arXiv:2602.10368v1 [cs.DS] 10 Feb 2026

（承诺）约束满足问题鲁棒可满足性的新算法与硬度结果*

Joshua Brakensiek Lorenzo Ciardo Venkatesan Guruswami 加州大学伯克利分校 格拉茨工业大学 西蒙斯研究所和加州大学伯克利分校 Aaron Potechin Stanislav Živný 芝加哥大学 牛津大学

2026年2月12日

摘要

本文继续研究承诺约束满足问题（PCSP）的鲁棒可满足性。这项研究始于（Brakensiek、Guruswami、Sandeep，STOC 2023 /《离散分析》2025），并取得了以下结果：

- 对于带否定的 PCSP 1-in-3-SAT 与 NAE-SAT，我们证明，在唯一游戏猜想（UGC）成立的前提下，对于一个 $(1-\epsilon)$-可满足的实例，满足 $1-\Omega(1/\log(1/\epsilon))$ 个约束是困难的。这表明，对于交替阈值多态的情形，BGS 算法所遭受的指数损失是不可避免的；与之相反，多数多态可实现多项式损失。

- 对于任何具有多数多态的布尔承诺约束满足问题，在承诺存在一个能够满足较强约束中 $1-\epsilon$ fraction 的赋值时，我们给出一种算法，能够满足较弱约束中 $1-O(\sqrt{\epsilon})$ fraction。该算法显著推广了针对 2-SAT 的 Charikar–Makarychev–Makarychev 算法，并达到了唯一博弈猜想下可能实现的最优权衡。对于定义在更大域上的承诺约束满足问题，只要满足某种结构条件，该算法也可推广，但会额外损失一个 $\log(1/\epsilon)$ 因子；例如，一族相对多数多态就能蕴含这一结构条件。

- 我们证明，假设唯一博弈猜想成立，加入等式约束后，鲁棒可满足性得以保留。因此，我们可以将用于判定/搜索部分约束满足问题的丰富代数技术扩展到鲁棒 PCSP。我们的方法包括为约束满足问题开发一种相关且鲁棒的通用半定规划舍入算法，该算法源自（Brown-Cohen、Raghavendra，ICALP 2016）；这一结果或许也具有独立的研究价值。

*本文的扩展摘要发表于 SODA 2026 会议论文集。本研究部分得到西蒙斯研究者奖、美国国家科学基金会 CCF-2211972、美国国家科学基金会 DMS-2503280 以及英国研究与创新署 EP/X024431/1 的支持。

目录

1 引言 **3**

1.1 我们的结果 .61.2 技术概述 .81.3 论文结构 .14

2 记号 与预备知识14

2.1 承诺约束满足问题.142.2 基本半定规划.152.3 多态性.162.4 分析事实.16

3 交替阈值的整数间隙交替阈值 **多态性** **17**

3.1 尝试构造的整数间隙实例 .173.2 连续整数间隙实例 .193.3 离散化整性间隙实例 .213.4 可靠性分析 .23

4 MAJ 的改进分析MAJ **多态性** **26**

4.1 CMM 算法 .264.2 定理 4.4 的证明 .28

5 舍入 可分 PCSP 的方案33

6 等式保持鲁棒性 **39**

6.1 Brown-Cohen 和 Raghavendra 的算法概述 . . . . . 406.2 配置与舍入方案 .426.3 平滑配置 .446.4 测度论基础 .516.5 定义REQ .536.6 相关舍入 .576.7 定理 6.1 的证明 .59

7 结论 **61**

A 省略的证明 **66**

A.1 第 3 节中省略的证明.67A.2 第 6 节中省略的证明.72

1 引言

CSP 二分定理准确地指出了丰富的约束满足问题（CSP）类别中哪些问题可以在多项式时间内求解，其余问题则是 NP 完全的 [Zhu20，Bul17]。令人瞩目的是，这一里程碑式成果表明，从 3-SAT 出发的简单构件归约，是 CSP 存在高效算法的唯一障碍；反过来，只要存在一个“非平凡多态运算”，就足以实现多项式时间的可满足性算法。通俗地说，多态运算是一种算子，它将多个满足定义 CSP 的谓词的赋值组合起来，得到另一个满足赋值。

从算法角度看，本质上只有两种主要方法：局部一致性（也可通过线性规划 Sherali–Adams 层级的若干层来刻画） [BK14]以及高斯消元的推广形式 [BD06，IMM$^+$10]。然而，CSP 二分定理中的整体算法极具挑战性，因为要解决任意可处理的 CSP，可能需要以复杂的方式组合这两种基本算法范式。

聚焦于可处理 *CSP* 的多项式时间鲁棒可满足性算法时，情况要简单明了得多（但仍不简单）。这一概念最早由 Zwick 在一项出色的工作中提出 [Zwi98]。这类算法不仅能在存在完美满足赋值时找到它们，而且具有鲁棒性：当输入为近似可满足实例（即存在一种赋值，仅有ϵ 比例的约束无法满足）时，它们也能找到一种赋值，使得除 $g(\epsilon)$比例的约束外，其余约束均得到满足，其中损失为 $g(\epsilon)$ ，并且当 $\epsilon \to 0$时趋于零。

为便于表述，我们将能够使用此类高效鲁棒可满足性算法的约束满足问题称为鲁棒 *CSP*。我们进一步将其称为$(\epsilon, g(\epsilon))$-鲁棒 CSP，以表示鲁棒算法所造成的损失。每个鲁棒 CSP 都是可处理的——这可由 Barto 和 Kozik 的两项工作推出 [BK14,BK16]。然而，反过来并不成立：有些可处理的 CSP 并不存在鲁棒可满足性算法。最典型的这类 CSP 由阿贝尔群上的线性关系定义。此类 CSP 的可满足性可通过高斯消元高效判定；但根据 Håstad 著名的不可近似性结果 [Hås01], ，它们并不具备鲁棒性。[1] 另一方面，由局部一致性算法求解的可处理 CSP（文献中称为有界宽度CSP）实际上是鲁棒的。对于布尔 CSP，这一点已隐含在 Zwick 开创鲁棒可满足性研究的原始工作中 [Zwi98]。对于定义在任意固定有限域上的 CSP，这一点由 Barto 和 Kozik 证明 [BK16]。Barto 和 Kozik 此前一项突破性成果 [BK14] 表明，任何无法表达线性方程（按某种形式化定义）的 CSP，都可由局部一致性算法求解。因此，我们得到了一幅令人满意的图景：由局部一致性求解的 CSP——这是两种基本算法策略之一——恰好就是鲁棒的 CSP（这一说法曾在 [GZ12]中被明确猜想）。此外，对于所有这类 CSP，都存在一种基于半定规划的鲁棒可满足性算法。因此，相较于 CSP 精确可满足性的高度复杂情形，我们为鲁棒可满足性提供了一种统一的方法。从某种意义上说，鲁棒 CSP 二分定理给出了一个更简洁、更易理解的复杂性判据。

鉴于鲁棒 CSP 方面的这一背景，以及更广泛地理解基于半定规划的算法鲁棒性的研究动机，

[1]事实上，即使对于近似可满足实例，要超越仅简单输出随机赋值的平凡算法所达到的近似比也是NP-困难的。

Brakensiek、Guruswami 和 Sandeep [BGS25] 开启了对承诺约束满足问题鲁棒算法的研究，下面我们将介绍这一问题。承诺约束满足问题（简称 PCSP）是约束满足问题的一个广义扩展，近年来受到了广泛关注 [GS20, BWŽ21, BBB21, BG21b, BK22, BŽ22, NŽ22, CŽ23d, CŽ23a, KOWŽ23, BGS23, CŽ23c, CŽ23b, NŽ24, FNO+24, CŽ24, HMNŽ24, BK24, AFO+25, LŽ25, NVWŽ25, CKK+25, Mot25]。承诺约束满足问题由某个定义域对 (D, E) 上一组固定的关系对 (P_i, Q_i) 定义，其中 $P_i \subseteq Q_i$.[2] 给定一个基于这些关系的约束满足问题实例，目标是在承诺存在一个满足由 P_i 关系给出的（强）约束的赋值（但该赋值未知）的前提下，找到一个满足由 Q_i 关系给出的（弱）约束的赋值。承诺约束满足问题的一个经典例子是近似图着色问题 [GJ76]：给定一个可 k着色的图，求它的一个 ℓ着色，其中 $3 \leq k \leq \ell$。用我们的术语来说，这只是一个只有一对关系 (P, Q) 的 PCSP，其中 P 是 k元集合上的不等关系，而 Q 是 ℓ元集合上的不等关系。

PCSP 的另一个较新的例子是（$2+\epsilon$）-SAT 问题，由 Austrin、Guruswami 和 Håstad 提出并研究 [AGH17]（他们还创造了“承诺约束满足问题”这一说法）。他们实际研究的是一个更一般的问题：给定一个 k-SAT 实例，并承诺存在一个赋值，使每个子句中至少有 g 个文字为真，其中$1 \leq g \leq k$，要求找出一个标准的满足赋值（即每个子句中至少有 1 个文字为真）。在此情形下，P 关系编码的是汉明重量至少为g的布尔子句赋值，而 Q 关系编码的是汉明重量至少为 1 的布尔子句赋值。另一个例子是 1-in-3-SAT 与 NAE-SAT 问题，该问题由 Brakensiek 和 Guruswami 在一篇颇具影响力的论文中提出 [BG21a]，该论文开启了对布尔 PCSP 的系统研究。这里给定一个可满足的 1-in-3-SAT 实例，目标是找到一个赋值，使每个子句中有 1 个或 2 个变量为真。令人惊讶的是，这个问题可以在多项式时间内求解（所用算法此前未曾在约束满足问题的背景下得到考虑） [BG21a]。此外，也无法通过归约到（有限域）约束满足问题来获得这样的算法 [BBKO21]!

PCSP 的研究需要大量新的算法技术和困难性技术。在更广泛的 PCSP 背景下研究此类技术，也促成了标准（非承诺）约束满足问题的新成果，例如，结合线性规划与线性丢番图方程的单一算法 [BGWŽ20] 能够解决所有可处理的布尔 CSP。尽管 PCSP 受到广泛关注且近期取得了进展，其复杂性格局仍然十分广阔，大部分尚未得到理解。事实上，布尔 PCSP 的复杂性本身就是一项重大挑战；相比之下，在约束满足问题领域，Schaefer 早在 20 世纪 70 年代就证明了布尔 CSP 的二分定理 [Sch78]。继 [BG21a], 对允许否定的布尔对称 PCSP 进行分类之后，Ficak、Kozik、Olšák 和 Stankiewicz 又对具有对称关系的布尔 PCSP 进行了分类 [FKOS19]。此外，Brakensiek、Guruswami 和 Sandeep 对单调布尔 PCSP 进行了（有条件的）分类 [BGS23]。[3]

回到鲁棒可满足性，鉴于鲁棒 CSP 的清晰图景——即自然的半定规划要么给出高效的鲁棒算法，要么根本不存在——研究鲁棒 PCSP 是一个自然的目标，正如 Brakensiek、Guruswami 和 Sandeep（BGS）所提出的 [BGS25]。由关系对定义的部分约束满足问题的鲁棒可满足性算法（P_i, Q_i）的含义如下：

[2]更一般地，必须存在一个映射 $h\colon\ D \to E$ 它是从每个 P_i 到 Q_i的同态。 [3]该分类以 Braverman、Khot 和 Minzer 的 Rich 2-to-1 猜想 [BKM21]为前提。

给定一个实例，使得（$1-\epsilon$）比例的约束被承诺可根据较强关系 P_i 得到满足，则存在一种算法，能够（根据关系 Q_i）弱满足（$1-g(\epsilon)$）比例的约束，其中随着 $\epsilon \to 0$， $g(\epsilon) \to 0$。与约束满足问题一样，在这种情况下，我们称该部分约束满足问题是鲁棒的，或（ϵ， $g(\epsilon)$）-鲁棒的。

BGS 研究了布尔 PCSP，其中已知的可满足性算法[4] 可归因于多态性的存在。对于关系对 (P, Q)，多态性是从 P^m 到 P 的（范畴）幂 Q 的一个同态，其中 $\mathrm{Pol}(P, Q)$ 表示所有多态性的集合。形式化定义见第 2.3 节。更具体地说，BGS 重点研究了三类多态性：多数（MAJ）、交替阈值（AT）和奇偶校验 [BG21a]。对于任意奇数 $L \in \mathbb{N}$，令 MAJ_L、AT_L、PAR_L： $\{-1,1\}^L \to \{-1,1\}$ 定义如下

$$\mathrm{MAJ}_L(x_1,\dots,x_L) := \mathbf{1}\left[\sum_{i=1}^{L} x_i \geq 0\right],$$
$$\mathrm{AT}_L(x_1,\dots,x_L) := \mathbf{1}\left[\sum_{i=1}^{L} (-1)^{i-1} x_i \geq 0\right],$$
$$\mathrm{PAR}_L(x_1,\dots,x_L) := \mathbf{1}\left[\sum_{i=1}^{L} x_i \equiv L \mod 4\right].$$

令 $\mathrm{MAJ} := \{\mathrm{MAJ}_L : L \in \mathbb{N} \text{ odd}\}$、$\mathrm{AT} := \{\mathrm{AT}_L : L \in \mathbb{N} \text{ odd}\}$、$\mathrm{PAR} := \{\mathrm{PAR}_L : L \in \mathbb{N} \text{ odd}\}$ 分别表示相应的多态性集合。在其中两种情形下，即多数和 AT，BGS 表明，基于半定规划的算法可使相应的 PCSP 具有鲁棒性 [BGS25]。他们还证明了一个部分逆命题成立：对于由单个对称布尔关系对 (P, Q) 定义的 PCSP（并允许使用否定），如果关系对 (P, Q) 不具有某个奇数元 MAJ 多态性，也不具有某个奇数元 AT 多态性，那么该 PCSP 就不是鲁棒的（假设唯一游戏猜想成立）。

然而， [BGS25]针对两种情形（多数和交替阈值）的鲁棒满足算法，在定量方面存在显著差异。对于多数情形，BGS 算法实际上与针对 2-SAT 的 Charikar–Makarychev–Makarychev 算法相同，只是在更一般的条件下进行分析，仅假设存在多数多态；该算法保证违反的约束比例至多为 $\widetilde{O}(\epsilon^{1/3})$。这弱于针对 2-SAT 的 [CMM09] 算法所给出的 $(\epsilon, O(\sqrt{\epsilon}))$-鲁棒性保证——在唯一游戏猜想下，该保证是紧的 [KKMO07, MOO10] [Kho02, KKMO07, MOO10]。[5] 因此，一个自然的问题是：针对多数多态的 BGS 损失保证能否改进为 $O(\sqrt{\epsilon})$？若能，就能得到针对 2-SAT 的 CMM 鲁棒算法在多态性上的恰当推广。

对于具有 AT 多态性的布尔 PCSP，鲁棒算法的情况更差，因为 BGS 算法仅证明了 $(\epsilon, O(\log\log(1/\epsilon)/\log(1/\epsilon)))$-鲁棒性。随之而来的一个自然问题是，这种指数损失是否必要，或者对于 AT 情形是否也能像多数情形那样实现多项式损失。我们在本工作中探讨并解决了这两个问题。

[4]请注意，鲁棒 PCSP 首先必须是可解的。[5]从历史上看，证明 Goemans–Williamson 鲁棒算法在最大割问题上的近乎最优性（该算法还能达到 $O(\sqrt{\epsilon})$ 损失），正是最初提出唯一游戏猜想的动机，见 [Kho02]。

1.1 我们的结果

本文的贡献分为三个部分。首先，我们证明，由 Brakensiek–Guruswami–Sandeep 提出的针对交替阈值的鲁棒算法 [BGS25]在唯一博弈猜想下具有近乎匹配的困难性结果。这基于一个针对(1-IN-3-SAT,NAE-SAT)的新颖整数间隙。其次，我们证明，任何具有多数多态的承诺模板都存在损失为 $g(\epsilon) = O(\sqrt{\epsilon})$ 的鲁棒算法，该结果渐近紧致，并改进了 BGS 对 $O(\epsilon^{1/3})$ 的分析。我们进一步扩展这一分析，证明类似算法可达到 $O(\sqrt{\epsilon \log(1/\epsilon)})$ 的鲁棒性，适用于相对多数及相关多态性。最后，我们证明,-在唯一博弈猜想下，承诺约束满足问题的鲁棒性在一大类构件归约下（近似地）得以保持。我们通过解决一个看似初等但技术上复杂的问题来做到这一点：给定一个具有鲁棒算法的承诺模板，证明向该模板添加等式关系（近似地）保持该问题的鲁棒性。

交替阈值的困难性。Brakensiek–Guruswami–Sandeep [BGS25] 的一个关键结果表明，对于任意满足 AT $\subseteq$ Pol(P, Q) 的承诺模板 (P, Q)，PCSP(P, Q) 是具有 $g(\epsilon) = O(^{\log} \log(1/\epsilon) \log(1/\epsilon))$ 损失的鲁棒问题。有趣的是，对手约束满足问题，或与与多态运算集合也呈现出类似的渐近行为，而且已知这是紧的 [Zwi98, GZ12]。我们通过证明其具有唯一博弈猜想困难性，表明交替阈值也表现出类似的行为。

定理 1.1 (交替阈值困难性，非正式表述)。 假设唯一博弈猜想成立，则fiPCSP(*1-in-3-SAT, NAE-SAT*) 不是$(\epsilon, \Omega(1/\log(1/\epsilon)))$-鲁棒的。

这里fiPCSP (折叠幂等部分约束满足问题)指的是允许对变量取否定并将其设为常量的部分约束满足问题（参见 [BGS25]）。使用否定是必要的，因为 Brakensiek– Guruswami–Sandeep [BGS25] 指出，不使用否定时，(1-IN-3-SAT,NAE-SAT) 具有多项式损失的鲁棒性。定理1.1 将在第3节证明。利用 Raghavendra 定理 [Rag08]，，我们通过构造一个显式的整数间隙来证明定理1.1 ；这与 Guruswami–Zhou 为 HORN-3-SAT [GZ12]所采用的总体策略相同，不过在我们的设定中，具体实施和分析要复杂得多。更多细节将在第1.2节说明。

多数及更广泛情形的改进分析。 我们的下一个结果是一个针对具有多数多态的部分约束满足问题的鲁棒算法，并采用了改进的损失函数。

定理 1.2 (MAJ 鲁棒性，非正式表述)。 对于任意承诺模板(P, Q)，若其满足MAJ $\subseteq$Pol(P, Q)，则PCSP(P, Q) 是$(\epsilon, O(\epsilon^{1/2}))$-鲁棒的。

该结果在第 4 节中证明。我们注意到，定理 1.2 中使用的算法与 [BGS25] 中使用的算法完全相同。分析方面的主要改进来自对多元正态分布更精细的分析。更多详情请参见第 1.2 节。

注意，定理 1.2仅适用于布尔 PCSP。多数多态的一种常见非布尔变体是相对多数 多态性。具有此类多态性的（P）CSP 的典型例子包括唯一博弈 [Kho02]，以及所谓的 SetSAT 问题——一种非布尔推广形式$(2+\epsilon)$-SAT [AGH17]，由 [BWŽ21] 引入。

[6]对于任意 $L \in \mathbb{N}$，若 OR$_L$(x_1、.....、x_L) $= 1$，则 $x_i = 1$ 对某个 $i \in [L]$ 成立；且若 AND$_L$(x_1、.....、x_L) $= 1$，则 $x_i = 1$ 对所有$i \in [L]$成立。

定理 1.3 (PLUR 鲁棒性，非正式表述)。 对于任意承诺模板 (P, Q)，若其具有 $\mathrm{PLUR} \subseteq \mathrm{Pol}(P, Q)$，则 $\mathrm{PCSP}(P, Q)$ 是$(\epsilon, O(\epsilon^{1/2}\log(1/\epsilon)))$-鲁棒的。

该结果在第 5 节中证明。我们指出，定理 1.3 只是第 5 节主要结果的一个特例，该结果适用于任意可分离的部分约束满足问题，见定理 5.3。我们将在第 1.2 节更精确地描述这一更广泛的类别。

鲁棒小工具归约（添加等式约束）。在几乎所有关于约束满足问题（及其变体）的分类中，一项重要工具都是约束满足问题模板之间的构件归约。例如，在 CSP 二分定理中，约束满足问题的困难性部分是通过从 3-SAT 进行构件归约来证明的 [BJK05]。鲁棒（P）CSP 也不例外，构件归约常用于研究模板之间的关系 [DK13、BGS25]。然而，普通 CSP 二分定理 [Bul17、Zhu20] 与鲁棒（P）CSP 的二分定理 [BK16]之间有一项重要区别：允许使用等式约束，我们将其记为 等式约束。对于（部分）约束满足问题的精确可满足性，如果指定某些变量必须相等，我们可以高效地计算等式关系的连通分量，并将问题简化为变量数更少且不含任何等式约束的形式。然而，对于鲁棒（P）CSP，等式是一个相当微妙的概念。如果最优赋值中只有 $1-\epsilon$ 个约束得到满足，我们并不清楚每个等式约束究竟应该被信任还是忽略。尽管如此，假设添加等式约束只会轻微改变所得部分约束满足问题的鲁棒性，仍然相当合理。

问题 1.4 (Barto–Kozik [BK16])。 设 Γ 是一个 *CSP* 模板，即一个关系集合。假设 $\mathrm{CSP}(\Gamma)$ 是 $(\epsilon, f(\epsilon))$-鲁棒的。那么 $\mathrm{CSP}(\Gamma \cup \{\text{等式约束}\})$ 是否 $(\epsilon, O(f(\epsilon)))$-鲁棒?

