\frac{1}{2}+\delta\right)\log_2\left(\frac{1}{2}+\delta\right) + \left(\frac{1}{2}-\delta\right)\log_2\left(\frac{1}{2}-\delta\right),$$

对所有 $\delta \in [0, 1/2]$ 均成立。 □

接下来，我们证明本节的主要引理：

引理 7.4 的证明。假设 $|\mathcal{T}| \geq 2^{(3-\delta)n}$ 存在某个 $\delta = o(1)$。那么，我们有

$$(3-\delta)n \leq H(X,Y,W) = H(X,Y) + H(W \mid X,Y) \leq 2n + \sum_{i=1}^{n} H(W_i \mid X,Y),$$

这意味着

$$\mathop{\mathbb{E}}_{i\sim[n]}\left[H(W_i \mid X,Y)\right] \geq 1-\delta.$$

定义集合

$$\mathcal{G} = \left\{ i \in [n] : H(W_i|X,Y) \geq 1-\sqrt{\delta} \right\}.$$

那么，由马尔可夫不等式可得 $\mathbf{Pr}_{i\sim[n]}\left[i \notin \mathcal{G}\right] \leq \sqrt{\delta}$。

现在，考虑任意一个 $i \in \mathcal{G}$。由柯西-施瓦茨不等式和引理A.1，可得

$$\begin{aligned}
\left(\mathop{\mathbb{E}}_{(x,y)\sim P_{X,Y}} \left| \Pr\left[W_i = 1 | X = x, Y = y\right] - \frac{1}{2} \right| \right)^2 &\leq \mathop{\mathbb{E}}_{(x,y)\sim P_{X,Y}} \left| \Pr\left[W_i = 1 | x, y\right] - \frac{1}{2} \right|^2 \\
&\leq \mathop{\mathbb{E}}_{(x,y)\sim P_{X,Y}} \left[1 - H(W_i|x,y)\right] \\
&= 1 - H(W_i|X,Y) \leq \sqrt{\delta}.
\end{aligned}$$

因此，由三角不等式可得

$$\left| \Pr\left[W_i = 1\right] - \frac{1}{2} \right| \leq \mathop{\mathbb{E}}_{(x,y)\sim P_{X,Y}} \left| \Pr\left[W_i = 1 | x, y\right] - \frac{1}{2} \right| \leq \delta^{1/4}.$$

由上述结果可得

$$\begin{aligned}
\left\| P_{X,Y|W_i=1} - P_{X,Y} \right\|_1 &= \sum_{x,y} \left| \Pr[x,y|W_i=1] - \Pr[x,y] \right| \\
&= \mathop{\mathbb{E}}_{(x,y)\sim P_{X,Y}} \left| \frac{\Pr[W_i=1|x,y]}{\Pr[W_i=1]} - 1 \right| \\
&\leq \mathop{\mathbb{E}}_{(x,y)\sim P_{X,Y}} \left| \frac{\Pr[W_i=1|x,y]}{1/2} - 1 \right| \\
&\quad + \mathop{\mathbb{E}}_{(x,y)\sim P_{X,Y}} \left[\Pr[W_i=1|x,y]\right] \cdot \left| \frac{1}{\Pr[W_i=1]} - \frac{1}{1/2} \right| \\
&\leq 2 \cdot \delta^{1/4} + \Pr[W_i=1] \cdot \frac{\delta^{1/4}}{\Pr[W_i=1] \cdot 1/2} \\
&\leq 4\delta^{1/4}.
\end{aligned}$$

因此，

$$\mathop{\mathbb{E}}_{i\sim[n]} \left\| P_{X,Y|W_i=1} - P_{X,Y} \right\|_1 \leq 4\delta^{1/4} + 2 \cdot \Pr_{i\sim[n]}[i \notin \mathcal{G}] \leq 4\delta^{1/4} + 2\delta^{1/2} \leq o(1). \qquad \square$$