尽管 Barto–Kozik [BK16] 对所有鲁棒 CSP 给出了完整分类，[7] 但他们并未回答问题 1.4，除了一种非常弱的意义： $\mathrm{CSP}(\Gamma \cup \{\text{等式约束}\})$ 是 $(\epsilon, O(\log\log(1/\epsilon)/\log(1/\epsilon)))$-鲁棒的，且与 f无关。在本文中，我们证明问题 1.4 对于 CSP 和 PCSP 几乎 都成立：

定理 1.5 (等式的鲁棒性，非正式表述)。 假设唯一博弈猜想成立。对于任意承诺模板 Γ，若 $\mathrm{PCSP}(\Gamma)$ 是 $(\epsilon, f(\epsilon))$-鲁棒的，则 $\mathrm{PCSP}(\Gamma \cup \{\text{等式约束}\})$ 是 $(\epsilon, O(f(\epsilon^{1/6})))$-鲁棒的。

作为一个直接推论，我们现在可以利用研究（P）CSP 时可用的最一般构件归约来研究鲁棒（P）CSP，但鲁棒性会有多项式损失。

定理 1.6 （构件归约，非正式表述）。 假设唯一博弈猜想成立。设 Γ 和 Γ' 是承诺模板，且存在一个构件归约[8]，将 $\mathrm{PCSP}(\Gamma')$ 归约到 $\mathrm{PCSP}(\Gamma)$。若 $\mathrm{PCSP}(\Gamma)$ 是$(\epsilon, f(\epsilon))$-鲁棒的，则 $\mathrm{PCSP}(\Gamma')$ 是 $(\epsilon, O(f(\epsilon^{1/6})))$-鲁棒的。

这些结果在第 6 节中得到证明。在技术概述（第1.2 节）中，我们介绍了用于确立这些结果的技术，包括对 Brown-Cohen 和 Raghavendra [BR16] 的近似（承诺）约束满足问题算法的改编。

[7]我们注意到，Barto–Kozik 通过使用不允许 等式的构件归约，成功确立了这一分类。利用定理 1.6，理论上可以简化 Barto–Kozik 证明中的部分内容，不过定理 1.6 的证明要复杂得多，远超 Barto–Kozik 所需的变通方法。[8]更确切地说，存在一个小族同态，将 $\mathrm{Pol}(\Gamma)$ 映射到 $\mathrm{Pol}(\Gamma')$。

1.2 技术概述

交替阈值的困难性。 我们针对 1-IN-3-SAT 与NAE-SAT 的整数性间隙实例，其高层思路与以下 Horn-SAT 的线性规划整数间隙实例类似 [GZ12]:

1. 我们有变量 $\{x_{j1}, x_{j2} : j \in [k]\}$ 其中 $k = \lceil 1/\log_2(\epsilon) \rceil + 1$。
2. 我们有一元约束 x_{11}、 x_{12} 和 $\neg x_{k1}$ ，其中 1 为真，而 -1 为假。
3. 对所有 $j \in [k-1]$，我们都有约束 $\neg x_{j1} \vee \neg x_{j2} \vee x_{(j+1)1}$ 和 $\neg x_{j1} \vee \neg x_{j2} \vee x_{(j+1)2}$。

显然，此实例不可满足，因为我们要求 x_{11}， x_{12} 为真；根据蕴含约束链， x_{k1}， x_{k2}也应为真，但我们要求 x_{k1} 为假。由于约束只有 $O(k) = O(\log(1/\epsilon))$ 个，此实例的整数值至多为 $1 - \Omega(1/\log(1/\epsilon))$。

另一方面，下面的线性规划解使所有约束的值至少为 $1 - \epsilon$：

1. 对于每个 $j \in [k]$，我们给出 x_{j1} 和 x_{j2} 的偏置 $1 - 2^{j+1-k}$。
2. 对于约束 x_{11}，我们可以以概率 $1 - 2^{1-k}$ 设置 $x_{11} = 1$ ，并以概率 2^{1-k} 设置 -1 ，这样就有 $\mathbb{E}[x_{11}] = 1 - 2^{1-k} - 2^{1-k} = 1 - 2^{2-k}$。因此，线性规划对该约束给出的值为 $1 - 2^{1-k} \geq 1 - \epsilon$。根据对称性，线性规划对约束 x_{12} 给出的值也为 $1 - 2^{1-k} \geq 1 - \epsilon$。
3. 对于每个 $j \in [k-1]$，对于约束 $\neg x_{j1} \vee \neg x_{j2} \vee x_{(j+1)1}$，我们可以采用如下分布：

   a. 以 $1 - 2^{j+1-k}$ 的概率，我们设置 $x_{j1} = x_{j2} = x_{(j+1)1} = 1$。b. 以 2^{j-k} 的概率，我们设置 $x_{j1} = 1$、 $x_{j2} = -1$ 和 $x_{(j+1)1} = 1$。c. 以 2^{j-k} 的概率，我们设置 $x_{j1} = -1$、 $x_{j2} = 1$ 和 $x_{(j+1)1} = 1$。

   在此分布下， $\mathbb{E}[x_{j1}] = \mathbb{E}[x_{j2}] = (1 - 2^{j-k}) - 2^{j-k} = 1 - 2^{j+1-k}$ 与 $\mathbb{E}[x_{(j+1)1}] = (1 - 2^{j+1-k}) - 2^{j+1-k} = 1 - 2^{j+2-k}$。因此，线性规划（LP）为该约束赋值 1。根据对称性，线性规划也为约束 $\neg x_{j1} \vee \neg x_{j2} \vee x_{(j+1)2}$ 赋值 1。
4. x_{k1} 的偏置为 $1 - 2 = -1$ ，因此 x_{k1} 始终设为 -1 ，这满足约束$\neg x_{k1}$。

可以这样理解这个整数性间隙实例：为了避免违反约束，必须满足以下条件。

1. 偏置为 $1 - 2^{j+1-k}$ 的变量必须舍入为 1。2. 对于所有 $j \in [k-1]$，如果偏置为 $1 - 2^{j+1-k}$ 的变量舍入为 1，那么偏置为 $1 - 2^{j+2-k}$ 的变量也舍入为 1。3. 偏置为 -1 的变量必须舍入为 -1。

由于我们可以在 $O(\log(1/\epsilon))$ 步内得到矛盾，因此至少有 $\Omega(1/\log(1/\epsilon))$ 个约束必须被违反。

我们将对整数性间隙实例采用类似的思路。我们将构造这个实例，使得尽管半定规划值至少为 $1-\epsilon$，但如果要避免违反大量约束，

1. 几乎所有偏置为 $1-2^{-k}$ 的变量都必须设为 1，几乎所有偏置为 $2^{-k}-1$ 的变量都必须设为 -1。2. 对所有 $j \in [k]$，如果几乎所有偏置为 $1-2^{-j}$ 的变量都设为 1，那么几乎所有偏置为 $2^{1-j}-1$ 的变量都设为 -1。类似地，对所有 $j \in [k]$，如果几乎所有偏置为 $2^{-j}-1$ 的变量都设为 -1，那么几乎所有偏置为$1-2^{1-j}$ 的变量都设为 1。

接着我们观察到，这些条件意味着几乎所有偏置为 0 的变量都设为 1，而几乎所有偏置为 0 的变量都设为 -1，这是不可能的。由于我们可以在 $O(\log(1/\epsilon))$ 步内得到一个矛盾，因此至少 $\Omega(1/\log(1/\epsilon))$ 个约束必须被违反。

为了得到 1-in-3-SAT 约束，我们发现需要使用形如 $\{x\mathbf{v}_0+\sqrt{1-x^2}\mathbf{w}\}$ 的一般向量，其中$\mathbf{w}$ 与$\mathbf{v}_0$正交。一种自然的选择是使用所有$\mathbf{w} \in S^{d-1}$，其中 d 足够大，且取决于 ϵ。虽然这能构造出一个整数性间隙实例，但它的规模是无限的，而且不太容易分析，因为它涉及球面上的函数，而不是以多元高斯输入为输入的函数。因此，我们对这个整数性间隙实例作如下修改：

1. 我们不再使用向量$\mathbf{w} \in S^{d-1}$，而改用向量$\mathbf{w} \sim \mathcal{N}(0,1/d)^d$。2. 对于除可忽略部分以外的所有约束，我们的向量$\mathbf{w} \sim \mathcal{N}(0,1/d)^d$ 都非常接近单位向量，因此可以舍弃向量性质不佳的那一小部分约束。3. 我们将空间划分为若干区域，并把每个区域中的所有向量映射到该区域的一个代表向量，从而对实例进行离散化。

经过仔细分析，我们证明，对于这个修改后的实例，必须违反 $\Omega(1/\log(1/\epsilon))$ 比例的约束；即使进行了这些修改，该实例的半定规划值仍至少为 $1-\epsilon$。

多数多态的改进分析。现在我们转而为一类部分约束满足问题设计鲁棒算法。首先，我们讨论 Brakensiek、Guruswami 和 Sandeep 所用的算法 [BGS25]，该算法适用于具有多数多态的承诺模板。该算法受到 Charikar、Makarychev 和 Makarychev 所用算法的启发 [CMM09]，后者用于鲁棒 MAX 2-SAT。

为方便起见，我们将布尔域重新标记为 $\{-1,+1\}$。固定一个模板 $(P,\ Q)$，其中 MAJ $\subseteq$ Pol$(P,\ Q)$。考虑一个定义在变量 x_1、……、x_n 和子句C_1、……、C_m上的 PCSP$(P,\ Q)$ 实例。该算法首先为此实例求解基本半定规划，方法是寻找单位

向量 $\mathbf{v}_0, \mathbf{v}_1$、……、$\mathbf{v}_n \in \mathbb{R}^{n+1}$（其中 $\mathbf{v}_0$ 表示“真值”向量），使得向子句进行向量赋值的平均值为 $1-\epsilon$，其中 $\epsilon > 0$ 是指定的鲁棒性参数。接下来，我们对多元正态向量 $\mathbf{r} \in \mathcal{N}(0^{n+1}, I_{n+1})$ 进行随机采样。然后，对所有 $i \in [n]$，若 $\langle \mathbf{v}_i, \mathbf{v}_0 + \mathbf{r} \cdot \epsilon^{2/3} \rangle \geq 0$，则将 x_i 舍入为 $+1$；否则采用另一种舍入方式。在此，我们通过新分析将$\epsilon^{2/3}$ 改进为 $\sqrt{\epsilon}$。

我们简要解释 Brakensiek、Guruswami、Sandeep [BGS25] 在分析该算法时的关键思想。利用他们论文中的一个归约，我们也可以不失一般性地假设 $Q = \{-1,+1\}^k \setminus \{(-1)^k\}$。换言之，假设对 P 的任意赋值列表的多数投票永远不会全是 -1。为简单起见，固定变量x_1，……，x_k 上的一个子句 C_i，使得半定规划向量 $\mathbf{v}_0, \mathbf{v}1$，……，$\mathbf{v}_k$ 给出的值为 $1-\epsilon$。可能出现的情况是，对所有 $i \in [n]$，$\langle \mathbf{v}_i, \mathbf{v}_0 \rangle \approx -\Theta(\epsilon)$，因此仅对 $\langle \mathbf{v}_i, \mathbf{v}_0 \rangle$ 进行舍入将无法满足任何子句。BGS 的一个关键观察是，只要这些向量具有完备性 $1-\epsilon$，就存在一个概率分布 $(w_1, \ldots, w_k)$，使得 $\sum_{i=1}^k w_i \langle \mathbf{v}_i, \mathbf{v}_0 \rangle \geq -\epsilon$（见引理 4.3）。令 $\mathbf{u}$：

$$= \sum_{i=1}^k w_i \quad i \qquad 1-\epsilon^{O(1)} \qquad |\langle \ , \ \rangle| = \mathbf{v}。$$

$$O \qquad 1/\epsilon \qquad \langle \ , \ _0 + \ \cdot \epsilon^{2/3} \rangle = \sum_{i=1}^k w_i \langle \ _i \quad _0 + \ \cdot \epsilon^{2/3} \rangle$$

由集中性，我们可以以一定概率假设 $\mathbf{u}$ r (log( ))。作为一个关键观察，注意到由于 u v r v，v r，如果所有 k 变量都舍入为 -1，则 $\langle \mathbf{u}, \mathbf{v}_0 + \mathbf{r} \cdot \epsilon^{2/3} \rangle$ 为负。然而，$\langle \mathbf{u}, \mathbf{v}_0 \rangle \geq -\epsilon$，且 $\langle \mathbf{u}, \mathbf{r} \cdot \epsilon^{2/3} \rangle$ 的标准差至多为 $\epsilon^{1/3}$。因此，如果 $\langle \mathbf{u}, \mathbf{v}_0 + \mathbf{r} \cdot \epsilon^{2/3} \rangle$ 为负，它也只是勉强为负。因此，这严格约束了每个 $\langle \mathbf{v}_i, \mathbf{v}_0 + \mathbf{r} \cdot \epsilon^{2/3} \rangle$的值，而由于正态分布的反集中性，这种情况不太可能发生。

通过更仔细地分析这些舍入概率，我们可以将舍入阈值改为 $\langle \mathbf{v}_i, \mathbf{v}_0 + \mathbf{r} \cdot \sqrt{\epsilon} \rangle$，并获得 $1 - O(\sqrt{\epsilon})$ 的成功概率（可靠性）。关键思路是，不直接将每个 $\langle \mathbf{u}, \mathbf{r} \rangle$ 与各自的分布 $\langle \mathbf{v}_i, \mathbf{r} \rangle$ 进行比较，而是对这些向量进行更仔细的分解。具体而言，定义 $\mathbf{v}_i^{=}$为平行于 $\mathbf{u}$ 的 $\mathbf{v}_i$分量，并令 $\mathbf{v}_i^{\perp}$为垂直于 $\mathbf{u}$ 的 $\mathbf{v}_i$ 分量。由于 $\mathbf{v}_i^{=}$与 $\mathbf{u}$ 仅相差一个标量因子，$\langle \mathbf{v}_i^{=}, \mathbf{r} \rangle$ 与 $\langle \mathbf{u}, \mathbf{r} \rangle$ 也仅相差一个标量因子。不过，$\langle \mathbf{v}_i^{\perp}, \mathbf{r} \rangle$ 与$\langle \mathbf{u}, \mathbf{r} \rangle$相互独立。利用这一观察，我们可以将论证分为三个高层次情形。

首先，如果 $\|\mathbf{u}\|_2^2 = \Omega(\epsilon \log(1/\epsilon))$，那么 $\langle \mathbf{u}, \mathbf{v}_0 \rangle$ 将主导 $\langle \mathbf{u}, \mathbf{r}\sqrt{\epsilon} \rangle$，因此$\langle \mathbf{u}, \mathbf{v}_0 + \mathbf{r} \sqrt{\epsilon} \rangle \leq 0$ 的概率相当小。

其次，如果垂直分量较大，即对于某个 $i \in [k]$，有 $\|w_i \mathbf{v}_i^{\perp}\|_2 = \Omega(1)$，那么即使我们以 $\langle \mathbf{u}, \mathbf{r} \rangle$ 为条件，$\langle w_i \mathbf{v}_i, \mathbf{v}_0 + \sqrt{\epsilon}\mathbf{r} \rangle$ 的方差仍然相当可观。特别是，$\langle w_i \mathbf{v}_i, \mathbf{v}_0 + \sqrt{\epsilon}\mathbf{r} \rangle$ 很可能会出现以下两种情况之一：(1) 过于正，此时 i 会被正确舍入；或 (2) 过于负，此时 $\sum_{j \neq i} w_j \langle \mathbf{v}^j, \mathbf{v}_0 + \sqrt{\epsilon}\mathbf{r} \rangle$ 的平均值为正，因此某个其他的 j 会被正确舍入。

仅这两种情况就足以带来 $\sqrt{\epsilon}\log(1/\epsilon)$ 的损失。为了消去对数因子，在第三种也是最后一种情况下，我们对可能出现的“坏”结果空间进行细致划分，并证明这些结果总共给舍入过程带来的损失至多为 $O(\sqrt{\epsilon})$。这是论证中技术性最强的部分。

相对多数与可分离族的新算法。 我们将针对多数情形的这些舍入技术推广到非布尔域和更一般的舍入函数。为此，我们抽象出多数情形分析中的关键特征：强形式的约束 P 与舍入结果落在弱形式 Q之外的半定规划配置之间存在超平面分离。我们将具有这一性质的推广形式的模板定义为 (P, Q)，

并称之为可分离族。具体描述见定义 5.1。概括来说，其思路如下。在布尔域的多数情形中，我们的分析依赖于一个线性函数，该函数将 $\langle \mathbf{v}_i, \mathbf{v}_0 \rangle$ 与 Q中的一个缺失元组分离开来；这又可以通过与权重向量 w的内积来表示。在非布尔域 D中，对于每个变量 x_i 和每个域元素 $d \in D$，我们都有一个独立的向量 $\mathbf{v}_{i,d}$ 。因此，我们将 P 以及舍入结果落在 Q 之外的半定规划配置编码为矩阵空间 $\mathbb{R}^{k \times D}$中的两个凸体，其中 k 是约束的元数。第一个凸体是元组 $\mathbf{p} \in P$ 的独热编码 $\Pi_{\mathbf{p}}$ 的凸包（其中，当且仅当 $p_i = d$ 时，(i,d) 项等于 1，否则等于 0 ）。第二个凸体是给定舍入函数 ρ 对“坏”元组（即落在 Q之外的元组）的原像。如果 (P,Q) 的多态性足够丰富，就可以证明这两个凸集互不相交；在这种情况下，它们必定存在超平面分离。后者可以自然地表示为 $R^{k \times D}$ 上的线性泛函，由 Frobenius 内积与适当的权重矩阵 W 确定；这就是权重向量 w在非布尔域中的对应物。如果某个舍入函数 ρ使模板 (P,Q) 存在这样的分离，我们就称其为 ρ-可分离。[9] 若 ρ 满足额外的保守性条件（粗略地说，给定分布中的获胜元素的权重必须与零保持一定距离），我们便能利用超平面分离性质，通过推广布尔域多数情形分析中的一部分，证明 (P,Q) 可由半定规划鲁棒地求解，损失为 $O(\sqrt{\epsilon}\log(1/\epsilon))$。请注意，在这种设定下，我们得到的损失比多数情形略差，差距为一个 $\log(1/\epsilon)$ 因子（不过，即便对多数情形而言，这仍优于 [BGS25]中得到的损失）。这是因为，将半定规划向量拆分为平行分量和正交分量的技巧无法推广到非布尔域。

可分族的一个显著例子是唯一博弈问题。由于 Charikar、Makarychev 和 Makarychev 的算法，唯一博弈长期以来一直被认为存在鲁棒算法 [CMM06]（不过，该算法与这些作者用于 2-SAT 的算法相当不同）。他们的 2-SAT 算法能够扩展到唯一博弈这一事实，或许本身就值得关注。推动这一结果的核心多态性是 相对多数，它会从一列域元素中选出出现次数最多的元素，即使该元素的出现频率远低于 $1/2$。更有意思的是，我们基于多态性的结果涵盖了所有具有相对多数的承诺约束满足问题，尤其包括所谓的 SetSAT 承诺约束满足问题族。该问题族在 [BWŽ21] 中被指出，是 $(2+\epsilon)$-SAT [AGH17]的一种自然的非布尔推广。与唯一博弈不同，此前人们并不知道这些问题在任何损失下都是鲁棒可解的。

鲁棒小工具归约（添加等式）。现在我们讨论定理 1.5 和定理 1.6 的证明。假设定理 1.5，结合已有的鲁棒（P）CSP 构件归约 [DK13、BK16、BGS25] 与最先进的（P）CSP 构件归约 [BBKO21]，即可直接证明定理 1.6。具体细节见推论 6.2。

因此，我们重点概述定理 1.5 的证明。我们主要基于 Brown-Cohen 和 Raghavendra 的算法 [BR16]（“BCR 算法”），用于求解近似 MAX

[9]这类谓词与 Brakensiek–Guruswami 定义的“区域多态性”有些相似 [BG19]。

（P）CSP。[10] 为了进行这一高层次概述，我们假设我们的承诺模板是由一对布尔关系 (P, Q) 组成，且 $P \subseteq Q \subseteq \{-1, 1\}^k$。

我们首先介绍 BCR 算法的核心特点。对于变量集为 $x_1, \ldots, x_n$、子句为 $C_1, \ldots, C_m$ 的 PCSP(P, Q) 实例，我们可以将半定规划解视为一组单位向量 $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{R}^{n+1}$。在找到一个目标值接近最优的半定规划解后，BCR 算法通过采样两个随机对象继续执行：(i) 从多元正态分布中采样得到的一列随机向量 $\mathbf{r}_1, \ldots, \mathbf{r}_D \in \mathbb{R}^{n+1}$，以及 (ii) 一个舍入函数[11] H：$\mathbb{R}^D \to [-1, 1]$。对于每个 $i \in [n]$，我们随后通过以下方式定义一个分数赋值$z_i \in [-1, 1]$

$$z_i := H(\mathbf{v}_0 \cdot \mathbf{v}_1 + \mathbf{v}_i^{\perp} \cdot \mathbf{r}_1, \ldots, \mathbf{v}_i \cdot \mathbf{v}_0 + \mathbf{v}_i^{\perp} \cdot \mathbf{r}_D),$$

其中我们设 $\mathbf{v}_i^{\perp} = \mathbf{v}_i - (\mathbf{v}_0 \cdot \mathbf{v}_i)\mathbf{v}_0$。。随后，我们通过独立舍入 x_i 得到 PCSP 的一个整数解：以概率 $\frac{1+z_i}{2}$ 将其舍入为 $+1$，否则舍入为 -1。——

令 $\mathcal{R}$ 为关于选择（$\mathbf{r}_1, \ldots, \mathbf{r}_D$）和 H的概率分布。因此，我们可以将 BCR 舍入方案视为一个映射 BCR：$\mathbb{R}^{n+1} \times \mathcal{R} \to [-1, 1]$，其中在算法开始时选取全局共享随机性 $R \in \mathcal{R}$，随后对于每个 $i \in [n]$，我们设$z_i :=$ BCR$(\mathbf{v}_i, R)$。于是，算法所假设的鲁棒性可转化为以下保证。

关键性质。 对于每个半定规划解 $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_n$，只要其值至少为 $1 - \epsilon$，舍入后的赋值 BCR$(\mathbf{v}_1, R) \ldots,$ BCR$(\mathbf{v}_n, R)$ 就能在对 $R \in \mathcal{R}$ 的选择取期望时满足我们实例中 $1 - f(\epsilon)$ 的约束。

现有方案本身对于 PCSP(EQ) 可能不具备鲁棒性，原因如下：给定两个在欧几里得距离上相隔 δ 的向量 $\mathbf{v}_i$ 和$\mathbf{v}^j$，对于典型的 $R \sim \mathcal{R}$，相应的 BCR$(\mathbf{v}_i, R)$ 和 BCR$(\mathbf{v}^j, R)$ 可能会有很大差异。[12] 为了使 BCR 舍入方案对等式约束也具备鲁棒性，我们以如下方式利用关键性质。考虑一个映射 M_δ：$\mathbb{R}^{n+1} \to \mathbb{R}^{n+1}$（不一定是线性的），使得对于每个单位向量 $\mathbf{v}$，$\mathbf{v}$ 与 $M_\delta(\mathbf{v})$ 之间的距离至多为 δ。于是我们可以考虑以下方案：$S_\delta(\mathbf{v}\ R) :=$ BCR$(M_\delta(\mathbf{v})\ R)$。一个关键观察是，$S_\delta$ 仍然是一个鲁棒舍入方案，只是参数稍差。

要看出其原因，用 S_δ 对解$\mathbf{v}_1, \ldots, \mathbf{v}_n$ 进行舍入，实际上等同于用BCR对 $M_\delta(\mathbf{v}_1) \ldots, M_\delta($ $\mathbf{v}_n)$进行舍入。由于每个$\mathbf{v}_i$与 $M_\delta(\mathbf{v}_i)$的欧几里得距离都很近，当 δ足够小时，解[13] $M_\delta(\mathbf{v}_1) \ldots,$ $M_\delta(\mathbf{v}_n)$的半定规划值仍约为$1 - \epsilon$，因此我们平均仍大约满足 $1 - f(\epsilon)$个约束。

---

[10]严格来说，Raghavendra 定理和 Brown-Cohen–Raghavendra 的结果只针对约束满足问题，但正如 Brakensiek、Guruswami、Sandeep [BGS25], 所指出的，他们的论证稍作修改后也适用于部分约束满足问题。[11]舍入函数的选择取决于某些近似多态是否存在，精确定义见第 6.1节。[12]一般而言 H 非常轻微地平滑，因此可以直接将 BCR 算法与相关舍入技巧结合，得到一个用于等式约束的鲁棒算法。问题在于，该鲁棒算法的可靠性取决于 BCR 所考虑的近似多态的元数。然而，BCR 并未给出这些近似多态规模的有效上界，因此其保证远不如定理 1.5。[13]可能会出现这样的情况：$M_\delta(\mathbf{v}_1)$.....，$M_\delta(\mathbf{v}_n)$ 由于违反三角不等式，不再是有效的半定规划解。解决这一问题在技术上相当复杂，需要改造 Raghavendra 和 Steurer 提出的平滑技巧 [RS09]。在本概述中，我们暂不讨论这个重要问题。

更一般地， M_δ： $\mathbb{R}^{n+1} \to \mathbb{R}^{n+1}$ 不必是确定性的，而可以是任意随机映射，使得输入向量与输出向量的距离绝不会超过 δ 。我们将这样的随机映射称为 δ-散布，如果对每个单位向量$\mathbf{v}$，其概率分布 $M_\delta(\mathbf{v})$ 的支撑集位于球 $B(\mathbf{v}\ \delta)$ 内，且概率随距离平滑衰减。参见定义 6.27 以获得精确定义。

对于给定的 δ-扩散（即 M_δ 的分布），相应的舍入方案 $S_\delta(\mathbf{v}\ R) := \mathbb{E}_{M_\delta}[\mathrm{BCR}(M_\delta(\mathbf{v})\ R)]$ 称为 BCR 的 δ-平滑化。根据前述逻辑，BCR 的任何 δ-平滑化仍然近似为 $(\epsilon, f(\epsilon))$-鲁棒。特别地，现在我们有大量舍入方案，它们对于 PCSP(P, Q) 都是鲁棒的。

下一步，我们要从这些 δ-平滑化中选出一个同时对等式约束也鲁棒的方案。对于每个单位向量 $\mathbf{v} \in \mathbb{R}^{n+1}$，我们考察以下范数：

$$\|S_\delta(\mathbf{v})\|_2 := \sqrt{\mathbb{E}_{R\sim\mathcal{R}}[S_\delta(\mathbf{v}, R)^2]}.$$

回想一下， S_δ的值域是 $[-1, 1]$，因此 $S_\delta(\mathbf{v}\ R)^2$ 大致衡量了舍入方案对这个值的确定性。虽然这相当违反直觉，但我们选择 BCR 的 δ-平滑化，使得对于所有单位向量 $\mathbf{v} \in \mathbb{R}^{n+1}$，$\|S_\delta(\mathbf{v})\|_2$ 都达到最小值。我们将此方案称为 REQ$_\delta$，因为很快就会看到，它对等式具有鲁棒性。粗略来说，REQ$_\delta$ 是具有最大熵的 BCR δ-平滑化。

我们要证明的关键引理是，存在一些（较小的）常数 c_1， $c_2 \geq 1$ 使得如果两个向量 $\mathbf{v}$ 和 $\mathbf{w}$ 之间的距离不超过 δ^{c_1} ，那么

$$\sqrt{\mathbb{E}_{R\sim\mathcal{R}}[(\mathrm{REQ}_\delta(\mathbf{v}, R) - \mathrm{REQ}_\delta(\mathbf{w}, R)^2]} \leq \delta^{c_2}.$$

引理 6.31给出了精确陈述。该引理的证明用到了这样一个事实：围绕 δ 的可能平滑化$\mathbf{v}$ 与围绕 δ 的平滑化$\mathbf{w}$ 相当相似（见命题 6.32）。如果把这些 δ-平滑化空间看作凸体，那么其中一个凸体的 L^2 极小化元必定与另一个凸体的 L^2 极小化元十分接近。这足以证明引理6.31。

然而，REQ$_\delta$ 本身并不是一个适用于具有等式约束的 $(P,\ Q)$ 的鲁棒舍入方案。原因是，到目前为止我们只证明了：如果 $\mathbf{v}_i$ 和 $\mathbf{v}^j$ 接近，那么对 $R \in \mathcal{R}$ 的选择取平均后，输出 $z_i = \mathrm{REQ}_\delta(\mathbf{v}\ R)$ 与 $^{z_j} = \mathrm{REQ}_\delta(\mathbf{w}\ R)$ 接近。然而，请记住，每个 z_i 都是通过独立的抛硬币方式舍入为整数赋值的。特别是，如果 $z_i = z_j = 0$，那么等式约束仅以 $1/2$ 的概率得到满足。

为解决这一问题，作为最后一步，我们将独立舍入改为相关舍入。在布尔情形下，这需要随机选取一个全局阈值 $t \in [-1/2, 1/2]$，并将每个 x_i 舍入为1 ，当 $z_i > t$ 且 -1 ；否则舍入为 0。现在，如果 $z_i \approx z_j$，相应的等式约束几乎总能得到满足。代价是，对于 $f(\epsilon)$ 的 PCSP(P, Q)，其鲁棒性会降低一个常数因子。精确细节见第6.6 节。

总而言之，我们的舍入方案是借助相关舍入实现的 REQ$_\delta$ ，适用于 $\delta = \epsilon^{O(1)}$ 。由于证明过程中存在各种多项式损失，这一新方案是（近似）$(\epsilon,\ f(\epsilon^{1/6}))$-鲁棒的。

1.3 论文结构

第 2 节介绍理解主要结果所需的背景知识和符号。第 3 节给出了鲁棒求解 fiPCSP(1-IN-3-SAT，NAE-SAT) 的整数间隙，从而证明定理 1.1。第 4 节对 Brakensiek–Guruswami–Sandeep 关于多数多态的算法进行了渐近最优分析，从而证明定理1.2。第 5 节将定理 1.1 推广到可分 PCSP，特别证明了定理 1.3。第 6 节通过改造 Brown-Cohen 和 Raghavendra 的舍入方案 [BR16]，证明定理 1.5 和定理 1.6 。第 7 节总结全文，并列出一些开放问题。

2 符号与预备知识

2.1 承诺约束满足问题

设 D、E 为有限域。PCSP 模板是由 $\Gamma = \{(P_1, Q_1) \dots, (P_t, Q_t)\}$ 组成的集合，其中每一对都是元数为 $k_1, \dots, k_t \in \mathbb{N}$ 的关系，并且对所有 $i \in [t]$ $P_i \subseteq D^{k_i}$ 和 $Q_i \subseteq E^{k_i}$ 都成立。我们还要求存在一个同态 h，使得对所有 $i \in [t]$，它都将 P_i 中的元组映射为 Q_i 中的元组；也就是说，存在映射 $h\colon D \to E$，满足对每个 $i \in [t]$ 和每个 $\mathbf{x} \in P_i$，都有 $h(\mathbf{x}) \in Q_i$。[14]当 $t = 1$ （即当 Γ 只包含一个承诺关系 (P, Q)）时，我们也将 PCSP(Γ) 写作 PCSP(P, Q)。此外，当对所有 $i \in [t]$ 都有 $P_i = Q_i$ 时，我们称 Γ 为 CSP 模板。

设 Γ 是一个 PCSP 模板。PCSP(Γ) 的一个实例由一组变量$V = \{x_1, \dots, x_n\}$和一组约束 $\mathcal{C} = \{C_1, \dots, C_m\}$ 构成，其中每个约束 C_i 由变量元组 $(x_{i,1}, \dots, x_{i,k_i})$ 以及一个元数为 k_i 的关系对 $(P_i, Q_i) \in \Gamma$ 描述。若映射 $g\colon V \to D$ 满足 $(g(x_{i,1}) \dots, g(x_{i,k_i})) \in P_i$，我们称其强满足 C_i；若映射 $g'\colon V \to E$ 满足 $(g'(x_{i,1}) \dots, g'(x_{i,k_i})) \in Q_i$，则称其弱满足 C_i。注意，将任意映射 $g\colon V \to D$ 与 P_i 和 Q_i 之间所需的同态 h 复合，可得到映射 $g'\colon V \to E$，它弱满足所有被 g 强满足的约束。

考虑函数 $f\colon (0, 1) \to (0, 1)$，其中 $f(\epsilon) \to 0$ 为 $\epsilon \to 0$。如果存在一个算法 Alg 满足以下性质，我们称 PCSP(Γ) 具有损失为 f-鲁棒可解（简写为 f-鲁棒）：

- Alg 的输入是 PCSP(Γ) 的一个实例和一个阈值参数 $\epsilon \in (0, 1)$，并承诺存在一个映射 $g\colon V \to D$，能够强满足至少 $1 - \epsilon$ 比例的约束；
- Alg 输出映射 $g'\colon V \to E$ 的描述，该映射能够弱满足至少 $1 - f(\epsilon)$ 比例的约束；
- Alg 的运行时间关于实例的规模是多项式的。

有时我们会考虑 PCSP(Γ) 的加权 实例，其中约束集 $\mathcal{C}$ 配备了概率分布 $w\colon \mathcal{C} \to \mathbb{R}^+$。此时，鲁棒

[14]有时，将 PCSP 模板 Γ 表示为一对同态的关系结构 $(\mathbf{A}, \mathbf{B})$ 会更加方便，其中$\mathbf{A}$ 的域为 A，在 A 上具有关系 P_1, ..., P_t；而$\mathbf{B}$ 的域为 B，在 B 上具有关系Q_1, ..., Q_t。我们将交替采用这两种记法。

PCSP(Γ) 的可解性定义完全类似，只是它考虑的是满足的约束的总权重，而非其比例。

2.2 基本半定规划

设 D 是有限域，设 $P \subseteq D^k$，且设 $\epsilon \in [0,1]$。设 $N \in \mathbb{N}$ 是正整数。我们称 $\mathbb{R}^N$ 中由 $|D|k+1$ 个向量组成的元组（$\mathbf{v}_0, \{\mathbf{v}_{1,d} \colon d \in D\}, \ldots, \{\mathbf{v}_{k,d} \colon d \in D\}$）是到 P 的一个近似向量赋值，如果存在定义在 D^k 上的概率分布 μ，并满足以下性质。

$$\mu(P) \geq 1 - \epsilon, \tag{1}$$

$$\forall i \in [k], d \in D, \langle \mathbf{v}_0, \mathbf{v}_{i,d} \rangle = \sum_{\mathbf{a} \in D^k} \mathbf{1}[a_i = d]\mu(\mathbf{a}), \tag{2}$$

$$\forall i, i' \in [k], d, d' \in D, \langle \mathbf{v}_{i,d}, \mathbf{v}_{i',d'} \rangle = \sum_{\mathbf{a} \in D^k} \mathbf{1}[a_i = d]\mathbf{1}[a_{i'} = d']\mu(\mathbf{a}). \tag{3}$$

若 $D = \{-1, 1\}$，这等价于考察 $\mathbf{v}_i := \mathbf{v}_{i,1} - \mathbf{v}_{i,-1}$ 满足以下约束（例如，参见 [BGS25] 以了解论证）

$$\mu(P) \geq 1 - \epsilon, \tag{4}$$

$$\forall i \in [k], \langle \mathbf{v}_0, \mathbf{v}_i \rangle = \sum_{\mathbf{a} \in D^k} a_i \mu(\mathbf{a}), \tag{5}$$

$$\forall i, i' \in [k], \langle \mathbf{v}_i, \mathbf{v}_{i'} \rangle = \sum_{\mathbf{a} \in D^k} a_i a_{i'} \mu(\mathbf{a}). \tag{6}$$

给定一个定义在变量 $x_1, \ldots, x_n$ 和子句 $C_1, \ldots, C_m$ 上的 CSP(P) 实例，我们称由 $|D|n+1$ 个向量组成的元组 (v0, {v1,d : $d \in D$}, ..., {vn,d : $d \in D$}) 为基本半定规划解，若对每个 $j \in [m]$，都存在 D^k 上的概率分布 μ_j，使得对应于子句 C_j 中变量 $x_{j,1}, \ldots, x_{j,k_j}$ 的向量元组满足 (2) 和 (3)（或者等价地，在布尔情形下满足 (5) 和 (6)）。该半定规划解的值（或完备性）等于 $\frac{1}{m}\sum_{j=1}^{m} \mu_j(P)$。注意，对任意 $\epsilon > 0$，都可以在 [时间内将半定规划的最优值计算到加性误差 ϵ 以内，参见 GLS93, GM12].[15]。

当我们提到 PCSP(P, Q) 实例的半定规划松弛时，指的是将该实例视为 CSP(P) 实例时的半定规划松弛。谓词 Q 只在半定规划松弛的舍入 过程中出现，在此过程中，连续向量被转换为离散赋值。

给定一个部分约束满足问题模板 Γ 和一个 PCSP(Γ)的加权实例，我们类似地定义 PCSP(Γ) 实例的半定规划松弛，其中每个约束 C_j 都具有与(2)和(3)对应的约束 P_j (以及 C_j 的变量)。此外，CSP 的值为 $\sum_{j=1}^{m} w(C_j)\mu_j(P_j)$。

[15] Brakensiek、Guruswami 和 Sandeep [BGS25] 指出，找到这样的解有些微妙，因为约束 (5) 和 (6) 需要被精确满足。更详细的讨论请参阅他们论文完整版的附录 A。

2.3 多态性

给定一对谓词 $P \subseteq Q \subseteq D^k$，若算子 $f\colon D^L \to D$ 是 (P,Q) 的多态性，则称其为 (P,Q) 的多态性；如果对任意 $t^1,\dots,t^L \in P$，都有 $t \in Q$，其中对所有 $i \in [k]$，$t_i = f(t_i^1,\dots,t_i^L)$。我们用 $\mathrm{Pol}(P,Q)$ 表示 (P,Q) 的所有多态性构成的集合，其中 $\mathrm{Pol}^L(P,Q)$ 特指元数为 L 的多态性集合。

本文重点讨论几类常见的多态性。对于任意奇数 $L \in \mathbb{N}$，定义 MAJ_L、AT_L：$\{-1,1\}^L \to \{-1,1\}$ 为

$$\mathrm{MAJ}_L(x_1,\dots,x_L) := \mathbf{1}\left[\sum_{i=1}^{L} x_i \geq 0\right],$$
$$\mathrm{AT}_L(x_1,\dots,x_L) := \mathbf{1}\left[\sum_{i=1}^{L} (-1)^{i-1} x_i \geq 0\right].$$

记 $\mathrm{MAJ} := \{\mathrm{MAJ}_L : L \in \mathbb{N} \text{ 奇数}\}$ 以及 $\mathrm{AT} := \{\mathrm{AT}_L : L \in \mathbb{N}\text{奇数}\}$。例如，$\mathrm{MAJ} \subseteq \mathrm{Pol}(P, Q)$ 表示 $\mathrm{Pol}(P, Q)$ 具有所有奇数元数的多数多态，实际上还具有所有折叠（即无偏）加权阈值函数作为多态 [BGS23]。

2.4 分析事实

记 $\mathcal{N}(a, b)$ 为均值为 a、方差为 b（即标准差为 $\sqrt{b}$）的正态分布。同理，给定 $\boldsymbol{\mu} \in \mathbb{R}^n$ 和 $\Sigma \in \mathbb{R}^{n\times n}$，记 $\mathcal{N}(\boldsymbol{\mu}, \Sigma)$ 为均值为 $\boldsymbol{\mu}$、协方差为 Σ 的 n 元正态分布。我们引用以下关于正态分布的标准事实。

Pr命题 2.1（例如，[Ver18], [BGS25]）。设 X 服从 $\mathcal{N}(\mu, \sigma^2)$。那么

(a) 对于任意区间 $[a,b] \subseteq \mathbb{R}$，概率$[X \in [a,b]] \leq \frac{b-a}{2\sigma}$。
(b) 对于任意 $t \geq 0$，概率$[X \geq t+\mu] \leq e^{-\frac{t^2}{2\sigma^2}}$。

命题 2.2（例如，[Ver18], [BGS25]）。设 x 是一个均值为零、方差为一的高斯变量。那么对于所有 $t \geq 0$

1. $P(x \geq t) \leq \frac{1}{2}e^{-\frac{t^2}{2}}$。2. $P(t \leq x \leq 2t) \leq \frac{t}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}$。3. 对所有 $a \in \mathbb{R}$、$P(|x-a| \leq t) \leq \frac{2t}{\sqrt{2\pi}} \leq t$。4. 给定 $I \subseteq [t,\infty)$、$P(x \in I) \leq |I|e^{-\frac{t^2}{2}}$。

Proof. Observe that $P(x \geq t) = \int_t^\infty \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}}dx = \int_0^\infty \frac{e^{-\frac{(y+t)^2}{2}}}{\sqrt{2\pi}}dy \leq e^{-\frac{t^2}{2}}\int_0^\infty \frac{e^{-\frac{y^2}{2}}}{\sqrt{2\pi}}dy = \frac{1}{2}e^{-\frac{t^2}{2}}$, $P(t \leq x \leq 2t) = \int_t^{2t} \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}}dx \leq \frac{t}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}$, and $P(|x-a| \leq t) = \int_{a-t}^{a+t} \frac{e^{-\frac{x^2}{2}}}{\sqrt{2\pi}}dx \leq \frac{2t}{\sqrt{2\pi}}$. □

我们还将使用以下关于矩阵$X \sim \mathcal{N}(\mathbf{0}, I_n)$平方范数的集中界，该界可由卡方分布集中性的 Laurent–Massart 界推得。

命题 2.3 ([LM00])。 设 X 服从分布 $X \sim \mathcal{N}(0_n, I_n)$。那么，对于每个 $\alpha \in \mathbb{R}$，都有

$$\Pr(\|X\|^2 \in [n - 2n^{1/2+\alpha}, n + 2n^{1/2+\alpha} + 2n^{\alpha}]) \geq 1 - e^{-n^{\alpha}}.$$

3 交替阈值多态性的整数间隙

3.1 尝试构造的整数间隙实例

在给出完整分析之前，我们先介绍一个简单的尝试构造的整数间隙实例。它虽然行不通，但体现了我们构造整数间隙实例的直观思路。

设 $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3$ 是三个与 $\mathbf{v}_0$ 正交的单位向量，满足 $\mathbf{w}_1 + \mathbf{w}_2 + \mathbf{w}_3 = 0$。例如，可以取 $\mathbf{v}_0 = (1, 0, 0)$、$\mathbf{w}_1 = (0, 1, 0)$、$\mathbf{w}_2 = (0, -\frac{1}{2}, \frac{\sqrt{3}}{2})$，以及 $\mathbf{w}_3 = (0, -\frac{1}{2}, -\frac{\sqrt{3}}{2})$。

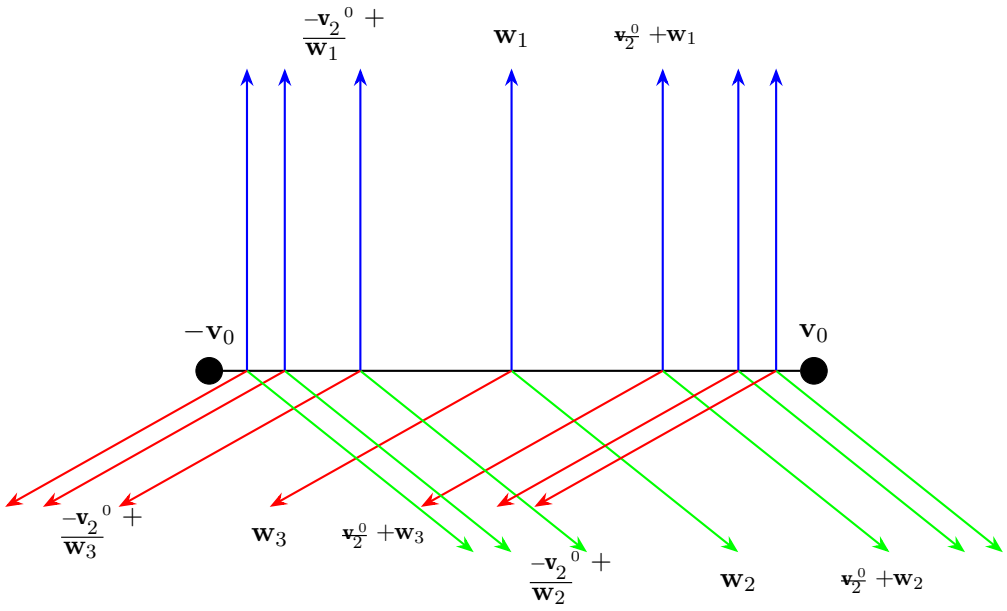
设 $k_0 = \lceil \log_2(n) \rceil$。假设我们有这些向量

$$\{(1-2^{-k})\mathbf{v}_0 + \mathbf{w}_i : k \in \{0, 1, \ldots, k_0\}, i \in [3]\} \bigcup \{-(1-2^{-k})\mathbf{v}_0 + \mathbf{w}_i : k \in \{1, 2, \ldots, k_0\}, i \in [3]\}$$

此外，以下两种情况之一成立

1. $(1 - 2^{-k_0})\mathbf{v}_0 + \mathbf{w}_i$ 对所有 $i \in [3]$， $-(1 - 2^{-k_0})\mathbf{v}_0 + \mathbf{w}_i$ 均舍入为 1。 2. $(1 - 2^{-k_0})\mathbf{v}_0 + \mathbf{w}_i$ 对所有 $i \in [3]$ 均舍入为 -1，并且对所有 $i \in [3]$， $-(1 - 2^{-k_0})\mathbf{v}_0 + \mathbf{w}_i$ 均舍入为 1。

当 $k_0 = 3$ 时，请参见下图了解这组向量。



若是如此，则考虑以下三元组

$$\{(b(1-2^{-k})\mathbf{v}_0+\mathbf{w}_i, b(1-2^{-k})\mathbf{v}_0+\mathbf{w}_{i'}, -b(1-2^{1-k})\mathbf{v}_0+\mathbf{w}_{i''})\}$$

其中 $k\in[k_0]$、 $b\in\{-1,1\}$ 和 i,i',i'' 是 $[3]$ 中互不相同的元素。每个这样的三元组中的向量之和为$\mathbf{v}_0$ 或 $-\mathbf{v}_0$，因此，对于每个这样的三元组，我们都可以针对这些向量或其否定添加一个 1-in-3-SAT 约束。然而，不难证明，所得的 NAE-SAT 约束中至少有一个必定不满足。

为说明这一点，假设所有 NAE 约束都得到满足。不失一般性，我们可以假设，对于所有 $i\in[3]$，$(1-2^{-k_0})\mathbf{v}_0+\mathbf{w}_i$ 都被舍入为 1；对于所有 $i\in[3]$，$(1-2^{-k_0})\mathbf{v}_0+\mathbf{w}_i$ 都被舍入为 -1。现在我们作如下观察：

1. 对于所有 $i\in[3]$，$(1-2^{-k_0})\mathbf{v}_0+\mathbf{w}_i$ 都被舍入为 1。

2. 由于三元组上有 NAE-SAT 约束

   $$((-1)^{k_0-k}(1-2^{-k})\mathbf{v}_0+\mathbf{w}_i, (-1)^{k_0-k}(1-2^{-k})\mathbf{v}_0+\mathbf{w}_{i'}, (-1)^{k_0-k+1}(1-2^{1-k})\mathbf{v}_0+\mathbf{w}_{i''})$$

   使得 i，i'，i'' 是 $[3]$, 的不同元素；如果 $(-1)^{k_0-k}(1-2^{-k})\mathbf{v}_0+\mathbf{w}_i$ 对所有 $i\in[3]$ 都舍入为 $(-1)^{k_0-k}$，那么 $(-1)^{k_0-k+1}(1-2^{1-k})\mathbf{v}_0+\mathbf{w}_i$ 对所有 $i\in[3]$ 都必须舍入为 $(-1)^{k_0-k+1}$。

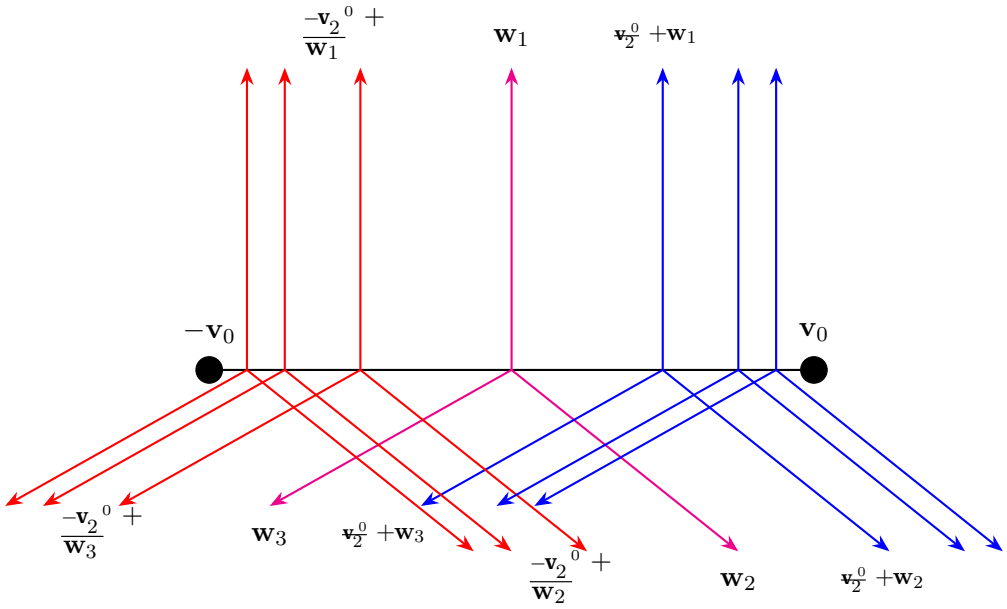
3. $-(1-2^{-k_0})\mathbf{v}_0+\mathbf{w}_i$ 对所有 $i\in[3]$ 都舍入为 -1。

4. 由于三元组上有 NAE-SAT 约束

   $$((-1)^{k_0-k+1}(1-2^{-k})\mathbf{v}_0+\mathbf{w}_i, (-1)^{k_0-k+1}(1-2^{-k})\mathbf{v}_0+\mathbf{w}_{i'}, (-1)^{k_0-k}(1-2^{1-k})\mathbf{v}_0+\mathbf{w}_{i''})$$

   使得 i，i'，i'' 是 $[3]$, 的不同元素；如果 $(-1)^{k_0-k+1}(1-2^{-k})\mathbf{v}_0+\mathbf{w}_i$ 对所有 $i\in[3]$ 都舍入为 $(-1)^{k_0-k+1}$，那么 $(-1)^{k_0-k}(1-2^{1-k})\mathbf{v}_0+\mathbf{w}_i$ 对所有 $i\in[3]$ 都必须舍入为 $(-1)^{k_0-k}$。

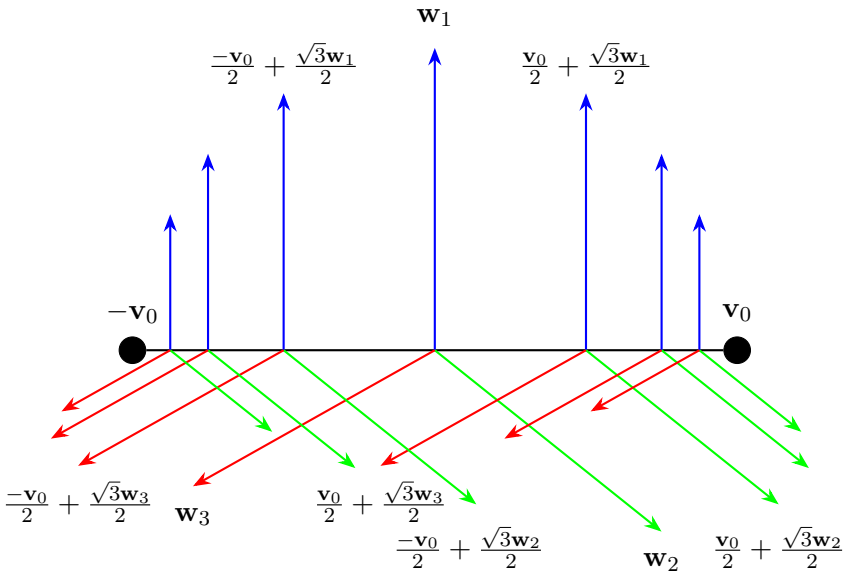
综合这些观察可知，对于所有 $k\in[k_0+1]$，$(-1)^{k_0-k+1}(1-2^{1-k})\mathbf{v}_0+\mathbf{w}_i$都必须舍入为 $(-1)^{k_0-k+1}$，对所有 $i\in[3]$ 均如此；而 $(-1)^{k_0-k}(1-2^{1-k})\mathbf{v}_0+\mathbf{w}_i$ 都必须舍入为 $(-1)^{k_0-k}$，对所有 $i\in[3]$ 均如此。代入 $k=1$ 后可知，$\mathbf{w}_1$, $\mathbf{w}_2$, 和 $\mathbf{w}_3$ 都必须同时舍入为 1 和 -1，这就产生了矛盾。下图展示了这一论证，其中蓝色表示应舍入为 1 的向量，红色表示应舍入为 -1 的向量。



这个尝试构造的整数间隙实例的问题在于，这些向量不是单位向量。若要使它们成为单位向量，我们需要这些向量

$$\{b(1-2^{-k})\mathbf{v}_0 + \sqrt{2^{1-k}-2^{-2k}}\mathbf{w}_i : k \in \{0,1,\ldots,k_0\}, b \in \{-1,1\}, i \in [3]\},$$

如下面的图所示。然而，我们不能再对这些向量施加 1-in-3-SAT 约束。为处理这一问题，我们将考虑形如 $b(1-2^{-k})\mathbf{v}_0 + \sqrt{2^{1-k}-2^{-2k}}\mathbf{w}$ 的向量，其中 $b \in \{-1,1\}$ 和 $||\mathbf{w}|| \approx 1$，并证明可以使用类似的论证。



3.2 连续整数间隙实例

现在我们将介绍对上述失败的整数间隙实例进行的一种自然修改，由此得到一个候选整数性间隙实例，其中包含无穷多个变量和约束。

随后，我们还将进一步修改这个整数性间隙实例，使其离散化，并改用多元高斯向量而非单位向量，因为多元高斯向量更易于分析，而且当维度足够高时，经过适当缩放后，它们与单位向量十分接近。

令 $k_0 = \lceil \log(\frac{1}{\epsilon}) \rceil + 20$。我们将在 $\mathbb{R}^{d+1}$ 中进行，其中 $\mathbf{v}_0 = \mathbf{e}_{d+1}$ 与 $\mathbb{R}^d$ 正交，而 d 将在稍后选定。

定义 3.1。令 A_x 为点 $\{x\mathbf{v}_0 + \sqrt{1-x^2}\mathbf{w} : \mathbf{w} \in S^{d-1}\}$ 的集合。

定义 3.2。对于每个形如 $1 - 2^{-k}$ 且满足 $k \in [k_0]$ 的 x，

1. 我们将 T_x 定义为满足 $p_1 + p_2 + p_3 = 0$、$p_1, p_2 \in A_x$ 和 $p_3 \in A_{1-2x}$ 的点三元组 (p_1, p_2, p_3) 的集合。*2.* 类似地，我们将 T_{-x} 定义为满足 $p_1 + p_2 + p_3 = 0$、$p_1, p_2 \in A_{-x}$ 和 $p_3 \in A_{2x-1}$ 的点三元组 (p_1, p_2, p_3) 的集合。

我们的候选整数性间隙实例如下：

1. 对于每个 $k \in [k_0]$，令 $x = 1 - 2^{-k}$，我们以 $\frac{1}{2(k_0+1)}$ 的概率从 T_x 中随机选取一个三元组，并以 $\frac{1}{2(k_0+1)}$ 的概率从 T_{-x} 中随机选取一个三元组。

2. 令 $x_0 = 1 - 2^{-k_0}$。以 $\frac{1}{2(k_0+1)}$ 的概率，我们随机选取一个 $\mathbf{p} \in A_{x_0}$，并取三元组 $(-v_0, -v_0, \mathbf{p})$。类似地，以 $\frac{1}{2(k_0+1)}$ 的概率，我们随机选取一个 $\mathbf{p} \in A_{-x_0}$，并取三元组 $(v_0, v_0, \mathbf{p})$。

直观来说，这是一个间隙实例，因为半定规划认为几乎所有约束都可以满足，但在任何实际赋值中，以下情况必有一种发生，从而导致至少 $\frac{\delta}{16(k_0+1)}$ 的 NAE-SAT 约束被违反，其中 $\delta > 0$ 是一个我们稍后会选定的绝对常数。不失一般性，我们可以假设 $\mathbf{v}_0$ 被舍入为 1，而 $-\mathbf{v}_0$ 被舍入为 -1。

1. $\mathbf{p}$ 中有 δ 比例的变量被赋值为 -1，这意味着三元组（$-v_0$、$-v_0$、$\mathbf{p}$）中有 δ 全部为 -1。2. $\mathbf{p}$ 中有 δ 比例的变量被赋值为 1，这意味着三元组（v_0、v_0、$\mathbf{p}$）中有 δ 全部为 1。3. 对于某个 $k \in [k_0]$，令 $x = 1 - 2^{-k}$，A_x 中被赋值为 -1 的向量少于 δ，而 A_{1-2x} 中被赋值为 1 的向量至少有 δ，这意味着三元组（$\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3$）中至少有 $\frac{\delta}{8}$ 个 $\in T_x$ 全部为 1。4. 对于某个 $k \in [k_0]$，令 $x = 1 - 2^{-k}$，A_{-x} 中被赋值为 1 的向量少于 δ，而 A_{1-2x} 中被赋值为 -1 的向量至少有 δ，这意味着三元组（$\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3$）中至少有 $\frac{\delta}{8}$ 个 $\in T_{-x}$ 全部为 -1。

在修改我们的整数性间隙实例并使这一直觉严格化之前，我们给出 T_x 中点三元组的更精确描述。

命题3.3. 如果$p_1,p_2 \in A_x$且$p_3 \in A_{1-2x}$，则$p_1+p_2+p_3=v_0$当且仅当$p_3=(1-2x)v_0+\sqrt{1-(2|x|-1)^2}w$，$p_1=xv_0+\sqrt{1-x^2}\left(-\frac{\sqrt{1-(2|x|-1)^2}}{2\sqrt{1-x^2}}w+\sqrt{1-\frac{1-(2|x|-1)^2}{4(1-x^2)}}u\right)$，且$p_2=xv_0+\sqrt{1-x^2}\left(-\frac{\sqrt{1-(2|x|-1)^2}}{2\sqrt{1-x^2}}w-\sqrt{1-\frac{1-(2|x|-1)^2}{4(1-x^2)}}u\right)$，对某些$w、u \in S^{d-1}$使得$w \cdot u=0$。

证明。假设 $\mathrm{p}_1,\mathrm{p}_2 \in A_x$、$\mathrm{p}_3 \in A_{1-2x}$和 $\mathrm{p}_1+\mathrm{p}_2+\mathrm{p}_3=\mathrm{v}_0$。由于 $\mathrm{p}_3 \in A_{1-2x}$，$\mathrm{p}_3=(1-2x)\mathrm{v}_0+\sqrt{1-(2|x|-1)^2}\mathrm{w}$，其中某个 $\mathrm{w} \in S^{d-1}$。现在写作 $\mathrm{p}_1=x\mathrm{v}_0+a\mathrm{w}+b\mathrm{u}$，其中 $\mathrm{u} \in S^{d-1}$，$\mathrm{w} \cdot \mathrm{u}=0$，且 $b \geq 0$。我们现在作如下观察：

1. 由于 $\mathbf{p}_1+\mathbf{p}_2+\mathbf{p}_3=\mathbf{v}_0, \mathbf{p}_2=x\mathbf{v}_0-\left(a+\sqrt{1-(2|x|-1)^2}\right)\mathbf{w}-b\mathbf{u}$。

2. 由于 $||\mathbf{p}_1||^2=||\mathbf{p}_2||^2, a^2=\left(a+\sqrt{1-(2|x|-1)^2}\right)^2$ 这意味着 $a=-\frac{1}{2}\sqrt{1-(2|x|-1)^2}$。

3. 由于 $||\mathbf{p}_1||^2=1, b=\sqrt{1-x^2-a^2}=\sqrt{1-x^2-\frac{1-(2|x|-1)^2}{4}}$。

另一个方向很容易直接验证。 □

基于此，我们定义如下噪声系数 ρ_x。

定义3.4。我们定义 $\rho_x=\frac{\sqrt{1-(2|x|-1)^2}}{2\sqrt{1-x^2}}$。

Observe that if $|x|=1-2^{-k}$ and k is large then $\rho_x=\frac{\sqrt{1-(2|x|-1)^2}}{2\sqrt{1-x^2}} \approx \frac{\sqrt{2^{2-k}}}{2\sqrt{2^{1-k}}}=\frac{1}{\sqrt{2}}$.

3.3 离散化整性间隙实例

现在，我们对候选整数性间隙实例进行修改，使其使用多元高斯向量而非单位向量，并将其离散化。

定义 3.5. 给定 $x \in [-1,1]$，我们将 A'_x 定义为通过对$\mathbf{w} \sim \mathcal{N}(0,1/d)^d$进行采样并取向量 $x\mathbf{v}_0+\sqrt{1-x^2}\mathbf{w}$所得到的向量分布。

定义 3.6. 给定 $x \in [-1,1]$，我们将 T'_x 定义为通过对$\mathbf{u}$、$\mathbf{w} \sim \mathcal{N}(0,1/d)^d$进行采样，然后取$(\mathbf{p}_1,\mathbf{p}_2,\mathbf{p}_3)$的三点组分布$\mathbf{p}_3=(1-2x)\mathbf{v}_0+\sqrt{1-(2|x|-1)^2}\mathbf{w}$,
$\mathbf{p}_1=x\mathbf{v}_0+\sqrt{1-x^2}\left(-\frac{\sqrt{1-(2|x|-1)^2}}{2\sqrt{1-x^2}}\mathbf{w}+\sqrt{1-\frac{1-(2|x|-1)^2}{4(1-x^2)}}\mathbf{u}\right)$，以及
$\mathbf{p}_2=x\mathbf{v}_0+\sqrt{1-x^2}\left(-\frac{\sqrt{1-(2|x|-1)^2}}{2\sqrt{1-x^2}}\mathbf{w}-\sqrt{1-\frac{1-(2|x|-1)^2}{4(1-x^2)}}\mathbf{u}\right)$。

类似地，我们将 T'_{-x} 定义为通过对 $(\mathbf{p}_1,\mathbf{p}_2,\mathbf{p}_3)$ 进行采样而得到的点三元组分布：先采样 $\mathbf{u}$、$\mathbf{w} \sim \mathcal{N}(0、1/d)^d$，然后取 $\mathbf{p}_3=(2x-1)\mathbf{v}_0+\sqrt{1-(2|x|-1)^2}\mathbf{w}$,
$\mathbf{p}_1=-x\mathbf{v}_0+\sqrt{1-x^2}\left(-\frac{\sqrt{1-(2|x|-1)^2}}{2\sqrt{1-x^2}}\mathbf{w}+\sqrt{1-\frac{1-(2|x|-1)^2}{4(1-x^2)}}\mathbf{u}\right)$, *and*
$\mathbf{p}_2=-x\mathbf{v}_0+\sqrt{1-x^2}\left(-\frac{\sqrt{1-(2|x|-1)^2}}{2\sqrt{1-x^2}}\mathbf{w}-\sqrt{1-\frac{1-(2|x|-1)^2}{4(1-x^2)}}\mathbf{u}\right)$.

修改后的整数性间隙实例如下：

1. 对于每个 $k \in [k_0]$，令 $x = 1 - 2^{-k}$，我们以概率 $\frac{1}{2(k_0+1)}$从 T'_x 中采样一个三元组，并以概率 $\frac{1}{2(k_0+1)}$从 T'_{-x} 中采样一个三元组。

2. 令 $x_0 = 1 - 2^{-k_0}$。以 $\frac{1}{2(k_0+1)}$ 的概率，我们从 A'_{x_0} 中采样一个向量 $\mathbf{p}$，并取三元组 $(-v_0, -v_0, \mathbf{p})$。类似地，以 $\frac{1}{2(k_0+1)}$ 的概率，我们从A'_{-x_0}中采样一个向量 $\mathbf{p}$，并取三元组 $(v_0, v_0, \mathbf{p})$。

3. 丢弃满足以下任一条件的三元组：

   (a) 当我们从 $\mathcal{N}(0, 1/d)^d$ 中采样 $\mathbf{w}$ 时，$|(||\mathbf{w}||^2 - 1)| > \frac{\epsilon}{1000}$；(b) 当我们从 $\mathcal{N}(0, 1/d)^d$ 中采样 $\mathbf{u}$ 时，或者 $|(||\mathbf{u}||^2 - 1)| > \frac{\epsilon}{1000}$，或者 $|\mathbf{w} \cdot \mathbf{u}| > \frac{\epsilon}{1000}$。

4. 我们通过将 $\mathbb{R}^{d+1}$ 中长度至多为 2 的向量集合划分为半径至多为 $\frac{\epsilon}{1000}$ 的区域，并为每个区域选取一个与该区域内所有点的距离均不超过$\frac{\epsilon}{1000}$ 的中心，来离散化该实例。我们还为包含长度大于 2 的向量的区域选取一个中心（该中心可以任意选取，因为只有被丢弃的点三元组才会包含属于此区域的向量）。随后，我们将所有向量替换为其所在区域的中心。

定理 3.7。对于所有 $\epsilon > 0$，如果 $d \geq \frac{80000000}{\epsilon^3}$ 则比上述整数性间隙实例（第3.3节）

1. 存在一个半定规划的解，使每个未被丢弃的约束都至少获得 $1 - \epsilon$ 的值。*2.* 被抽样的约束中，至多有 $6e^{-\frac{10}{\epsilon}}$ 被丢弃。*3.* 所有赋值至少违反 $\frac{1}{10^{60\lceil log(\frac{1}{\epsilon})\rceil}}$ 个抽样得到的 *NAE-SAT* 约束（包括已被丢弃的约束）。

根据 Raghavendra 定理 [Rag08], ，这个整数间隙立即推出 UGC 困难性。

推论 3.8。假设唯一博弈猜想成立，对于所有 ϵ 使得 $0 < \epsilon \leq \frac{1}{100}$，fiPCSP(*1-in-3-SAT*、*NAE-SAT*)不是$(\epsilon, 1 - 10^{61}\log(1/\epsilon))$-鲁棒的。

定理3.7第一条陈述的证明思路：对于每个非外部区域的中心向量$\mathbf{v}$，我们可以取向量$\mathbf{v}' = \sqrt{1 - \frac{\epsilon}{4}}\frac{\mathbf{v}}{||\mathbf{v}||} + \frac{\sqrt{\epsilon}}{2}\mathbf{z}_v$，其中$\mathbf{z}_v$ 与其他所有向量正交。我们将$\mathbf{v}_0$ 赋值给其自身。

为了证明这给出了一个有效的半定规划解，并且对每个未被舍弃的约束，其值至少为 $1 - \epsilon$，我们首先注意到，对于每组三个单位向量$\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$，只要$\mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3 = \pm\mathbf{v}_0$，就存在一个概率为 D 的概率分布，该分布定义在对应约束的满足赋值上，使得

1. 对所有 $i \in [3]$, $\mathbb{E}_D[x_i] = \mathbf{v}_i \cdot \mathbf{v}_0$。

2. 对所有互不相同的 $i, j \in [3]$, $\mathbb{E}_D[x_i x_j] = \mathbf{v}_i \cdot \mathbf{v}_j$。

接下来我们注意到，若 $\mathbf{v}_1'$、$\mathbf{v}_2'$ 和 $\mathbf{v}_3'$ 是与 $\mathbf{v}_1$, $\mathbf{v}_2$, 和 $\mathbf{v}_3$ 接近的单位向量，那么就存在一个伪分布 D'（它可能会对某些赋值 $(x_1, x_2, x_3) \in \{-1, 1\}^3$赋予负概率），使其与 D 接近，并且

1. 对所有 $i \in [3]$, $\mathbb{E}_{D'}[x_i] = \mathbf{v}_i' \cdot \mathbf{v}_0$。 2. 对所有互不相同的 $i, j \in [3]$, $\mathbb{E}_{D'}[x_i x_j] = \mathbf{v}_i' \cdot \mathbf{v}_j'$。

最后，我们注意到，将每个向量 $\mathbf{v}$ 替换为 $\sqrt{1 - \frac{\epsilon}{4}}\,\mathbf{v} + \frac{\sqrt{\epsilon}}{2||\mathbf{v}||}\mathbf{z}_{\mathbf{v}}$，会通过将每个概率 p 替换为 $(1 - \frac{\epsilon}{4})p + \frac{\epsilon}{32}$ 来修改每个伪分布 D'，这足以使所有概率均非负。

□

完整的 第一条定理的证明细节 3.7 见附录 A .

定理第二条结论的证明 *3.7*: 我们可以使用切尔诺夫界证明定理3.7 的第二条结论。为保证完整性，我们在附录 A中给出这些界的证明。

引理 3.9。 以下尾界成立：

1. 对所有 $t \in [0, 1]$，若$\mathbf{w} \sim \mathcal{N}(0, 1/d)^d$，则 $P\left(|(||\mathbf{w}||^2 - 1)| \geq t\right) \leq 2e^{-\frac{dt^2}{8}}$。*2.* 给定一个向量$\mathbf{w}$，对所有 $t \geq 0$，若$\mathbf{u} \sim \mathcal{N}(0, 1/d)^d$与$\mathbf{w}$独立，则 $P(|\mathbf{w} \cdot \mathbf{u}| \geq t) \leq 2e^{-2||\mathbf{w}||^2 t}$。

根据引理 3.9，由于 $d \geq \frac{80000000}{\epsilon^3}$，若 $\mathbf{w}$ 和 $\mathbf{u}$ 独立地从 $\mathcal{N}(0, 1/d)^d$中抽取，则

1. $P(|(||\mathbf{w}||^2 - 1)| \geq \frac{\epsilon}{1000}) = P(|(||\mathbf{u}||^2 - 1)| \geq \frac{\epsilon}{1000}) \leq 2e^{-\frac{10}{\epsilon}}$
2. 只要 $||\mathbf{w}|| \leq 2$, $P(|\mathbf{w} \cdot \mathbf{u}| \geq \frac{\epsilon}{1000}) \leq 2e^{-\frac{10}{\epsilon}}$。

因此，丢弃的约束所占比例至多为 $6e^{-\frac{10}{\epsilon}}$。 □

3.4 可靠性分析

现在我们证明定理 3.7的第三个结论。为此，我们将对整数间隙实例中各点的赋值视为一个映射 $f\colon \mathbb{R}^{d+1} \to \{-1, 1\}$ 其中 $f(\mathbf{v})$ 是赋给与区域中心对应的点的值，而该区域 $\mathbf{v}$ 包含此点。

定义 3.10。 给定一个映射 $f\colon \mathbb{R}^{d+1} \to \{-1, 1\}$，对于每个向量 $\mathbf{w} \in \mathbb{R}^d$，我们定义 $f_x(\mathbf{w})$为赋给 $\mathbf{p} = x\mathbf{v_0} + \sqrt{1 - x^2}\mathbf{w}$的值。

定义 3.11。 给定 $\rho \in [-1, 1]$ 和函数 $f\colon \mathbb{R}^d \to \mathbb{R}$，我们定义

$$(N_\rho f)(\mathbf{x}) = E_{\mathbf{y} \sim \mathcal{N}(0,1/d)^d}[f(\rho\mathbf{x} + \sqrt{1 - \rho^2}\mathbf{y})].$$

定理 3.7 的第三个陈述可由以下引理推出。

引理 3.12. 对于所有 $\delta \in [0, 10^{-55}]$，如果存在一个 $x = 1 - 2^k$，使得 $E_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[f_x(\mathbf{w})] > 1 - 2\delta$ 但 $E_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[f_{1-2x}(\mathbf{w})] \geq 2\delta - 1$，那么 T'_x 中单色三元组$(\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3)$的比例至少为 $\frac{\delta}{8}$。

证明。假设这不为真。注意到，每当 $f_{1-2x}(\mathbf{w}) = 1$时，三元组$(\mathbf{p}_1,\mathbf{p}_2,(1-2x)\mathbf{v}_0 + \sqrt{1-(2|x|-1)^2}\mathbf{w})$中单色三元组的比例至少为

$$1 - 2P_{\mathbf{w}'\sim\mathcal{N}(0,1/d)^d}(f_x(\rho_x\mathbf{w} + \sqrt{1-\rho_x^2}\mathbf{w}') = -1) = (N_{\rho_x}f_x)(-\mathbf{w}).$$

由于 $\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[f_{1-2x}(\mathbf{w})] \geq 2\delta - 1$，$f_{1-2x}(\mathbf{w}) = 1$ 对至少 δ 比例的$\mathbf{w}$成立。这意味着，为了避免出现 $\frac{\delta}{8}$ 比例的单色三元组，我们必须有$(N_{\rho_x}f_x)(-\mathbf{w}) < \frac{1}{4}$对至少 $\frac{\delta}{2}$ 比例的$\mathbf{w} \sim \mathcal{N}(0, 1/d)^d$成立。我们现在证明这不可能发生。为此，我们写出$f_x = \mathbb{E}[f_x] + f'_x$，并证明 $||(N_{\rho_x}f'_x)||^2$很小。

引理 3.13. 对所有 $t \in \mathbb{N}$，若 $\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[f_x(\mathbf{w})] > 1 - 2\delta$ 则

$$\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[(N_{\rho_x}f'_x)(\mathbf{w})^2] \leq 10(3^t)\delta^{\frac{3}{2}} + 4\rho_x^{2t}\delta$$

证明。设 $S = \{\mathbf{w} \in \mathbb{R}^d : f_x(\mathbf{w}) = -1\}$，并设 $\delta' = \mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[1_{\mathbf{w}\in S}] < \delta$为随机 $\mathbf{w} \sim \mathcal{N}(0, 1/d)^d$ 时 $f_x(\mathbf{w}) = -1$ 的概率。令 $\{h_i : i \in \mathbb{N}\cup\{0\}\}$ 为厄米特多项式，我们可以写成 $f_x = (1-2\delta') + f'_{x,\ low} + f'_{x,\ high}$，其中 $f'_{x,\ low}$ 是多项式 $\{\prod_{j=1}^d h_{i_j}(\sqrt{d}w_j) : 1 \leq \sum_{j=1}^d i_j \leq t\}$ 的线性组合（即在分布$\mathcal{N}(0, 1/d)^d$下正交的、次数介于 1 与 t 之间的广义多元厄米特多项式），而 $f'_{x,\ high} = f_x - (1-2\delta') - f'_{x,\ low}$ 是多项式$\{\prod_{j=1}^d h_{i_j}(\sqrt{d}w_j) : t+1 \leq \sum_{j=1}^d i_j \leq deg(f_x)\}$ 的线性组合。

我们注意到，如果有一个界 $\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[f'_{x,low}(\mathbf{w})^2] \leq B$，那么就可以得出以下结论。

1. 正如 Ryan O'Donnell 的教材《布尔函数分析》第 9 章所述，[O'D14], Bonami 引理（超收缩定理的一个特例）指出，若 p 是一个次数至多为 t 的多项式，则 $\mathbb{E}_{\mathbf{x}\in\{-1,1\}^n}[p(\mathbf{x})^4] \leq 9^t\left(\mathbb{E}_{\mathbf{x}\in\{-1,1\}^n}[p(\mathbf{x})^2]\right)^2$。Gross [Gro75], 指出，由于高斯输入可以用大量布尔变量的线性组合来近似，因此超收缩定理（尤其是 Bonami 引理）既适用于高斯输入，也适用于布尔输入。换言之，$\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[p(\mathbf{w})^4] \leq 9^t\left(\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[p(\mathbf{w})^2]\right)^2$。因此，$\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[(f'_{x,low}(\mathbf{w}))^4] \leq 9^tB^2$，这意味着$\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d:f_x(\mathbf{w})=-1}[|f'_{x,low}(\mathbf{w})|] \leq \sqrt[4]{\frac{9^tB^2}{\delta'}}$。关于 Bonami 引理和超收缩定理的历史讨论，请参见 O'Donnell 的书第 9.7 章 [O'D14]。

2. 对所有满足 $f_x(\mathbf{w}) = -1$, $f'_{x,high}(\mathbf{w}) = 2\delta' - 1 - f'_{x,low}(\mathbf{w})$ 的 $\mathbf{w} \in S^{d-1}$。这意味着

$$\begin{aligned}\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d:f_x(\mathbf{w})=-1}[f'_{x,low}(\mathbf{w})f'_{x,high}(\mathbf{w})] &= \mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d:f_x(\mathbf{w})=-1}[(2\delta'-1)f'_{x,low}(\mathbf{w}) - f'_{x,low}(\mathbf{w})^2] \\ &\leq \sqrt[4]{\frac{9^tB^2}{\delta'}} - \mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d:f_x(\mathbf{w})=-1}[f'_{x,low}(\mathbf{w})^2]\end{aligned}$$

3. 对所有满足 $f_x(\mathbf{w}) = 1$, $f'_{x,high}(\mathbf{w}) = 2\delta' - f'_{x,low}(\mathbf{w})$ 的 $\mathbf{w} \in S^{d-1}$。这意味着

$$\begin{aligned}\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d:f_x(\mathbf{w})=1}[f'_{x,low}(\mathbf{w})f'_{x,high}(\mathbf{w})] &= \mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d:f_x(\mathbf{w})=1}[2\delta' f'_{x,low}(\mathbf{w}) - f'_{x,low}(\mathbf{w})^2] \\ &\le 2(\delta')^2 - \frac{1}{2}\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d:f_x(\mathbf{w})=1}[f'_{x,low}(\mathbf{w})^2]\end{aligned}$$

其中，该不等式利用了如下观察：

$$2\delta' f'_{x,low}(\mathbf{w}) - f'_{x,low}(\mathbf{w})^2 = 2\delta'^2 - \frac{1}{2}\left(2\delta' - f'_{x,low}(\mathbf{w})\right)^2 - \frac{1}{2}f'_{x,low}(\mathbf{w})^2 \le 2\delta'^2 - \frac{1}{2}f'_{x,low}(\mathbf{w})^2$$

4. 综合这些观察，

$$\begin{aligned}0 = \mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[f'_{x,low}(\mathbf{w})f'_{x,high}(\mathbf{w})] &= \delta'\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d:f_x(\mathbf{w})=-1}[f'_{x,low}(\mathbf{w})f'_{x,high}(\mathbf{w})] \\ &\quad + (1-\delta')\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d:f_x(\mathbf{w})=-1}[f'_{x,low}(\mathbf{w})f'_{x,high}(\mathbf{w})] \\ &\le \delta'\sqrt[4]{\frac{9^t B^2}{\delta'}} + 2(\delta')^2 - \frac{1}{2}\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[f'_{x,low}(\mathbf{w})^2]\end{aligned}$$

这意味着

$$\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[f'_{x,low}(\mathbf{w})^2] \le 2\left(\sqrt[4]{9^t(\delta')^3B^2} + 2(\delta')^2\right)$$

因此，若 $B > 2\sqrt[4]{9^t(\delta')^3B^2} + 4(\delta')^2$，那么我们可以改进关于 $\mathbb{E}_{\mathbf{w}\in S^{d-1}}[f'_{x,low}(\mathbf{w})^2]$ 的界。令 B^* 为我们所能得到的界的下确界，则必有 $B^* = 2\sqrt[4]{9^t(\delta')^3(B^*)^2} + 4(\delta')^2$。解出 $\sqrt{B^*}$ 得到

$$\sqrt{B^*} = \sqrt[4]{C(\delta')^3} + \sqrt{\sqrt{9^t(\delta')^3} + 4(\delta')^2} \le \max\left\{3\sqrt[4]{9^t(\delta')^3}, 3\delta'\right\} \le 3\sqrt[4]{9^t(\delta')^3}$$

其中，第一个不等式是通过考察 $4(\delta')^2 \le 3\sqrt{9^t(\delta')^3}$ 或 $4(\delta')^2 > 3\sqrt{9^t(\delta')^3}$ 得出的。因此，$\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[f'_{x,low}(\mathbf{w})^2] \le 10\sqrt{9^t\delta^3}$，这意味着 $\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[(N_{\rho_x}f'_{x,low})(\mathbf{w})^2] \le 10\sqrt{9^t\delta^3}$。

由于 $\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,\ 1/d)^d}[(f(\mathbf{w}) - (1-2\delta'))^2] = 4(1-\delta')\delta'^2 + \delta'(-2+2\delta')^2 \le 4\delta'$，我们有 $\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,\ 1/d)^d}[f'_{x,high}(\mathbf{w})^2] \le 4\delta'$，这意味着 $\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,\ 1/d)^d}[(N_{\rho_x}f'_{x,\ high})(\mathbf{w})^2] \le 4\rho_x^{2t}\delta$。因此可得

$$\begin{aligned}\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[(N_{\rho_x}f'_x)(\mathbf{w})^2] &= \mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[(N_{\rho_x}f'_{x,low})(\mathbf{w})^2] + \mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[(N_{\rho_x}f'_{x,high})(\mathbf{w})^2] \\ &\le 10(3^t)\delta^{\frac{3}{2}} + 4\rho_x^{2t}\delta.\end{aligned}$$

□

现在我们证明，单色三元组的比例必须至少为 $\frac{\delta}{8}$。正如我们先前所观察到的，为了避免出现 $\frac{\delta}{8}$ 单色三元组的比例，我们必须满足：对于至少 $\frac{\delta}{2}$ 比例的 $\mathbf{w} \sim \mathcal{N}(\mathbf{0}, 1/d)^d$，都有 $(N_{\rho_x}f_x)(-\mathbf{w}) < \frac{1}{4}$。由于 $N_{\rho_x}f_x = \mathbb{E}_{\bar{\mathbf{w}}\sim\mathcal{N}(0,1/d)^d}[f_x(\bar{\mathbf{w}})] + N_{\rho_x}f'_x \ge 1 - 2\delta + N_{\rho_x}f'_x$，我们有，对于至少 $\frac{\delta}{2}$ 比例的 $\mathbf{w} \in S^{d-1}$，都有 $|(N_{\rho_x}f'_x)(\mathbf{w})| \ge \frac{3}{4} - 4\delta$。由于 $\delta \le \frac{1}{16}$，这意味着 $\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[(N_{\rho_x}f'_x)(\mathbf{w})^2] \ge \frac{\delta}{2}\cdot(\frac{1}{2})^2 = \frac{\delta}{8}$。

然而，引理 3.13 表明，如果 $\delta > 0$ 足够小，那么 $\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[(N_{\rho_x} f'_x)] \leq \frac{\delta}{10}$。为此，取 $t = 50$ 并注意到，由于出现的每个 ρ 至多为 9，$\rho^{2t} \leq \frac{1}{80}$。由于 $\delta < \frac{1}{40000(9^t)}$，$10(3^t)\delta^{\frac{3}{2}} \leq \frac{\delta}{20}$。由引理 3.13，

$$\mathbb{E}_{\mathbf{w}\sim\mathcal{N}(0,1/d)^d}[(N_{\rho_x} f'_x)(\mathbf{w})^2] \leq 10(3^t)\delta^{\frac{3}{2}} + 4\rho^{2t}\delta \leq \frac{\delta}{20} + \frac{\delta}{20} = \frac{\delta}{10}.$$

这就导出了矛盾，因此单色三元组的比例必须至少为 $\frac{\delta}{8}$，这正是所需结论。 □

4 MAJ 多态性的改进分析

在本节中，我们证明，Charikar– Makarychev–Makarychev 的 2-SAT 鲁棒近似算法 [CMM09] 对任何具有 $f(\epsilon) = O(\sqrt{\epsilon})$ MAJ 多态性族的部分约束满足问题模板，都能提供相同的 MAJ 损失保证。这改进了 Brakensiek–Guruswami–Sandeep [BGS25], 的分析；该分析仅证明了 $f(\epsilon) = O(\sqrt[3]{\epsilon})$ 损失。此外，在下一节中，我们将把这一结果推广到定义在非布尔域上的部分约束满足问题模板，并允许更一般类型的多态性（但损失保证会略差）。

定理 4.1。设 Γ 是一个具有 MAJ $\subseteq \mathrm{Pol}(\Gamma)$ 的承诺模板。那么，$\mathrm{PCSP}(\Gamma)$ 具有一个损失函数为 $f(\epsilon) = O_\Gamma(\sqrt{\epsilon})$ 的统一鲁棒算法。

4.1 CMM 算法

我们将 Charikar–Makarychev–Makarychev（以下简称“CMM”）的算法陈述如下。

- 输入：$\epsilon > 0$，一个$\mathrm{PCSP}(\Gamma)$ 上的加权实例，变量为 $x_1, \ldots, x_n$，子句为$C_1, \ldots, C_m$，如第 2.1节所述。
- 求解基本半定规划，找到向量解$\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{R}^{n+1}$，其目标值至少为 $1 - \epsilon$。
- 采样一个随机高斯向量$\mathbf{r} \in \mathcal{N}(0_{n+1}, I_{n+1})$。
- 对于所有 $i \in [n]$，若 $\langle \mathbf{v}_i, \mathbf{v}_0 + \mathbf{r}\sqrt{\epsilon} \rangle \geq 0$，则将 x_i 舍入为 $+1$；否则如此。

我们将其称为 ϵ-CMM 算法，以明确地选择 ϵ。我们将用到以下由 [BGS25]证明的结构引理。

引理 4.2（根据 [BGS25], 的引理 4.5 改编）。设 $P \subseteq Q \subseteq \{-1, 1\}^k$ 满足MAJ $\subseteq \mathrm{Pol}(P, Q)$。对于任意$\mathbf{b} \notin Q$，存在$\mathbf{w} \in \mathbb{R}^k$，使其满足以下性质。

- $\|\mathbf{w}\|_1 = 1$。
- 对于所有 $i \in [k]$, $b_i w_i \leq 0$。

</output>

- 对所有$\mathbf{a} \in P$，$\langle \mathbf{a}, \mathbf{w} \rangle \geq 0$。

我们注意到，该引理在命题5.6中以更为一般的形式得到了证明。作为推论，引理4.2 的一个近似版本对半定规划的近似解成立。

引理 4.3 (隐含于 [BGS25])。 设 $P \subseteq Q \subseteq \{-1,1\}^k$ 满足 MAJ $\subseteq \mathrm{Pol}(P,Q)$。固定 $\mathbf{b} \in \{-1,1\}^k \setminus Q$，并令 $\mathbf{w} \in \mathbb{R}^k$ 为引理 *4.2* 所保证的取值。那么，对于任意 $1-\gamma$近似向量赋值 $(\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k)$，其对 P有：

$$\sum_{i=1}^{k} w_i \langle \mathbf{v}_i, \mathbf{v}_0 \rangle \geq -\gamma. \tag{7}$$

证明。 由于 $(\mathbf{v}_0, \ldots, \mathbf{v}_k)$ 是 $1-\gamma$对 P的近似向量赋值，因此存在一个概率分布 μ，定义在 $\{-1,1\}^k$上，使得 $\mu(P) \geq 1-\gamma$，且对所有 $i \in [k]$,

$$\langle \mathbf{v}_i, \mathbf{v}_0 \rangle = \sum_{\mathbf{a} \in \{-1,1\}^k} a_i \mu(\mathbf{a}).$$

因此，我们有：

$$\begin{aligned} \sum_{i=1}^{k} w_i \langle \mathbf{v}_i, \mathbf{v}_0 \rangle &= \sum_{i=1}^{k} w_i \sum_{\mathbf{a} \in \{-1,1\}^k} a_i \mu(\mathbf{a}) \\ &= \sum_{\mathbf{a} \in \{-1,1\}^k} \langle \mathbf{a}, \mathbf{w} \rangle \mu(\mathbf{a}). \end{aligned}$$

根据引理 4.2， $\langle \mathbf{a}, \mathbf{w} \rangle \geq 0$ 对所有 $\mathbf{a} \in P$。此外， $\langle \mathbf{a}, \mathbf{w} \rangle \geq -1$ 对所有 $\mathbf{a} \in \{-1,1\}^k$ 因为 $\|\mathbf{w}\|_1 = 1$。因此， （7） 成立，因为 $\mu(\{-1,1\}^k \setminus P) \leq \gamma$。 □

现在陈述我们的主要技术结果。

定理 4.4。 设 $P \subseteq Q \subseteq \{-1,1\}^k$ 具有 MAJ $\subseteq \mathrm{Pol}(P,Q)$。设 $(\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_k)$ 是 $1-\gamma$到 P 的近似向量赋值。对任意$\mathbf{b} \in \{-1,1\}^k \setminus Q$，运行于$(\mathbf{v}_0, \ldots, \mathbf{v}_k)$ 上的 ϵ-*CMM* 算法输出$\mathbf{b}$ 的概率至多为

$$600k \frac{\max(\epsilon, \gamma)}{\sqrt{\epsilon}} \tag{8}$$

由此可轻易推出定理 4.1 。

定理 *4.1* 的证明。 我们的基本半定规划解 $(\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_n)$ 具有如下性质：每个子句 C_j 均 $1-\gamma_j$ 近似满足，其中 $\mathbb{E}_j[\gamma_j] \leq \epsilon$。令 k_j 表示子句 C_j的元数，并定义 $k_{\max}$ =最大值$j(k_j)$。根据定理 4.4， C_j 被赋予某个特定赋值，且该赋值不能弱满足 C_j 的概率至多为

$$600k_j \frac{\max(\epsilon, \gamma_j)}{\sqrt{\epsilon}}.$$

因此，根据并集界， C_j 被弱满足的概率至少为

$$1 - 2^{k_j} \left(600k_j \frac{\max(\epsilon, \gamma_j)}{\sqrt{\epsilon}} \right) \geq 1 - 2^{k_j} \left(600k_j \frac{\epsilon + \gamma_j}{\sqrt{\epsilon}} \right) \geq 1 - 2^{k_{\max}} \left(600k_{\max} \frac{\epsilon + \gamma_j}{\sqrt{\epsilon}} \right).$$

因此，弱满足的子句所占比例的期望至少为

$$1 - 1200 \cdot 2^{k_{\max}} k_{\max} \sqrt{\epsilon},$$

正如所需。 □

4.2 定理4.4 的证明

我们要界定以下事件发生的概率：

$$b_i \langle \mathbf{v}_i, \mathbf{r} + \mathbf{v}_0/\sqrt{\epsilon} \rangle \geq 0, \quad \forall i \in [k]. \tag{9}$$

令 $\mathbf{w}$ 对应于 $\mathbf{b}$，如引理 4.2中所述。令 $\mathbf{u}: = w_1\mathbf{v}_1 + \cdots + w_k\mathbf{v}_k$。由引理 4.3，可得 $\langle \mathbf{u}, \mathbf{v}_0 \rangle \geq -\gamma$。此外，由于 $b_i w_i \leq 0$ 对所有 $i \in [k]$，我们知道式（9）成立意味着

$$\langle w_i \mathbf{v}_i, \mathbf{r} + \mathbf{v}_0/\sqrt{\epsilon} \rangle \leq 0, \quad \forall i \in [k]. \tag{10}$$

对所有 $i \in [k]$ 求和，可得。

$$\langle \mathbf{u}, \mathbf{r} + \mathbf{v}_0/\sqrt{\epsilon} \rangle \leq 0. \tag{11}$$

To 为此，我们首先证明 $\langle \mathbf{u},\mathbf{u} \rangle$ 与 $\langle \mathbf{u},\mathbf{v}_0 \rangle$ 的偏离不会太大 .

引理 4.5. $\langle \mathbf{u}, \mathbf{u} \rangle \leq \langle \mathbf{u}, \mathbf{v}_0 \rangle + 2\gamma$。

证明。令 μ 为定义在 $\{-1, 1\}^k$ 上的概率分布，满足 $\mu(P) \geq 1 - \gamma$ 对应于 $(\mathbf{v}_0, \ldots, \mathbf{v}_k)$。回顾引理 4.3 的证明可知

$$\langle \mathbf{u}, \mathbf{v}_0 \rangle = \sum_{\mathbf{a} \in \{-1,1\}^k} \langle \mathbf{a}, \mathbf{w} \rangle \mu(\mathbf{a}).$$

同样，我们可以计算得出

$$\begin{aligned} \langle \mathbf{u}, \mathbf{u} \rangle &= \sum_{i=1}^{k} \sum_{j=1}^{k} w_i w_j \langle \mathbf{v}_i, \mathbf{v}_j \rangle \\ &= \sum_{i=1}^{k} \sum_{j=1}^{k} w_i w_j \sum_{\mathbf{a} \in \{-1,1\}^k} a_i a_j \mu(\mathbf{a}) \\ &= \sum_{\mathbf{a} \in \{-1,1\}^k} \langle \mathbf{a}, \mathbf{w} \rangle^2 \mu(\mathbf{a}). \end{aligned}$$

因此，

$$\langle \mathbf{u}, \mathbf{u} \rangle - \langle \mathbf{u}, \mathbf{v}_0 \rangle = \sum_{\mathbf{a} \in \{-1,1\}^k} \langle \mathbf{a}, \mathbf{w} \rangle (\langle \mathbf{a}, \mathbf{w} \rangle - 1) \mu(\mathbf{a}).$$

回想一下，$\|\mathbf{w}\|_1 = 1$。对于任意 $\mathbf{a} \in P$，我们有 $\langle \mathbf{a}, \mathbf{w} \rangle \in [0, 1]$，因此 $\langle \mathbf{a}, \mathbf{w} \rangle (\langle \mathbf{a}, \mathbf{w} \rangle - 1) \leq 0$。此外，对于任意 $\mathbf{a} \in \{-1, 1\}^k$, $\langle \mathbf{a}, \mathbf{w} \rangle \in [-1, 1]$，这意味着 $\langle \mathbf{a}, \mathbf{w} \rangle (\langle \mathbf{a}, \mathbf{w} \rangle - 1) \leq 2$。因此，$\langle \mathbf{u}, \mathbf{u} \rangle - \langle \mathbf{u}, \mathbf{v}_0 \rangle \leq 2\gamma$。 □

对于每个 $i \in [k]$，令$\mathbf{v}_i^{=}$为$\mathbf{v}_i$ 平行于$\mathbf{u}$的分量，并令$\mathbf{v}_i^{\perp}$为$\mathbf{v}_i$ 垂直于$\mathbf{u}$的分量。也就是说，

$$\mathbf{v}_i^{=} := \frac{\langle \mathbf{v}_i, \mathbf{u} \rangle}{\langle \mathbf{u}, \mathbf{u} \rangle} \mathbf{u},$$
$$\mathbf{v}_i^{\perp} := \mathbf{v}_i - \frac{\langle \mathbf{v}_i, \mathbf{u} \rangle}{\langle \mathbf{u}, \mathbf{u} \rangle} \mathbf{u}.$$

令 $\eta := \max(\gamma, \epsilon)$。现在我们分情形讨论。

情形 1， $\|\mathbf{u}\|^2 \geq 8\eta \ln(1/\epsilon)$。 在这种情况下，我们有 $\|\mathbf{u}\|^2 \geq 4\gamma$。因此，根据引理 4.5，

$$\langle \mathbf{u}, \frac{1}{\sqrt{\epsilon}} \mathbf{v}_0 \rangle \geq \frac{1}{\sqrt{\epsilon}} (\|\mathbf{u}\|^2 - 2\gamma) \geq \frac{\|\mathbf{u}\|^2}{2\sqrt{\epsilon}}.$$

因此，(11) 成立的条件是

$$\langle \mathbf{r}, -\frac{\mathbf{u}}{\|\mathbf{u}\|} \rangle > \frac{\|\mathbf{u}\|}{2\sqrt{\epsilon}}.$$

注意，左端服从均值为 0、方差为 1 的正态分布。因此，根据命题 2.2，我们推得 (9) 成立的概率至多为

$$\frac{1}{2} \exp\left(-\frac{1}{2} \left(\frac{\|\mathbf{u}\|}{2\sqrt{\epsilon}} \right)^2 \right) \leq \frac{1}{2} \exp\left(-\frac{\eta}{\epsilon} \log(1/\epsilon) \right) \leq \frac{\epsilon}{2} \leq \frac{\eta}{\sqrt{\epsilon}}.$$

情形 2，存在 $i \in [k]$ **使得** $\|w_i \mathbf{v}_i^{\perp}\| \geq 1/(10k)$。 首先，注意到根据命题 2.2，对于所有 $\delta \geq 0$，我们有

$$\Pr[\delta \leq |\langle \mathbf{r}, \mathbf{u} \rangle| \leq 2\delta] = \Pr\left[\frac{\delta}{||\mathbf{u}||} \leq \left| \langle \mathbf{r}, \frac{\mathbf{u}}{\|\mathbf{u}\|} \rangle \right| \leq \frac{2\delta}{||\mathbf{u}||} \right] \leq 2 \frac{\delta}{\|u\|\sqrt{2\pi}} e^{-\frac{\delta^2}{2\|\mathbf{u}\|^2}} \leq \frac{\delta}{\|\mathbf{u}\|} e^{-\frac{\delta^2}{2\|\mathbf{u}\|^2}}. \tag{12}$$

假设（9）成立。那么，根据（10）、（11）和引理 4.5，我们有

$$0 \geq \left\langle w_i \mathbf{v}_i, \mathbf{r} + \frac{\mathbf{v}_0}{\sqrt{\epsilon}} \right\rangle \geq \langle \mathbf{u}, \mathbf{r} \rangle + \frac{1}{\sqrt{\epsilon}} \langle \mathbf{u}, \mathbf{v}_0 \rangle \geq \langle \mathbf{u}, \mathbf{r} \rangle + \frac{1}{\sqrt{\epsilon}} (\|\mathbf{u}\|^2 - 2\gamma) \geq \langle \mathbf{u}, \mathbf{r} \rangle - \frac{2}{\sqrt{\epsilon}} \gamma. \tag{13}$$

现在考虑随机变量 $\langle w_i \mathbf{v}_i$、$\mathbf{r} + \mathbf{v}_{\sqrt{\epsilon}}^{0} \rangle$ 在给定 $\langle \mathbf{u}$、$\mathbf{r} \rangle$取值的条件下的概率分布。注意，这是一个标准差为$\|w_i \mathbf{v}_i^{\perp}\| \geq \frac{1}{10k}$（均值任意）的高斯分布。根据命题 2.2，（13）成立的概率至多为 —

$$10k(|\langle \mathbf{u}, \mathbf{r} \rangle| + \frac{2}{\sqrt{\epsilon}} \gamma) \leq 10k \left(2\delta + \frac{2}{\sqrt{\epsilon}} \gamma \right).$$

因此，$\delta \leq |\langle \mathbf{r}$、$\mathbf{u} \rangle| \leq 2\delta$ 以及（9）同时成立的概率至多为

$$\frac{\delta}{\|\mathbf{u}\|} e^{-\frac{\delta^2}{2\|\mathbf{u}\|^2}} \cdot 10k \left(2\delta + \frac{2}{\sqrt{\epsilon}} \gamma) \right) \leq \frac{40k\delta e^{-\frac{\delta^2}{2||\mathbf{u}||^2}}}{||\mathbf{u}||} \max\left\{ \delta, \frac{\gamma}{\sqrt{\epsilon}} \right\}.$$

将上述表达式的右端记为 $f(\delta)$。现在，我们根据 $\|\mathbf{u}\|^2$的大小将分析细分为若干种情况。

情形 2a， $\|\mathbf{u}\|^2 \le 4\eta$。我们要给出 $\sum_{i=-\infty}^{\infty} f(2^i\|\mathbf{u}\|)$ 的上界。如果 $i \le 1$，注意到

$$f(2^i\|\mathbf{u}\|) \le \frac{40k\cdot 2^i\|\mathbf{u}\|}{\|\mathbf{u}\|}\max\left\{2^i\|\mathbf{u}\|, \frac{\gamma}{\sqrt{\epsilon}}\right\} \le 40k\cdot 2^i\cdot\frac{\eta}{\sqrt{\epsilon}}.$$

对所有 $i \le 1$ 求和后，得到的贡献至多为 $160k\eta/\sqrt{\epsilon}$。否则，若 $i \ge 2$，则有

$$f(2^i\|\mathbf{u}\|) \le 40k\cdot 2^i\cdot e^{-2^{2i-1}}\cdot\max\left\{2^{i+1}\sqrt{\eta}, \frac{\eta}{\sqrt{\epsilon}}\right\} \le \frac{160k\eta}{\sqrt{\epsilon}}\cdot 2^{2i-1}e^{-2^{2i-1}}.$$

利用函数 $x \mapsto x\cdot e^{-x}$ 在 $[1,\infty)$ 上单调不增这一性质，可得

$$\sum_{i=2}^{\infty} 2^{2i-1}e^{-2^{2i-1}} \le \sum_{i=2}^{\infty} ie^{-i} \le \int_0^{\infty} x\cdot e^{-x}\,dx = 1$$

因此，

$$\sum_{i=2}^{\infty} f(2^i\|\mathbf{u}\|) \le \frac{160k\eta}{\sqrt{\epsilon}}.$$

因此，总概率界至多为 $\frac{320k\eta}{\sqrt{\epsilon}}$。

情形 2b， $\|\mathbf{u}\|^2 > 4\eta$。按照与情形 1 类似的逻辑，只有在以下条件成立时，式（9）才成立：$\langle \mathbf{r}_{-\mathbf{u}\|\mathbf{u}\|}\rangle > \|\mathbf{u}\|$。因此，我们只需考虑 $\delta \ge \frac{\|\mathbf{u}\|^2}{2\sqrt{\epsilon}}$。考虑任意这样的 $\delta = \lambda\|\mathbf{u}\| \ge \|\mathbf{u}\|^2/(2\sqrt{\epsilon})$，使得 $2\lambda\sqrt{\epsilon} \ge \|\mathbf{u}\|$。我们有

$$f(\lambda\|\mathbf{u}\|) = 40k\lambda e^{-\frac{\lambda^2}{2}}\max\left\{\lambda\|\mathbf{u}\|, \frac{\gamma}{\sqrt{\epsilon}}\right\} \le 160k\lambda^3 e^{-\frac{\lambda^2}{2}}\sqrt{\epsilon}.$$

由于 $2\lambda\sqrt{\epsilon} \ge \|\mathbf{u}\| > \sqrt{4\eta}$，我们有 $\lambda > 1$。因此，(9) 发生的相关概率至多为

$$\sum_{i=0}^{\infty} 160k\cdot 2^{3i}\cdot e^{-2^{2i-1}}\sqrt{\epsilon} \le 600k\sqrt{\epsilon} \le 600k\eta/\sqrt{\epsilon},$$

正如所需。

情形 3， $\|\mathbf{u}\|^2 < 8\eta\ln\left(\frac{1}{\epsilon}\right)$ **并且不存在** i **使得** $\|w_i\mathbf{v}_i^{\perp}\| \ge \frac{1}{10k}$。在这种情况下，由于 $\mathbf{u} = \sum_{i=1}^k w_i\mathbf{v}_i$ 且 $\sum_{i=1}^k \|w_i\mathbf{v}_i\| = \sum_{i=1}^k |w_i|\|\mathbf{v}_i\| = \sum_{i=1}^k |w_i| = 1$，我们得到

$$1 = \sum_{i=1}^k ||w_i\mathbf{v}_i|| \le \sum_{i=1}^k ||w_i\mathbf{v}_i^{=}|| + \sum_{i=1}^k ||w_i\mathbf{v}_i^{\perp}|| \le \sum_{i=1}^k ||w_i\mathbf{v}_i^{=}|| + \frac{1}{10},$$

and

$$\left\|\sum_{i=1}^k w_i\mathbf{v}_i^{=}\right\|^2 + \left\|\sum_{i=1}^k w_i\mathbf{v}_i^{\perp}\right\|^2 = \|\mathbf{u}\|^2 \le 8\eta\ln\left(\frac{1}{\epsilon}\right).$$

综合这些观察，必定存在一个 i 使得 $w_i\mathbf{v}_i = c\,\frac{\mathbf{u}}{\|\mathbf{u}\|} + w_i\mathbf{v}_i^{\perp}$其中$|c| \geq \frac{1}{2k}$。现在我们定义 t, x, y如下

$$t := -\frac{\langle w_i\mathbf{v}_i, \mathbf{v}_0\rangle}{c\sqrt{\epsilon}},$$
$$x := \langle \frac{\mathbf{u}}{||\mathbf{u}||}, \mathbf{r}\rangle,$$
$$y := -\sum_i \langle w_i\mathbf{v}_i, \mathbf{r} + \mathbf{v}_0/\sqrt{\epsilon}\rangle.$$

注意， t 是一个常数，而 x 和 y 是依赖于$\mathbf{r}$的随机变量。特别地， x 是一个均值为零、方差为一的高斯随机变量。此外，注意

$$\langle w_i\mathbf{v}_i, \mathbf{r} + \mathbf{v}_0/\sqrt{\epsilon}\rangle = c(x-t) + \langle w_i{\mathbf{v}_i}^{\perp}, \mathbf{r}\rangle.$$

接下来我们观察到以下结论。首先，为了使 (9) 成立，我们必须有 $-y \leq \langle w_i\mathbf{v}_i, \mathbf{r} + \mathbf{v}_0/\sqrt{\epsilon}\rangle \leq 0$，这意味着

$$|\langle w_i{\mathbf{v}_i}^{\perp}, \mathbf{r}\rangle + c(x-t)| \leq y. \tag{14}$$

其次，由于 $-y = \sum_i \langle w_i\mathbf{v}_i, \mathbf{r} + \mathbf{v}_0/\sqrt{\epsilon}\rangle = \langle \mathbf{u}, \mathbf{r}\rangle + \frac{1}{\sqrt{\epsilon}}\langle \mathbf{u}, \mathbf{v}_0\rangle \geq \langle \mathbf{u}, \mathbf{r}\rangle + \frac{1}{\sqrt{\epsilon}}(||\mathbf{u}||^2 - 2\gamma) = ||\mathbf{u}||x + \frac{1}{\sqrt{\epsilon}}(||\mathbf{u}||^2 - 2\gamma)$，我们有

$$|x| \geq -x \geq \frac{||\mathbf{u}||}{\sqrt{\epsilon}} - \frac{2\gamma}{||\mathbf{u}||\sqrt{\epsilon}} + \frac{y}{||\mathbf{u}||}. \tag{15}$$

为完成证明，我们根据（$y, c(x-t)$).的取值分情况讨论。

情形 3a， $y \leq 4\frac{\eta}{\sqrt{\epsilon}}$。由于 $|c| \geq \frac{1}{2k}$，但 $\|w_i{\mathbf{v}_i}^{\perp}\| \leq \frac{1}{10k}$，我们有 $\langle w_i\mathbf{v}_i, \mathbf{r} + \mathbf{v}_0/\sqrt{\epsilon}\rangle = c(-x-t) + \langle w_i{\mathbf{v}_i}^{\perp}, \mathbf{r}\rangle$ 的标准差至少为 $|c|/2 \geq \frac{1}{4k}$。因此，根据命题2.2

$$\Pr\left[|\langle w_i{\mathbf{v}_i}^{\perp}, \mathbf{r}\rangle + c(x-t)| \leq 4\frac{\eta}{\sqrt{\epsilon}}\right] \leq \frac{4\eta}{|c|\sqrt{\epsilon}/2} \leq 16k\frac{\eta}{\sqrt{\epsilon}}.$$

也就是说，若我们以 $y \leq \frac{4\eta}{\sqrt{\epsilon}}$为条件，则式（14）成立（因而式（9）成立）的概率至多为 $16k\frac{\eta}{\sqrt{\epsilon}}$。

情形 3b，存在 $\delta \geq 4\eta/\sqrt{\epsilon}$ 使得 $y \geq \delta$ 且 $|c(x-t)| \leq 4\delta$。 注意到 $\delta/2 \geq 2\gamma/\sqrt{\epsilon}$，因此由（15）， 我们有

$$|x| \geq \frac{||\mathbf{u}||}{\sqrt{\epsilon}} + \frac{\delta}{2||\mathbf{u}||}. \tag{16}$$

因此，根据命题 2.2，我们有

$$\Pr[|c(x-t)| \leq 4\delta \wedge y \geq \delta] \leq \Pr[|c(x-t)| \leq 4\delta \wedge (16)]$$
$$\leq \frac{8\delta}{|c|}e^{-\frac{1}{2}\left(\frac{\|\mathbf{u}\|}{\sqrt{\epsilon}} + \frac{\delta}{2\|\mathbf{u}\|}\right)^2} \leq \frac{8\delta}{|c|}e^{-\frac{\delta}{\sqrt{\epsilon}}} \leq 16k\delta e^{-\frac{\delta}{\sqrt{\epsilon}}}.$$

情形 3c，存在 $\delta' \geq 4\delta \geq 16\eta/\sqrt{\epsilon}$ 使得 $y \in [\delta, 2\delta]$ 且 $|c(x-t)| \in [\delta', 2\delta']$。 注意，(16) 仍然成立，因此我们有

$$\begin{aligned}\Pr[|c(x-t)| \in [\delta', 2\delta'] \wedge y \in [\delta, 2\delta]] &\leq \Pr[|c(x-t)| \in [\delta', 2\delta'] \wedge (16)] \\ &\leq \frac{2\delta'}{|c|} e^{-\frac{1}{2}\left(\frac{\|\mathbf{u}\|}{\sqrt{\epsilon}} + \frac{\delta}{2\|\mathbf{u}\|}\right)^2} \leq \frac{2\delta'}{|c|} e^{-\frac{\delta}{\sqrt{\epsilon}}}.\end{aligned}$$

令 $d = \|w_i \mathbf{v}_i^{\perp}\|$。根据命题 2.2，我们有

$$\begin{aligned}\Pr[(9) \mid |c(x-t)| \in [\delta', 2\delta'] \wedge y \in [\delta, 2\delta]] &\leq \Pr[(14) \mid |c(x-t)| \in [\delta', 2\delta'] \wedge y \in [\delta, 2\delta]] \\ &\leq \frac{4\delta}{d} e^{-\frac{\delta'^2}{8d^2}},\end{aligned}$$

最后一个不等式成立，是因为 $\langle w_i \mathbf{v}_i^{\perp}, \mathbf{r} \rangle$ 必须落在一个长度至多为 2δ、最小值为 $\delta' - 2\delta \geq \frac{\delta'}{2}$ 的区间内。因此，结合前面的两项计算，我们有

$$\Pr[(9) \wedge |c(x-t)| \in [\delta', 2\delta'] \wedge y \in [\delta, 2\delta]] \leq \frac{8\delta\delta'}{|c|d} e^{-\frac{\delta}{\sqrt{\epsilon}} - \frac{\delta'^2}{8d^2}}.$$

完成情形 3。 现在我们把这些子情形合并起来。首先，以 $\delta \geq 4\eta/\sqrt{\epsilon}$ 为条件。根据情形 3b 和 3c，我们有

$$\begin{aligned}\Pr[(9) \wedge y \in [\delta, 2\delta]] &\leq \Pr[|c(x-t)| \in [\delta', 2\delta'] \wedge y \in [\delta, 2\delta]] \\ &\quad + \sum_{i=2}^{\infty} \Pr[(9) \mid |c(x-t)| \in [2^i\delta, 2^{i+1}\delta] \wedge y \in [\delta, 2\delta]] \\ &\leq 6k\delta e^{-\frac{\delta}{\sqrt{\epsilon}}} + \sum_{i=2}^{\infty} \frac{2^{i+3}\delta^2}{|c|d} e^{-\frac{\delta}{\sqrt{\epsilon}} - \frac{2^{2i}\delta^2}{8d^2}} \\ &= 6k\delta e^{-\frac{\delta}{\sqrt{\epsilon}}} + 16k \cdot \delta e^{-\delta/\sqrt{\epsilon}} \sum_{i=2}^{\infty} \frac{2^i\delta}{d} e^{-\frac{2^{2i}\delta^2}{8d^2}}.\end{aligned}$$

Now,

$$\sum_{i=2}^{\infty} \frac{2^i\delta}{d} e^{-\frac{2^{2i}\delta^2}{8d^2}} \leq \sum_{i=2}^{\infty} 2 \int_{2^{i-1}}^{2^i} \frac{\delta}{d} e^{-\frac{s^2\delta^2}{8d^2}}\, ds \leq \int_{-\infty}^{\infty} \frac{\delta}{d} e^{-\frac{s^2\delta^2}{8d^2}}\, ds = \int_{-\infty}^{\infty} e^{-\frac{s^2}{8}}\, ds = 2\sqrt{2\pi} \leq \frac{11}{2},$$

so

$$\Pr[(9) \wedge y \in [\delta, 2\delta]] \leq 100k\delta e^{-\frac{\delta}{\sqrt{\epsilon}}}.$$

接下来，我们纳入情形 3a 的界，得到

$$\begin{aligned}\Pr[(9)] &\leq \Pr[(9) \wedge y \leq 4\eta/\sqrt{\epsilon}] + \sum_{i=2}^{\infty} \Pr[(9) \wedge y \in [2^i\eta/\sqrt{\epsilon}, 2^{i+1}\eta/\sqrt{\epsilon}]] \\ &\leq 16k\frac{\eta}{\sqrt{\epsilon}} + 100k \cdot \frac{\eta}{\sqrt{\epsilon}} \sum_{i=2}^{\infty} 2^i e^{-\frac{2^i\eta}{\epsilon}} \\ &\leq 16k\frac{\eta}{\sqrt{\epsilon}} + 100k \cdot \frac{\eta}{\sqrt{\epsilon}} \sum_{i=2}^{\infty} 2^i e^{-2^i} \\ &\leq 50k \cdot \frac{\eta}{\sqrt{\epsilon}},\end{aligned}$$

按需完成。这就完成了定理 4.4 的证明，因而也完成了定理 4.1的证明。

5 可分部分约束满足问题的舍入方案

本节旨在将第 4 节的结果推广到非布尔域上的承诺约束满足问题。在本节中，我们始终关注弱约束语言与强约束语言的域相同的承诺约束满足问题。

我们先给出两个定义。给定一个元组 $\mathbf{a} \in A^k$，我们用 $\Pi_{\mathbf{a}} \in \mathbb{R}^{k \times A}$ 表示$\mathbf{a}$的独热编码；也就是说，矩阵 $\Pi_{\mathbf{a}}$ 的第 (i, a) 个元素在 $a_i = a$时为 $\mathbf{1}$，否则为 $\mathbf{0}$。此外，我们用$\langle -, - \rangle_{\mathrm{F}}$表示矩阵的 Frobenius 内积，其定义为 $\langle M, N \rangle_{\mathrm{F}} = \mathrm{Tr}(M^\top N)$。

定义 5.1。 固定一个 *PCSP* 模板 $(\mathbf{A},\mathbf{B})$ 和一个函数 $\rho : \mathbb{R}^A \to A$。我们称$(\mathbf{A}, \mathbf{B})$ 是 ρ-可分的，如果 $A = B$，并且对于某个元数为 k 的承诺关系 (P, Q) 以及每个$\mathbf{b} \in A^k \setminus Q$，都存在一个矩阵 $W \in \mathbb{R}^{k \times A}$ 使得

1. $\|W\|_1 = 1$；*2.* $W\mathbf{1} = \mathbf{0}$；*3.* 对每个 $\mathbf{a} \in P$，$\langle W, \Pi_{\mathbf{a}} \rangle_{\mathrm{F}} \geq 0$；以及 *4.* 对每个 $M \in \rho^{-1}(\mathbf{b})$，$\langle W, M \rangle_{\mathrm{F}} \leq 0$。

在上述定义的第 4 部分中，表达式 $\rho^{-1}(\mathbf{b})$ 表示这样的实矩阵集合：对每个 $i \in [k]$，其第 i 行属于 $\rho^{-1}(b_i)$ 的矩阵 $k \times A$。

直观地说，在定义 5.1中， ρ 应被视为任意的舍入方案；我们的想法是考虑与该方案相容的多态函数族，也就是说，这些函数族可以用来避免出现较大的整数间隙。我们还将假设舍入函数 ρ 满足以下较弱意义上的良好性质。

定义 5.2。 固定某个参数 $\alpha > 0$。我们称函数 $\rho : \mathbb{R}^A \to A$ 是 α-保守的，如果不等式

$$q_{\rho(\mathbf{q})} \geq \alpha \sum_{b \in A} q_b$$

对每个 $\mathbf{q} \in \mathbb{R}^A$ 成立。

定理 5.3. 设 $(\mathbf{A},\mathbf{B})$ 连同 $A = B$ 是一个关于 α-保守函数 $\rho\colon \mathbb{R}^A \to A$ 的 ρ-可分 *PCSP* 模板。则 $\mathrm{PCSP}(\mathbf{A},\mathbf{B})$ 可借助半定规划以损失 $O_{\alpha,A}(\sqrt{\epsilon}\log(1/\epsilon))$ 鲁棒求解。

注记 5.4. 我们指出，对 ρ 在定义 *5.1* 中所施加的条件本身过于宽泛，不足以保证具有定理 *5.3* 之损失保证的鲁棒可解性，因为它们也被诸如 *Horn-SAT* 之类的 *CSP* 模板所满足，而这些模板（在假设唯一博弈猜想时）并不具备 $\epsilon^{O(1)}$-鲁棒舍入方案。因此， α-保守性对于 ρ 是必要的。

证明。 不失一般性，我们考虑 $\mathrm{PCSP}(\mathbf{A},\mathbf{B})$ 仅包含一个元数为 k 的承诺关系 (P, Q) 的情形。令 $(\mathbf{v}_0, \{\mathbf{v}_{1,a} \colon a \in A\}, \ldots, \{\mathbf{v}_{k,a} \colon a \in A\})$ 为

一个 $(1-\gamma)$-近似向量赋值，其对象为 P，其中 $\gamma > 0$ 如第 2.2 节所述。固定 $\epsilon > 0$，并对该向量赋值运行 ϵ-CMM 算法，使用 ρ 作为舍入函数（见第 4.1 节）。更准确地说，我们执行以下过程：

1. 采样一个随机高斯向量$\mathbf{r} \in \mathcal{N}(0_n, I_n)$（其中，$n$ 是半定规划向量所在空间的维度）。

2. 定义$\mathbf{z} = \mathbf{r} + \mathbf{v}_{\sqrt{\epsilon}}$ 并令$\mathbf{c}^{(i)} \in \mathbb{R}^A$ 为满足其 a 次项为 $c_a^{(i)} = \langle \mathbf{v}_{i,a}\, \mathbf{z} \rangle$（对每个 $i \in [k]$）的向量。

3. 对每个 $i \in [k]$，令 $b_i = \rho(\mathbf{c}^{(i)})$。

现在考虑向量$\mathbf{b} = (b_i)_{i\in[k]} \in A^k$，并假设$\mathbf{b} \notin Q$。取一个相应的矩阵 $W \in \mathbb{R}^{k,A}$ 这是由（$\mathbf{A}$，$\mathbf{B}$）是 ρ-可分的这一事实所保证的，并定义向量

$$\mathbf{u} = \sum_{i\in[k]} \sum_{a\in A} w_{i,a} \mathbf{v}_{i,a}.$$

另请考虑矩阵 $M \in \mathbb{R}^{k\times A}$，其 $(i,\ a)$ 项为 $c_a^{(i)}$。注意到 $M \in \rho^{-1}(\mathbf{b})$，因此定义 4. 的第 5.1 部分保证了

$$\langle \mathbf{u}, \mathbf{z} \rangle = \langle W, M \rangle_{\mathrm{F}} \leq 0. \tag{17}$$

现在注意到，对于每个$\mathbf{a} \in A^k$，成立

$$\langle W, \Pi_{\mathbf{a}} \rangle_{\mathrm{F}} = \sum_{i\in[k]} w_{i,a_i}.$$

因此，令 μ 表示与向量赋值对应的概率分布，我们得到

$$\begin{aligned}\langle \mathbf{u}, \mathbf{u} \rangle &= \sum_{i,i'\in[k]} \sum_{a,a'\in A} w_{i,a} w_{i',a'} \langle \mathbf{v}_{i,a}, \mathbf{v}_{i',a'} \rangle = \sum_{i,i'\in[k]} \sum_{a,a'\in A} w_{i,a} w_{i',a'} \sum_{\substack{\mathbf{a}\in A^k \\ a_i = a \\ a_{i'} = a'}} \mu(\mathbf{a}) \\ &= \sum_{\mathbf{a}\in A^k} \mu(\mathbf{a}) \sum_{i,i'\in[k]} w_{i,a_i} w_{i',a_{i'}} = \sum_{\mathbf{a}\in A^k} \mu(\mathbf{a}) \langle W, \Pi_{\mathbf{a}} \rangle_{\mathrm{F}}^2.\end{aligned}$$

类似地，

$$\begin{aligned}\langle \mathbf{u}, \mathbf{v}_0 \rangle &= \sum_{i\in[k]} \sum_{a\in A} w_{i,a} \langle \mathbf{v}_{i,a}, \mathbf{v}_0 \rangle = \sum_{i\in[k]} \sum_{a\in A} w_{i,a} \sum_{\substack{\mathbf{a}\in A^k \\ a_i = a}} \mu(\mathbf{a}) = \sum_{\mathbf{a}\in A^k} \mu(\mathbf{a}) \sum_{i\in[k]} w_{i,a_i} \\ &= \sum_{\mathbf{a}\in A^k} \mu(\mathbf{a}) \langle W, \Pi_{\mathbf{a}} \rangle_{\mathrm{F}}.\end{aligned} \tag{18}$$

现在，定义 5.1 的第 1 部分意味着，对于每个 $\mathbf{a} \in A^k$，

$$|\langle W, \Pi_{\mathbf{a}} \rangle_{\mathrm{F}}| = |\sum_{i\in[k]} w_{i,a_i}| \leq \sum_{i\in[k], a\in A} |w_{i,a}| = \|W\|_1 = 1,$$

而第 3 部分意味着 $0 \le \langle W, \Pi_{\mathbf{a}} \rangle_{\mathrm{F}}$ 对于每个 $\mathbf{a} \in P$。因此，量 $\langle W, \Pi_{\mathbf{a}} \rangle^2{}_{\mathrm{F}} - \langle W, \Pi_{\mathbf{a}} \rangle_{\mathrm{F}}$ 对于每个 $\mathbf{a} \in A^k$ 至多为 2；如果 $\mathbf{a} \in P$，则它非正。由此可得

$$\langle \mathbf{u}, \mathbf{u} \rangle - \langle \mathbf{u}, \mathbf{v}_0 \rangle = \sum_{\mathbf{a} \in A^k} \mu(\mathbf{a}) (\langle W, \Pi_{\mathbf{a}} \rangle_{\mathrm{F}}^2 - \langle W, \Pi_{\mathbf{a}} \rangle_{\mathrm{F}}) \le 2\gamma \tag{19}$$

（这里我们用到了向量 $\mathbf{v}_0, \{\mathbf{v}_{i,a}\}$ 构成了 $1-\gamma$ 近似向量赋值 P。）

取 $\delta = 2\max(\epsilon, \gamma) \log(1/\epsilon)$ 和 $\eta = \sqrt{2(\delta + 2\gamma) \log(1/\epsilon)} + \frac{\delta+\gamma}{\sqrt{\epsilon}}$。首先假设 $\langle \mathbf{u}, \mathbf{v}_0 \rangle > \delta$。注意，随机变量 $\langle \mathbf{u}, \mathbf{z} \rangle = \langle \mathbf{u}, \mathbf{r} + \mathbf{v}_0 / \sqrt{\epsilon} \rangle$ 服从均值为 $\mu = \frac{1}{\sqrt{\epsilon}} \langle \mathbf{u}, \mathbf{v}_0 \rangle$、标准差为 $\sigma = \|\mathbf{u}\|$ 的高斯分布。应用命题 2.1 的 (b) 部分，并注意到 $\gamma \le \frac{\delta}{2}$，我们可以推得 (17) 成立的概率上界为

$$\exp\left(-\frac{\langle \mathbf{u}, \mathbf{v}_0 \rangle^2}{2\epsilon \|\mathbf{u}\|^2}\right) \le \exp\left(-\frac{\langle \mathbf{u}, \mathbf{v}_0 \rangle^2}{2\epsilon(\langle \mathbf{u}, \mathbf{v}_0 \rangle + 2\gamma)}\right) \le \exp\left(-\frac{\delta^2}{2\epsilon(\delta + 2\gamma)}\right) \le \exp\left(-\frac{\delta}{4\epsilon}\right) \le \sqrt{\epsilon}.$$

在上面的表达式中，第二个不等式利用了函数 $x \mapsto \frac{x^2}{x+c}$ 在 $x, c \ge 0$ 时递增这一事实，而最后一个不等式成立是因为

$$-\frac{\delta}{4\epsilon} = -\frac{2\max(\epsilon, \gamma)\log(1/\epsilon)}{4\epsilon} = \frac{\max(\epsilon, \gamma)\log\epsilon}{2\epsilon} \le \frac{\log\epsilon}{2} = \log(\sqrt{\epsilon}).$$

因此，在这种情况下，$\mathbf{b} \notin Q$ 的概率至多为 $\sqrt{\epsilon}$。

现在假设 $\langle \mathbf{u}, \mathbf{v}_0 \rangle \le \delta$。利用 (19)，我们推得在这种情况下，$\langle \mathbf{u}, \mathbf{u} \rangle \le 2\gamma + \delta$。回想一下，$\mathbf{r}$ 是从分布 $\mathcal{N}(0_n, I_n)$ 中抽取的随机高斯向量，因此 $\langle \mathbf{u}, \mathbf{r} \rangle$ 服从均值为 0、标准差为 $\|\mathbf{u}\|$ 的高斯分布。利用命题 2.1 的第 (b) 部分，我们得到

$$\Pr\left(|\langle \mathbf{u}, \mathbf{r} \rangle| \ge \sqrt{2(\delta + 2\gamma)\log(1/\epsilon)}\right) \le 2\exp\left(-\frac{2(\delta + 2\gamma)\log(1/\epsilon)}{2\|\mathbf{u}\|^2}\right) \le 2\exp\left(-\log(1/\epsilon)\right) = 2\epsilon. \tag{20}$$

现在注意到 $\langle \mathbf{u}, \mathbf{v}_0 \rangle \ge -\gamma$。事实上，我们有

$$\langle \mathbf{u}, \mathbf{v}_0 \rangle = \sum_{\mathbf{a} \in A^k} \mu(\mathbf{a}) \langle W, \Pi_{\mathbf{a}} \rangle_{\mathrm{F}} \ge \sum_{\mathbf{a} \in A^k \setminus P} \mu(\mathbf{a}) \langle W, \Pi_{\mathbf{a}} \rangle_{\mathrm{F}} \ge -\|W\|_1 \sum_{\mathbf{a} \in A^k \setminus P} \mu(\mathbf{a}) \ge -\gamma,$$

其中，第一个等式为 (18)，而第一个和最后一个不等式分别来自定义 5.1 的第 3 部分和第 1 部分。特别地，这意味着 $|\langle \mathbf{u}, \mathbf{v}_0 \rangle| \le \max(\delta, \gamma) < \delta + \gamma$。因此，根据 (20)，概率至少为 $1 - 2\epsilon$ 时，有

$$|\langle \mathbf{u}, \mathbf{z} \rangle| = |\langle \mathbf{u}, \mathbf{r} \rangle + \frac{1}{\sqrt{\epsilon}} \langle \mathbf{u}, \mathbf{v}_0 \rangle| \le |\langle \mathbf{u}, \mathbf{r} \rangle| + \frac{1}{\sqrt{\epsilon}} |\langle \mathbf{u}, \mathbf{v}_0 \rangle| \le \sqrt{2(\delta + 2\gamma)\log(1/\epsilon)} + \frac{\delta + \gamma}{\sqrt{\epsilon}} = \eta. \tag{21}$$

现在，对于每个 $i \in [k]$，考虑集合 $A_{i,+} = \{a \in A : w_{i,a} > 0\}$ 和 $A_{i,-} = \{a \in A : w_{i,a} \le 0\}$，并令 $c_i = \sum_{a \in A} |w_{i,a}|$。利用定义 5.1 的第 2 部分，我们得出 $\sum_{a \in A} w_{i,a} = 0$，因此

$$\sum_{a \in A_{i,+}} w_{i,a} = -\sum_{a \in A_{i,-}} w_{i,a}.$$

固定 $i \in [k]$，并取某个 $\lambda > 0$。考虑 $k \times A$ 矩阵 $M^{(i,\lambda)}$，其第 (i, b_i) 个元素为 1，对每个 $j \neq i \in [k]$，第 (j, b_j) 个元素为 λ，其余元素均为 0。回忆一下，假设函数ρ 对于某个 $\alpha > 0$ 是 α-保守的。由此可得 $M^{(i,\lambda)} \in \rho^{-1}(\mathrm{b})$，因此根据定义 5.1 的第 4 部分，$\langle W, M^{(i,\lambda)} \rangle_{\mathrm{F}} \leq 0$。由于这对每个正的 λ 都成立，我们可推得 $w_{i,b_i} \leq 0$，因此对每个 $i \in [k]$，都有 $b_i \in A_{i,-}$。

现在令 $\beta = \min(\frac{\alpha}{2}, \frac{1}{2|A|})$。考虑由 $N_i^{(i,\lambda)}{}_{,b_i} = 1 - \beta |A_{i,+}|$,$N(i,\lambda)_{\,i,a} = \beta$ 对每个 $a \in A_{i,+}$，$N(i,\lambda)_{\,i,a} = 0$ 对每个 $a \in A_{i,-} \setminus \{b_i\}$，$N_j^{(i,\lambda)}{}_{,b_j} = \lambda$ 对每个 $j \neq i \in [k]$，以及 $N_j^{(i,\lambda)}{}_{,a} = 0$ 在其他情况下定义的矩阵 $N^{(i,\lambda)}$。再次利用 ρ 的 α-保守性，我们得到 $N(i, \lambda) \in \rho^{-1}(\mathrm{b})$，因此 $\langle W, N^{(i,\lambda)} \rangle_{\mathrm{F}} \leq 0$。令 $\lambda \to 0$ 取极限，这意味着 $\beta \sum_{a \in A_{i,+}} w_{i,a} \leq (\beta |A_{i,+}| - 1) w_{i,b_i}$。因此，对每个 $i \in [k]$，我们有

$$\begin{aligned} c_i = \sum_{a \in A} |w_{i,a}| &= \sum_{a \in A_{i,+}} w_{i,a} - \sum_{a \in A_{i,-}} w_{i,a} = 2 \sum_{a \in A_{i,+}} w_{i,a} \leq 2 \frac{\beta |A_{i,+}| - 1}{\beta} w_{i,b_i} \\ &= 2 \frac{1 - \beta |A_{i,+}|}{\beta} |w_{i,b_i}|. \end{aligned} \tag{22}$$

α的 ρ 保守性也保证了

$$\langle \mathbf{v}_{i,b_i}, \mathbf{z} \rangle = c_{b_i}^{(i)} \geq \alpha \sum_{a \in A} c_a^{(i)} = \alpha \sum_{a \in A} \langle \mathbf{v}_{i,a}, \mathbf{z} \rangle = \alpha \langle \mathbf{v}_0, \mathbf{z} \rangle. \tag{23}$$

利用命题2.3，我们发现

$$\Pr(\|\mathbf{r}\| > \frac{1}{2\sqrt{\epsilon}}) \leq O(\exp(-1/\sqrt{\epsilon})).$$

因此，由柯西–施瓦茨不等式可得

$$\langle \mathbf{v}_0, \mathbf{z} \rangle = \langle \mathbf{v}_0, \mathbf{r} + \frac{\mathbf{v}_0}{\sqrt{\epsilon}} \rangle = \langle \mathbf{v}_0, \mathbf{r} \rangle + \frac{1}{\sqrt{\epsilon}} \geq -|\langle \mathbf{v}_0, \mathbf{r} \rangle| + \frac{1}{\sqrt{\epsilon}} \geq -\|\mathbf{r}\| + \frac{1}{\sqrt{\epsilon}} \geq \frac{1}{2\sqrt{\epsilon}} \tag{24}$$

以 $1 - O(\exp(-1/\sqrt{\epsilon}))$ 的概率。类似地，我们有

$$\langle \mathbf{v}_{i,b_i}, \mathbf{z} \rangle \leq \|\mathbf{v}_{i,b_i}\| \cdot \|\mathbf{z}\| = \|\mathbf{v}_{i,b_i}\| \cdot \|\mathbf{r} + \frac{\mathbf{v}_0}{\sqrt{\epsilon}}\| \leq \|\mathbf{v}_{i,b_i}\| \cdot (\|\mathbf{r}\| + \frac{1}{\sqrt{\epsilon}}) \leq \frac{2}{\sqrt{\epsilon}} \|\mathbf{v}_{i,b_i}\| \tag{25}$$

概率为 $1 - O(\exp(-1/\sqrt{\epsilon}))$。结合（23）、（24）和（25），我们可得

$$\|\mathbf{v}_{i,b_i}\| \geq \frac{\sqrt{\epsilon}}{2} \langle \mathbf{v}_{i,b_i}, \mathbf{z} \rangle \geq \frac{\alpha \sqrt{\epsilon}}{2} \langle \mathbf{v}_0, \mathbf{z} \rangle \geq \frac{\alpha}{4} \tag{26}$$

概率为 $1 - O(\exp(-1/\sqrt{\epsilon}))$。

现在定义 $\mathbf{y}_i = \sum_{a \in A} w_{i,a} \mathbf{v}_{i,a}$ 对每个 $i \in [k]$。注意到 $\beta |A_{i,+}| \leq \beta |A| \leq \frac{1}{2}$。将式（22）与式（26）结合，可得

$$\|\mathbf{y}_i\| = \sqrt{\sum_{a \in A} w_{i,a}^2 \|\mathbf{v}_{i,a}\|^2} \geq |w_{i,b_i}| \|\mathbf{v}_{i,b_i}\| \geq \frac{\beta c_i}{2(1 - \beta |A_{i,+}|)} \cdot \frac{\alpha}{4} = \frac{\alpha \beta c_i}{8(1 - \beta |A_{i,+}|)} \geq \frac{\alpha \beta c_i}{8}$$

以 $1 - O(\exp(-1/\sqrt{\epsilon}))$ 的概率。现在注意到

$$\Pr\left(|\langle \mathbf{y}_i, \mathbf{z}\rangle| < \frac{8}{\alpha\beta}\eta\|\mathbf{y}_i\|\right) \le \frac{\frac{16}{\alpha\beta}\eta\|\mathbf{y}_i\|}{2\|\mathbf{y}_i\|} = \frac{8}{\alpha\beta}\eta$$

根据命题 (a) 的2.1部分。按照之前类似的方式使用定义 4。的5.1 第 4 部分，我们得到 $\langle \mathbf{y}_i, \mathbf{z}\rangle \le 0$；因此，

$$\Pr\left(\langle \mathbf{y}_i, \mathbf{z}\rangle < -\frac{8}{\alpha\beta}\eta\|\mathbf{y}_i\|\right) \ge 1 - \frac{8}{\alpha\beta}\eta.$$

因此，根据并集界，该性质

$$\langle \mathbf{y}_i, \mathbf{z}\rangle < -\frac{8}{\alpha\beta}\eta\|\mathbf{y}_i\| \quad \text{for each} \quad i \in [k]$$

以概率 $1 - O_{\alpha,A}(\eta)$ 成立。现在注意到

$$\eta \ge \frac{\delta+\gamma}{\sqrt{\epsilon}} \ge \frac{\delta}{\sqrt{\epsilon}} \ge \frac{2\epsilon\log(1/\epsilon)}{\sqrt{\epsilon}} \ge \sqrt{\epsilon} \ge \exp(-1/\sqrt{\epsilon})$$

当 ϵ 误差较小时 够了。因此，综合以上结果可知，以概率 $1 - O_{\alpha,A}(\eta)$，

$$\langle \mathbf{u}, \mathbf{z}\rangle = \sum_{i\in[k]}\langle \mathbf{y}_i, \mathbf{z}\rangle < -\frac{8}{\alpha\beta}\eta\sum_{i\in[k]}\|\mathbf{y}_i\| \le -\eta\sum_{i\in[k]} c_i = -\eta\|W\|_1 = -\eta,$$

从而与（21）矛盾。因此，在这种情况下，$\mathbf{b} \in Q$ 以概率 $1 - O_{\alpha,A}(\eta)$。

最后，回顾一下，$\eta = \sqrt{2(\delta+2\gamma)\log(1/\epsilon)} + \frac{\delta+\gamma}{\sqrt{\epsilon}}$，其中 $\delta = 2\max(\epsilon,\ \gamma)\log(1/\epsilon)$，而 γ 是我们的向量赋值在单个子句 $(P,\ Q)$ 上的误差。由于假设我们的实例是 $(1-\epsilon)$- 可满足的，因此我们知道 γ 在所有子句上的平均值至多为 ϵ，即 $\mathbb{E}[\gamma] \le \epsilon$，其中期望是对部分约束满足问题$(\mathbf{A},\ \mathbf{B})$实例的子句取的。因此，

$$\begin{aligned}
&\mathbb{E}[\delta] \le \mathbb{E}[2(\epsilon+\gamma)\log(1/\epsilon)] = 2(\epsilon+\mathbb{E}[\gamma])\log(1/\epsilon) \le 4\epsilon\log(1/\epsilon), \text{ and}\\
&\mathbb{E}[\eta] \le \sqrt{2(\mathbb{E}[\delta]+2\mathbb{E}[\gamma])\log(1/\epsilon)} + \frac{\mathbb{E}[\delta]+\mathbb{E}[\gamma]}{\sqrt{\epsilon}} \qquad \text{（詹森不等式）}\\
&\quad \le \sqrt{2(4\epsilon\log(1/\epsilon)+2\epsilon)\log(1/\epsilon)} + \frac{4\epsilon\log(1/\epsilon)+\epsilon}{\sqrt{\epsilon}}\\
&\quad \le 10\sqrt{\epsilon}\log(1/\epsilon).
\end{aligned}$$

总之，无论是 $\langle \mathbf{u},\ \mathbf{v}_0\rangle > \delta$ 还是 $\langle \mathbf{u},\ \mathbf{v}_0\rangle \le \delta$，半定规划的损失至多为 $O_{\alpha,\ A}(\sqrt{\epsilon}\log(1/\epsilon))$，符合要求。 □

容易验证，容许所有（奇数）元数多数多态的布尔承诺约束满足问题满足定理5.3的假设。（不过请注意，上述定理中的损失略差，相差一个$\log(1/\epsilon)$ 因子，相较于 $O(\sqrt{\epsilon})$ 损失，即我们在布尔多数情形中设法得到的损失，见定理4.1。）更有趣的是，定理5.3可应用于其他类别的承诺约束满足问题，其鲁棒可解性此前并不为人所知。这是通过将定义此类承诺约束满足问题的多态函数族与相应的舍入函数按定义5.1联系起来实现的。特别地，我们现在证明，任何部分约束满足问题只要包含相对多数多态性（所有元数）就满足定理5.3 的假设，因而鲁棒可解。

定义 5.5 ([BWŽ21]). 函数 $f : A^n \to A$ 是相对多数，如果

$$f(\mathbf{a}) = \mathrm{argmax}_{a\in A}\{\#\ of\ occurrences\ of\ a\ in\ \mathbf{a}\}$$

对所有$\mathbf{a} \in A^n$，打破平局的方式使得 f 具有对称性。

命题 5.6。 设(**A**,**B**) 连同 $A = B$ 是一个 *PCSP* 模板，且Pol(**A**, **B**) 包含所有元数的相对多数多态。则PCSP(**A**,**B**) 可通过半定规划鲁棒求解，损失为$O(\sqrt{\epsilon}\log(1/\epsilon))$。

证明。 考虑任意满足 $q_{\rho(\mathbf{q})} \geq q_a$ 的函数 ρ：$\mathbb{R}^A \to A$，对每个$\mathbf{q} \in \mathbb{R}^A$, $a \in A$ 均成立（即，ρ 是取最大值函数，平局时任意打破）。注意，ρ 对 $\alpha = \frac{1}{|A|}$是 α-保守的。我们声称 **(A, B)** 是 ρ-可分离的。

固定 (A, B) 的一个元数为 k的承诺关系 (P, Q)，并选取某个元组 $\mathbf{b} \in A^k \setminus Q$。令 $K \subseteq \mathbb{R}^{k\times A}$ 为集合 $\{\Pi_{\mathbf{a}}$ 的凸包：一个 $\in P\}$。再令 L 为 $\mathbb{R}^{k\times A}$ 的子集，其中 $\mathbf{b}$ 是（严格）相对多数坐标构成的向量。也就是说，当且仅当对每个$i \in [k]$ 和每个 $a \in A \setminus \{b_i\}$，都有$M_{i,b_i} > M_{i,a}$时，$M \in L$ 成立。注意，K 是闭集，而 L 是开集，且它们都是凸集。我们声称二者不相交。反设$M \in K \cap L$。由于 M 受一个有理系数不等式系统约束，我们可以假设存在一个族 $\{\lambda_{\mathbf{a}}$：一组和为 1 的有理非负权重 $\in P\}$，使得$M = \sum_{\mathbf{a}\in P} \lambda_{\mathbf{a}}\Pi_{\mathbf{a}}$。取一个正整数 n，使得每个 $\mathbf{a}$ 的 $n\lambda_{\mathbf{a}}$ 都是整数，并选取一个元数为 n的相对多数多态 $f \in$ Pol(A, B)。令 $\mathbf{c} \in A^k$ 为将 f逐坐标作用于元组列表 $\mathbf{a}^{(1)}, \mathbf{a}^{(2)}, \ldots, \mathbf{a}^{(n)} \in P$所得的元组，其中每个 $\mathbf{a}$ 出现 $n\lambda_{\mathbf{a}}$ 次。由于 f 是多态性，$\mathbf{c} \in Q$。另一方面，$M \in L$意味着对每个 $i \in [k]$ 和每个 $b_i \neq a \in A$，都有$M_{i,b_i} > M_{i,a}$。根据相对多数的定义，我们可推得 $\mathbf{c} = \mathbf{b} \notin Q$，矛盾。因此 $K \cap L = \emptyset$，如所声称。

利用关于凸体超平面分离的已知结果 [BV04], 由于 $\mathbb{R}^{k\times A}$是有限维的，存在一个线性算子 $W \in \mathbb{R}^{k\times A}$ 和一个标量 $\mu \in \mathbb{R}$ 使得对每个 $M \in K$ 都有 $\langle W, M\rangle_{\mathrm{F}} \geq \mu$，并且对每个 $M \in L$ 都有 $\langle W, M\rangle_{\mathrm{F}} < \mu$。我们断言 W 就是定义 5.1所要求的权重矩阵。

首先观察到，由于 L 是一个开锥，我们有 $\langle W, M\rangle_{\mathrm{F}} < \mu$ 对所有 $M \in L$成立，当且仅当 $\langle W, \lambda M\rangle_{\mathrm{F}} < \mu$ 对所有 $M \in L$ 和 $\lambda > 0$成立。令 $\lambda \to \infty$趋于极限，我们得到$\langle W, M\rangle_{\mathrm{F}} < 0$ 对所有 $M \in L$ 成立，且该不等式的右端不能再变得更小。换言之，我们可以不失一般性地假设 $\mu = 0$。然后，必要时只需重新缩放，我们也可以不失一般性地假设 W 的1-范数为1。因此，1。 成立。条件 $\langle W, M\rangle_{\mathrm{F}} \geq 0$ 对所有 $M \in K$ 成立，等价于 $\langle W, \Pi_{\mathbf{a}}\rangle_{\mathrm{F}} \geq 0$ 对所有$\mathbf{a} \in P$成立，因此3。 成立。为证明4。，只需注意到 ρ^{-1}(**b**)是 L的拓扑闭包的一个子集。因此，4。 由映射 $\bullet \mapsto \langle W, \bullet\rangle_{\mathrm{F}}$的连续性得出。

为了证明条件 2。，选择 $i \in [k]$。对于每个 $\alpha, \beta \geq 0$，考虑以下矩阵：

- $D(\alpha)$ 是一个 $k \times k$ 对角矩阵，其中第 i 个对角元素为 1，第 j 个对角元素为 α，对每个 $j \neq i$ 均如此；
- J 是一个 $k \times A$ 全一矩阵；
- $M_{(\alpha,\ \beta)} = D_{(\alpha)}(J + \beta\Pi_{\mathbf{b}})$;

- $N_{(\alpha,\beta)} = D_{(\alpha)}(-J + \beta\Pi_{\mathbf{b}})$.

注意，对每个 $\alpha > 0, \beta > 0$， $\rho(M_{(\alpha,\beta)}) = \rho(N^{(\alpha,\beta)}) = \mathbf{b}$。因此，由条件 4.可知， $\langle W, M_{(\alpha,\beta)}\rangle_{\mathrm{F}} \leq 0$ 且 $\langle W, N^{(\alpha,\beta)}\rangle_{\mathrm{F}} \leq 0$。利用 Frobenius 内积的连续性，我们推出

$$0 \geq \langle W, M^{(0,0)}\rangle_{\mathrm{F}} = \sum_{a\in A} w_{i,a} \qquad \text{and} \qquad 0 \geq \langle W, N^{(0,0)}\rangle_{\mathrm{F}} = -\sum_{a\in A} w_{i,a},$$

从而证明了所需的 $W\mathbf{1} = \mathbf{0}$。

总之，我们已经证明 $\mathrm{PCSP}(\mathbf{A}, \mathbf{B})$ 是 ρ-可分的，且对应于一个 $\frac{1}{|A|}$-保守函数ρ。因此，结论由定理 5.3得出。 □

6 等式保持鲁棒性

给定一个域 A，我们定义 $\mathrm{EQ}_A := \{(a, a) : a \in A\}$。类似地，对于定义域对 (A, B)，我们将 $\mathrm{EQ}_{A,B}$ 定义为承诺关系 $(\mathrm{EQ}_A, \mathrm{EQ}_B)$。作为一种非正式的简写，给定一个承诺模板 (A, B)，我们用 (A, B) + EQ 表示添加了 $\mathrm{EQ}_{A,B}$ 的承诺模板。固定参数 $0 < \alpha < \beta < 1$。如果存在一个多项式时间算法，使得当输入是一个变量集为 V 的实例，且存在一个映射 $g : V \to A$，强满足至少 $1 - \alpha$ 比例的约束时，该算法输出一个映射 $g' : V \to B$，弱满足至少 $1 - \beta$ 比例的约束，那么我们称 PCSP(A, B) 是 (α, β)-鲁棒的。

本节的主要目标是证明以下定理。

定理 6.1. 假设唯一博弈猜想成立。若 部分约束满足问题$(\mathbf{A}, \mathbf{B})$ 对某个 $0 < \alpha < \beta < 1$ 是(α, β)-鲁棒的，则部分约束满足问题$((\mathbf{A}, \mathbf{B}) +$ 等式约束$)$ 是$(\alpha_{\mathrm{EQ}}, \beta_{\mathrm{EQ}})$-鲁棒的

$$\alpha_{\mathrm{EQ}} = \Omega_{\mathbf{A}}(\alpha^2\beta^4), \tag{27}$$
$$\beta_{\mathrm{EQ}} = O_{\mathbf{B}}(\beta). \tag{28}$$

假设唯一博弈猜想是必要的，因为它将鲁棒算法的存在与基本半定规划的整数性比联系起来，见定理 6.4。通过将鲁棒性重新定义为基本半定规划的整数间隙，可以使定理 6.1 成为无条件定理，但本文不采用这种改写。

由上述结果可直接得出，在唯一博弈猜想成立的前提下，两个部分约束满足问题模板的多态运算集合之间存在小族同态[16]$\mathrm{Pol}(\mathbf{A},\mathbf{B}) \to \mathrm{Pol}(\mathbf{C}, \mathbf{D})$ 会保留鲁棒可解性。

推论 *6.2.* 设函数 $f : (0, 1) \to (0, 1)$，满足 $f(\epsilon) \to 0$ as $\epsilon \to 0$。在唯一博弈猜想成立的前提下，若 $\mathrm{Pol}(A, B) \to \mathrm{Pol}(C, D)$，且 (A, B) 是 f-鲁棒的，则 (C, D) 是 g-鲁棒的，其中$g(\epsilon) = O_{\mathbf{A},\mathbf{B},\mathbf{C},\mathbf{D}}(f(\epsilon^{1/6}))$。

证明。我们首先按照 [BG21a、BBKO21]中的做法，介绍一些代数 PCSP 理论的术语。固定一个关系签名 σ（即一个由关系符号组成的有限集 R_1， R_2，……，每个

[16]关于小群及其同态的定义，请参阅 [BBKO21]。

具有整数元数 $r_1, r_2, \ldots$）。域 σ 上的原始正合取公式是一个形式表达式 ψ，由存在量化的谓词合取构成，谓词的形式为（i）“$x = y$”，或（ii）“$(x_{i_1}, \ldots, x_{i_r}) \in R$”，其中某个 $R \in \sigma$ 的元数为 r，而 $x, y, x_{i_1}, \ldots, x_{i_r}$ 均为变量。设 k 为 ψ 中自由（即未量化）变量的数量。给定一个 σ-结构 A，ψ 在 A 中的解释是集合 $\psi(\mathbf{A}) \subseteq A^k$，其中包含所有满足 ψ 的元组 $(a_1, \ldots, a_k) \in A^k$；其中，出现在 ψ 中的每个符号 R 都在 A 中进行解释。现在设 A′ 是一个 σ'-结构，其签名 σ' 可能不同，并且满足 $A' = A$。若对每个符号 $S \in \sigma'$，都有 $S^{\mathbf{A}'} = \psi_S(\mathbf{A})$ 可由某个域 σ 上的原始正合取公式 ψ_S 定义，则称 A′ 可由 A 原始正合取定义。现在假设 $A' = A^n$ 对某个 $n \in \mathbb{N}$ 成立，并令 $\mathrm{vec}_n(\mathbf{A}')$ 为域为 A、关系定义如下的结构：对于每个 r 元符号 $S \in \sigma'$，$\mathrm{vec}_n(\mathbf{A}')$ 都有一个 rn 元关系；对于每个满足 $\in S^{\mathbf{A}'}$ 的元组 $(\mathbf{b}^{(1)}, \ldots, \mathbf{b}^{(r)})$，该关系包含元组 $(b_1^{(1)}, \ldots, b_n^{(1)}, \ldots, b_1^{(r)}, \ldots, b_n^{(r)})$。若 $\mathrm{vec}_n(\mathbf{A}')$ 可由 A 原始正合取定义，则称 A′ 是 A 的 n 重原始正合取幂。

现在，取 corollary 陈述中的 A、B、C 和 D，令 σ 为 A、B 的签名，令 σ' 为 C、D 的签名。[BBKO21 的定理 4.12] 证明了，存在小族同态 Pol(A, B) $\to$ Pol(C, D)，等价于存在 ˜ ˜ ˜ ˜ ˜两个 σ'-结构 A、B，使得 (i) C $\to$ A $\to$ B $\to$ D，且 (ii) A 和 B 分别是 A 和 B 的原始正合取幂，所用幂次相同（即 $n \in \mathbb{N}$），并且使用相同的原始正合取公式。

回顾一下，我们假设 PCSP(A, B) 是 f-鲁棒的。由定理 6.1 可知，对于 $g(\epsilon) = f(\epsilon^{1/6})$，PCSP((A, B) + EQ) 是 g-鲁棒的。根据 [BGS25 的命题 2.10],˜ ˜，我们推得 PCSP(vec_n(A), vec_n(B)) 是 $O_{\mathbf{A},\mathbf{B},}$ˆA ˜B(1) · g-鲁棒的。现在考虑从 PCSP(A, B) 到 PCSP(vec_n(A), vec_n(B)) 的（标准）归约，定义如下。对于 PCSP(A, B) 的一个˜ ˜ ˆ ˜ ˜实例 X，输出 PCSP(vec_n(A), vec_n(B) 的一个实例 X，其域包含每个 $x \in X$ 的 n 个副本 $x^{(1)}, \ldots, x^{(n)}$，其关系 $R^{\hat{\mathbf{X}}}$ 则对 $R^{\mathbf{X}}$ 中的每个元组 $(x_1, \ldots, x_r)$，包含元组 $(x_1^{(1)}, \ldots, x_1^{(n)}, \ldots, x_r^{(1)}, \ldots, x_r^{(n)})$。显然，这种归约 ˜ ˜ 以相同的损失保持鲁棒可解性，因此我们推得 PCSP(A, B) 是 $O_{\mathbf{A},\mathbf{B},}$ˆA ˜B(1)·$g$-˜ ˜ 鲁棒的。最后，由于 (C, D) 是 (A, B) 的同态松弛，我们得出 PCSP(C, D) 也满足同样的结论，从而证毕。 □

如引言中所述，推论 6.2 部分印证了 Barto 和 Kozik 提出的猜想1.4，该猜想归因于 Barto 和 Kozik [BK16]。定理 6.1 的证明相当复杂，因为它对 Brown-Cohen 和 Raghavendra 的算法进行了大量修改 [BR16],，而该算法本身是对 Raghavendra 算法的修改版本 [Rag08]。本节首先概述 Brown-Cohen 和 Raghavendra 的算法（下文简称*BCR* 算法）。

6.1 Brown-Cohen 和 Raghavendra 算法概述

本节将介绍 BCR 算法及其主要正确性保证。我们先介绍必要的预备知识。

6.1.1 BCR 预备知识

BCR 算法的一个关键要素是近似多态这一概念。对于承诺模板（$\mathbf{A}$,$\mathbf{B}$）和正整数 R，考虑映射 p: $A^R \to B$ 的概率分布 $\mathcal{P}$。

定义 *6.3*（近似多态性 [*BR*16]）。我们称 $\mathcal{P}$ 是 *(A, B)* 的 *(c, s)*-近似多态性，如果对于变量集 X 上 *PCSP(A, B)* 的所有（归一化）加权实例 $\mathcal{X}$，给定 R 个赋值 $a_1, \ldots, a_R \colon X \to A$，且每个赋值的值至少为 c，则

$$\mathbb{E}_{p\sim\mathcal{P}}[\mathrm{val}_{\mathcal{X}}(p \circ (a_1, \ldots, a_R))] \geq s,$$

其中，对所有 $x \in X$，我们都有 $(p \circ (a_1, \ldots, a_R))(x) = p(a_1(x) \ldots, a_R(x))$。

我们还定义 $\mathcal{P}$ 为（α, β）-鲁棒多态性，若 $\mathcal{P}$ 是（$1-\alpha, 1-\beta$）-近似多态。注意，存在许多参数良好的平凡近似多态，例如仅由独裁函数支撑的概率分布。为了识别“有意义的”近似多态，BCR 使用拟随机性 这一概念，以确保鲁棒/近似多态具有足够的非平凡性。

我们首先回顾一些标准的傅里叶分析概念。固定一个概率分布$\mu \in \Delta_A$，并令 $\{\chi_0 = 1, \ldots, \chi_{|A|-1}\}$ 为向量空间 $L_2(A, \mu)$的一组标准正交基。任意函数 $f \colon A^R \to \mathbb{R}$ 都可以写成 $f = \sum_{\sigma\in\mathbb{N}^R} \hat{f}_\sigma \chi_\sigma$，其中 $\chi_\sigma(x) = \prod_{j=1}^R \chi_{\sigma_j}(x_j)$，$\hat{}$且 f_σ 是 f的傅里叶系数。令 $|\sigma|$ 表示 σ的非零坐标数。在概率测度 μ下， f 的第 i 个坐标的次数 d 影响 定义为

$$\mathrm{Inf}_{i,\mu}^{<d}(f) = \sum_{\substack{\sigma\in\mathbb{N}^R \\ \sigma_i\neq 0 \\ |\sigma|<d}} \hat{f}_\sigma^2.$$

我们称近似多态性 $\mathcal{P}$ 是 (τ, d)-拟随机 的，如果对每一个概率测度 $\mu \in \Delta_A$，都有

$$\mathbb{E}_{p\sim\mathcal{P}}\left[\max_{i\in[R]} \mathrm{Inf}_{i,\mu}^{<d}(p)\right] \leq \tau.$$

为了描述 BCR 算法，我们还需要使用噪声算子。给定参数 $\rho \in [0, 1]$，我们令 T_ρ 为如下定义的算子：对每个函数 $f \colon A^R \to \mathbb{R}$,

$$T_\rho f(x) = \mathbb{E}_{y\sim_\rho x}[f(y)],$$

其中表达式“$y \sim_\rho x$”表示，对每个 $i \in [R]$， y_i 以概率 ρ 等于 x_i，而 y_i 以概率 $1-\rho$ 按照 μ 独立采样。由此定义可知，该算子的傅里叶展开由 $T_\rho f = \sum_{\sigma\in\mathbb{N}^R} \hat{f}_\sigma \rho^{|\sigma|} \chi_\sigma$ 给出。

6.1.2 BCR 算法

Brown-Cohen 和 Raghavendra 的主要结果 [BR16] 如下。

定理 *6.4*。对于任意 *PCSP* 模板 *(A, B)* 以及任意 $\theta > 0$，存在 $\tau > 0$ 和$d \in \mathbb{N}$，使得对每个 $0 < \alpha < \beta < 1$，若 *(A, B)* 具有一个 *(α, β)*-鲁棒的 *(τ, d)*-准随机多态映射，则 *BCR* 算法对 *PCSP(A, B)* 是 *(α−θ, β+θ)*-鲁棒的。反之，在假设唯一博弈猜想成立的前提下，若 *PCSP(A, B)* 具有任意 *(α, β)*-鲁棒算法，则对任意 $\theta > 0$，*PCSP(A, B)* 可通过上述算法过程得到一个 *(α − θ, β + θ)*-鲁棒算法。

我们现在给出 BCR 算法。令 $\Psi\colon \mathbb{R}^A \to \Delta_A$ 为 Δ_A 上恒等函数的一个利普希茨连续延拓。

- 设 $\mathcal{P}$ 是一个 R 元（d，τ）准随机（α，β）鲁棒多态性。选取足够小的 $\eta > 0$。
- 设 $\mathcal{X}$ 是定义在变量集 X 上的 PCSP(**A**，**B**) 加权实例。
- 针对 $\mathcal{X}$ 求解 CSP($\mathbf{A}$) 的基本半定规划，得到一个单位向量 $\mathbf{v}_0 \in \mathbb{R}^N$ 以及向量 $\mathbf{v}_{x,a} \in \mathbb{R}^N$ 对所有 $x \in X$ 和 $a \in A$ 其完备性至少为 $1-\alpha$（见第 6.2.2节）。
- 采样 $p \sim \mathcal{P}$ 并独立采样 R 向量 $\zeta^{(1)}, \dots, \zeta^{(R)} \sim \mathcal{N}(0^N, I_N)$。
- 对于所有 $x \in X$、$a \in A$ 和 $i \in [R]$，计算

$$g_{x,a,i} := \langle \mathbf{v}_{x,a}, \mathbf{v}_0 \rangle + \langle \mathbf{v}_{x,a} - \mathbf{v}_0 \langle \mathbf{v}_0, \mathbf{v}_{x,a} \rangle, \zeta^{(i)} \rangle.$$

- 对于每个 $x \in X$ 和 $i \in [R]$，计算

$$h_{x,i} := \Psi(g_{x,a,i} : a \in A).$$

- 令 H_η 为与函数 $T_{1-\eta}p : \Delta_A^R \to \Delta_B$ 对应的多重线性多项式。[17]对于每个 $x \in X$，

$$q_x := H_\eta(h_{x,1}, \dots, h_{x,R}) \in \Delta_B.$$

- 对于每个 $x \in X$，根据概率分布 q_x 分配 $\sigma(x)$。

6.2 配置与舍入方案

为了描述我们对 BCR 算法所做的修改，我们首先需要抽象出半定规划舍入方案的本质属性。

6.2.1 配置

给定一个单位向量 $\mathbf{v}_0 \in \mathbb{R}^N$，我们定义 $\mathbb{S}_A^N(\mathbf{v}_0) \subseteq (\mathbb{R}^N)^A$ 为所有满足以下条件的 A 元向量组 $\{\mathbf{v}_a : a \in A\}$ 的集合：

$$\langle \mathbf{v}_a, \mathbf{v}_{a'} \rangle = 0 \quad \forall a \neq a' \in A$$
$$\sum_{a \in A} \mathbf{v}_a = \mathbf{v}_0.$$

我们将这些 A 元组称为**局部配置**，通常记为 $\mathbf{V} \in \mathbb{S}_A^N$。注意，对每个 $a \in A$，都存在一个整数局部配置 $\mathbf{V} \in \mathbb{S}_A^N$，使得 $\mathbf{v}_a = \mathbf{v}_0$，且对所有 $a' \in A \setminus \{a\}$，都有 $\mathbf{v}_{a'} = 0$。我们用 $\mathbf{I}_a$ 表示这个整数局部配置。

[17]这里，我们将映射 $p\colon A^R \to B$ 解释为实值函数 $p\colon A^R \to \mathbb{R}^B$，其中 $p(\mathbf{a})_b = 1$ 若 $p(\mathbf{a}) = b$，否则为 0。然后，我们逐坐标应用噪声算子 $T_{1-\eta}$。可以证明，对任意 $\mathbf{a} \in \Delta_A^R$，都有 $T_{1-\eta}p(\mathbf{a}) \in \Delta_B$。

当$\mathbf{v}_0$ 在上下文中固定时，为了简洁起见，我们令 $\mathbb{S}_A^N$ 表示 $\mathbb{S}_A^N(\mathbf{v}_0)$。我们在 $\mathbb{S}_A^N$ 上定义一个（赋范）度量：

$$\|\mathbf{V}-\mathbf{V}'\|_2=\sqrt{\sum_{a\in A}\|\mathbf{v}_a-\mathbf{v}'_a\|_2^2}.$$

注意，如果将$\mathbf{V}$ 和$\mathbf{V}'$ 视为 $\mathbb{R}^{N\times A}$ 中的矩阵，那么上式就是弗罗贝尼乌斯矩阵范数。

现在，我们将全局配置 定义为局部配置的元组

$$\mathcal{V}:=(\mathbf{V}_x\in\mathbb{S}_A^N : x\in X)\in(\mathbb{S}_A^N)^X.$$

特别地，给定一个 $\in A^X$，我们用 $\mathcal{I}_{\mathbf{a}}:=(\mathbf{I}_{a_x}:\ x\in X)$ 表示整数全局配置。给定 $\mathcal{V}\in(\mathbb{S}_A^N)^X$，我们用 $\mathrm{Mat}(\mathcal{V})\in\mathbb{R}^{(X\times A)^2}$ 表示所有点积的格拉姆矩阵。也就是说，对于任意 $(x,a),(x',a')\in X\times A$，有

$$\mathrm{Mat}(\mathcal{V})_{(x,a),(x',a')}:=\langle\mathbf{v}_{x,a},\mathbf{v}_{x',a'}\rangle.$$

对于 一个 $\in A^X$，我们将 $\mathrm{Mat}(\mathbf{a})$ 作为 $\mathrm{Mat}(\mathcal{I}_{\mathbf{a}})$的简写。换言之 $\mathrm{Mat}(\mathbf{a})_{(x,a),(x',a')}=1$当且仅当 $\mathbf{a}_x=a$ 且 $\mathbf{a}_{x'}=a'$，否则为 0 。注意，$\mathrm{Mat}(\mathbf{a})$ 可视为克罗内克积 $\Pi_{\mathbf{a}}\otimes\Pi_{\mathbf{a}}$，其中 $\Pi_{\mathbf{a}}$ 的定义见第 5节。

需要注意的是，对于任意全局配置 $\mathcal{V}$，以下等式成立：

$$\mathrm{Tr}(\mathrm{Mat}(\mathcal{V}))=\sum_{(x,a)\in X\times A}\|\mathbf{v}_{x,a}\|_2^2=\sum_{x\in X}\|\mathbf{v}_0\|_2^2=|X|. \tag{29}$$

6.2.2 半定规划解与舍入方案

给定变量集 X 上的一个（带权）部分约束满足问题（$\mathbf{A}$,$\mathbf{B}$）实例 $\mathcal{X}$，其半定规划松弛的任意有效解都可以视为某个全局配置 $\mathcal{V}\in(\mathbb{S}_A^N)^X$，其中维度 N 足够大（尽管可以将其设为至多 $|X|\cdot|A|$，但我们通常会令 N 更大）。然而，并非每个 $\mathcal{V}\in(\mathbb{S}_A^N)^X$ 都是半定规划的有效解，因为 $\mathcal{X}$ 的每个子句 (Y,P,Q) 都会对 $\mathcal{V}$ 施加一定结构。更准确地说，若令 $\mathcal{V}|_Y:=(\mathbf{V}_y:\ y\in Y)$，则在 A^Y 上存在一个概率分布 $\Lambda_{Y,P}$，使得

$$\mathrm{Mat}(\mathcal{V}|_Y)=\mathop{\mathbb{E}}_{\mathbf{a}\sim\Lambda_{Y,P}}[\mathrm{Mat}(\mathbf{a})]. \tag{30}$$

我们称 $\Lambda_{Y,P}$ 与 一致 于 $\mathcal{V}$，如果（30）成立。注意，这正是二阶矩条件（3）的翻译，而一阶矩条件（2）已隐含在局部配置的定义中。

我们令 $\mathbb{V}^N_{\mathcal{X},\,A}\subseteq(\mathbb{S}_A^N)^X$ 表示所有满足 (30) 的 $\mathcal{V}\in(\mathbb{S}_A^N)^X$ 的集合，其中某个 $\Lambda_{Y,\,P}$ 的选择使得对 $\mathcal{X}$ 的所有约束 $(Y,\ P,\ Q)$ 均成立。我们进一步将映射 $\mathrm{comp}_{\mathcal{X},\,\mathbf{A}}:\mathbb{V}^N_{\mathcal{X},\,\mathbf{A}}\to[0,1]$ 定义为

$$\mathrm{comp}_{\mathcal{X},\mathbf{A}}(\mathcal{V}):=\max_{\substack{\{\Lambda_{Y,P}\mid(Y,P,Q)\in\mathcal{X}\}\\ \text{consistent with }\mathcal{V}}}\ \mathop{\mathbb{E}}_{(Y,P,Q)\sim\mathcal{X}}\left[\Pr_{\mathbf{a}\sim\Lambda_{Y,P}}[\mathbf{a}\in P]\right].$$

类似地，我们将 $\mathsf{sound}_{\mathcal{X},\mathbf{B}}: \Delta_B^X \to [0,1]$ 定义为

$$\mathrm{sound}_{\mathcal{X},\mathbf{B}}(\mathbf{z}) := \mathop{\mathbb{E}}_{(Y,P,Q)\sim\mathcal{X}} \left[\sum_{\mathbf{q}\in Q} \prod_{y\in Y} z_y(q_y) \right].$$

直观地说，$\mathsf{sound}_{\mathcal{X},\mathbf{B}}(\mathbf{z})$ 是通过按照分布 z_x 独立地为每个 $x \in X$ 从 B 中赋值后所得解的期望值。为了最大化可靠性，我们希望能够控制如何选择这些分布 $z_x \in \Delta_B$。这引出了（无须知晓输入的）舍入方案这一概念。

定义 6.5 (舍入方案)。设 Ξ 是一个概率分布。我们将一个（无须知晓输入的）舍入方案 定义为函数 $S: \mathbb{S}_A^N \times \Xi \to \Delta_B$。如果能够高效地计算 S，则称 S 为一个舍入算法。

定义 6.6 (鲁棒舍入方案)。对于约束满足问题实例 $\mathcal{X}$，若舍入方案 $S: \mathbb{S}_A^N \times \Xi \to \Delta_B$ 满足以下条件，则称其为(α,β)-鲁棒的：对于所有全局配置 $\mathcal{V} \in \mathbb{V}_{\mathcal{X},\mathbf{A}}^N$，都有

$$\mathrm{comp}_{\mathcal{X},\mathbf{A}}(\mathcal{V}) \geq 1-\alpha \implies \mathop{\mathbb{E}}_{\xi\sim\Xi}[\mathrm{sound}_{\mathcal{X},\mathbf{B}}(S(\mathbf{V}_x,\xi) : x \in X)] \geq 1-\beta.$$

请注意，一旦选定 $\xi \sim \Xi$，每个 $x \in X$ 都会根据 $(\mathbf{V}_x,\xi)S$ 独立舍入。然而， Ξ 中的随机性会带来非平凡的相关性，我们将对其进行系统分析。对于 BCR 算法，我们考虑概率分布 $\Xi_{N\,\theta}^{\mathrm{BCR}}$，$:= \mathcal{P} \times \mathcal{N}(0^N, I_N)^R$，其中 $\mathcal{P}$ 是在定理 6.4 中带来损失 θ 的、元数为 R 的 (α,β)-鲁棒准随机多态映射。于是，对于任意选择的 $N \in \mathbb{N}$ 和 $\theta > 0$，我们可以将 BCR 算法视为舍入算法 $\mathrm{BCR}_\theta^N: \mathbb{S}_A^N \times \Xi_N^{\mathrm{BCR}},_\theta \to \Delta_B$。特别地，一旦求得半定规划解，为每个变量指定的概率分布就只取决于 $\Xi_{N\,\theta}^{\mathrm{BCR}}$ 选定的全局随机性。由此，我们可以将定理 6.4 中的第二个推论重新表述如下。

推论 6.7. 假设唯一博弈猜想。若部分约束满足问题$(\mathbf{A},\mathbf{B})$是(α,β)-鲁棒的，则对任意 $\theta > 0$ 以及部分约束满足问题$(\mathbf{A},\mathbf{B})$的任意实例 $\mathcal{X}$，对所有充分大的 N（作为 θ和 $|\mathcal{X}|$的函数），$\mathrm{BCR}_\theta^N: \mathbb{S}_A^N \times \Xi_N^{\mathrm{BCR}},_\theta \to \Delta_B$是$(\alpha-\theta,\beta+\theta)$-鲁棒的。

利用推论6.7 作为我们所需的BCR 算法的唯一性质，我们将构造另一个满足定理6.1要求的舍入过程。

6.3 平滑配置

我们称，对某个 $\delta \geq 0$，若对所有 $x \in X$都有 $\|\mathbf{V}_x - \mathbf{W}_x\|_2^2 \leq \delta$，则 $\mathcal{V},\mathcal{W} \in (\mathbb{S}_A^N)^X$互为 δ-修改。我们令 $B(\mathcal{V},\delta) \subseteq \mathbb{V}_{\mathcal{X},\mathbf{A}}^N$表示 $\mathcal{V}$的所有 δ-修改构成的集合。注意，若 $\mathcal{V}$与 $\mathcal{W}$是满足$\mathcal{V} \in \mathbb{V}_{\mathcal{X},\mathbf{A}}^N$的 δ-修改，则未必有$\mathcal{W} \in \mathbb{V}_{\mathcal{X},\mathbf{A}}^N$，因为 $\mathcal{X}$中可能存在一个子句(Y,P,Q)，使得不存在与 $\mathcal{W}$一致的边缘分布$\Lambda_{Y,P}$。

作为关键定义，令 $\mathbb{V}^{N,\mathcal{X}^\delta},_{\mathbf{A}} := \bigcup_{\mathcal{V}\in\mathbb{V}_{\mathcal{X},\mathbf{A}}^N} B(\mathcal{V},\delta)$。作为构造我们的舍入方案的重要步骤，我们首先试图将 BCR_θ^N从对 $\mathbb{V}_{\mathcal{X},\mathbf{A}}^N$ 鲁棒扩展为对 $\mathbb{V}^{N,\mathcal{X}^\delta},_{\mathbf{A}}$鲁棒。

定义 6.8（宽松鲁棒舍入方案）. 给定 部分约束满足问题(**A,B**) 的实例 $\mathcal{X}$，我们称舍入方案 $S\colon \mathbb{S}_A^N \times \Xi \to \Delta_B$ 对 $\mathcal{X}$ 是 (δ,α,β)- 宽松鲁棒的，如果对于所有全局配置 $\mathcal{V} \in \mathbb{V}_{\mathcal{X},\mathbf{A}}^N$ 以及所有 $\mathcal{W} \in B(\mathcal{V},\delta)$，我们有

$$\mathrm{comp}_{\mathcal{X},\mathbf{A}}(\mathcal{V}) \geq 1-\alpha \implies \mathop{\mathbb{E}}_{\xi\sim\Xi}[\mathrm{sound}_{\mathcal{X},\mathbf{B}}(S(\mathbf{W}_x,\xi) : x \in X)] \geq 1-\beta.$$

显然，对于该部分约束满足问题的所有加权实例，任何宽裕鲁棒舍入方案都是鲁棒的，因为对任意 δ，$\mathcal{V} \in B(\mathcal{V},\delta)$。还需注意，一般而言 $\mathrm{comp}_{\mathcal{X},\mathbf{A}}(\mathcal{W})$ 未定义（因为如上所述，可能存在 $\mathcal{W} \notin \mathbb{V}_{\mathcal{X},\mathbf{A}}^N$），因此我们使用 $\mathcal{V}$ 的完备性作为替代。

6.3.1 平滑提升

给定一个 (α,β)-鲁棒方案 S，我们希望找到一种通用方法，将其转化为一个 (δ,α,β)-宽裕鲁棒方案 S'。为此，我们采用一种与 Raghavendra 和 Steurer 使用的填充技巧类似的方法 [RS 09]。

定义 6.9。给定 $\mathbf{u} \in \mathbb{R}^M$、$\mathbf{v} \in \mathbb{R}^N$ 和 $\rho \in [0,1]$，令 $\mathbf{u} \oplus_\rho \mathbf{v} \in \mathbb{R}^{M+N}$ 为 连接 $\mathbf{u}$ 与 $\mathbf{v}$；也就是说，它是由下式定义的向量

$$(\mathbf{u} \oplus_\rho \mathbf{v})_i := \begin{cases} \sqrt{\rho}u_i & i \in [M] \\ \sqrt{1-\rho}v_i & i \in [M+N]\setminus[M]. \end{cases}$$

对每个 $i \in [M+N]$。

定义 6.10. 给定 $\mathbf{U} \in \mathbb{S}_A^M(\mathbf{u}_0)$、$\mathbf{V} \in \mathbb{S}_A^N(\mathbf{v}_0)$ 和 $\rho \in [0,1]$，我们将 $\mathbf{U}$ 与 $\mathbf{V}$ 的 ρ-拼接定义为列表 $\mathbf{U} \oplus_\rho \mathbf{V} := (\mathbf{u}_a \oplus_\rho \mathbf{v}_a : a \in A)$。

命题 6.11. $\mathbf{U} \oplus_\rho \mathbf{V} \in \mathbb{S}_A^{M+N}(\mathbf{u}_0 \oplus_\rho \mathbf{v}_0)$。

证明。首先，对于任意不同的 $a,a' \in A$，我们有

$$\langle \mathbf{u}_a \oplus_\rho \mathbf{v}_a, \mathbf{u}_{a'} \oplus_\rho \mathbf{v}_{a'}\rangle = \rho\langle \mathbf{u}_a,\mathbf{u}_{a'}\rangle + (1-\rho)\langle \mathbf{v}_a,\mathbf{v}_{a'}\rangle = 0.$$

其次，

$$\sum_{a\in A} \mathbf{u}_a \oplus_\rho \mathbf{v}_a = \left(\sum_{a\in A}\mathbf{u}_a\right) \oplus_\rho \left(\sum_{a\in A}\mathbf{v}_a\right) = \mathbf{u}_0 \oplus_\rho \mathbf{v}_0. \qquad \square$$

同样，对于 $\mathcal{U} \in (\mathbb{S}_A^M)^X$ 和 $\mathcal{V} \in (\mathbb{S}_A^N)^X$，我们可以定义 $\mathcal{U} \oplus_\rho \mathcal{V} := (\mathbf{U}_x \oplus_\rho \mathbf{V}_x : x \in X)$。回顾全局配置 $\mathrm{Mat}(\mathcal{V})$的格拉姆矩阵，它在第 6.2.1节中定义。

命题 6.12。$\mathrm{Mat}(\mathcal{U} \oplus_\rho \mathcal{V}) = \rho\,\mathrm{Mat}(\mathcal{U}) + (1-\rho)\,\mathrm{Mat}(\mathcal{V})$。

证明。对于任意 x，$x' \in X$ 和 a，$a' \in A$，我们有

$$\begin{aligned} \mathrm{Mat}(\mathcal{U} \oplus_\rho \mathcal{V})_{(x,a),(x',a')} &= \langle \mathbf{u}_{x,a} \oplus_\rho \mathbf{v}_{x,a}, \mathbf{u}_{x',a'} \oplus_\rho \mathbf{v}_{x',a'}\rangle. \\ &= \rho\langle \mathbf{u}_{x,a},\mathbf{u}_{x',a'}\rangle + (1-\rho)\langle \mathbf{v}_{x,a},\mathbf{v}_{x',a'}\rangle \\ &= \rho\,\mathrm{Mat}(\mathcal{U})_{(x,a),(x',a')} + (1-\rho)\,\mathrm{Mat}(\mathcal{V})_{(x,a),(x',a')}, \end{aligned}$$

如所需。 $\square$

现在，我们构造一个特定的全局配置 $\mathcal{U}$，它将有助于我们的舍入方案。

定义 6.13。 我们称 $\mathcal{U}_{X,A} \in (\mathbb{S}_A^M)^X$ 为均匀 配置，若对于所有 $x, x' \in X$和 $a, a' \in A$，都有

$$\langle \mathbf{u}_{x,a}, \mathbf{u}_{x',a'} \rangle = \begin{cases} \frac{1}{|A|} & x = x' \text{ and } a = a' \\ 0 & x = x' \text{ and } a \neq a' \\ \frac{1}{|A|^2} & \text{otherwise.} \end{cases}$$

命题 6.14。 对于 $M = |X| \cdot |A|$, $\mathcal{U}_{X,A}$ 是良定义的。此外，对于任意约束满足问题$\mathrm{CSP}(\mathbf{A})$的实例 $\mathcal{X}$，都有 $\mathcal{U}_{X,A} \in \mathbb{V}_{\mathcal{X},\mathbf{A}}^M$。

证明。 首先，容易验证

$$\mathrm{Mat}(\mathcal{U}_{X,A}) = \frac{1}{|A|^{|X|}} \sum_{\mathbf{a} \in A^X} \mathrm{Mat}(\mathbf{a}).$$

因此，Mat($\mathcal{U}_{X,A}$) 是半正定的，因而在 $\mathbb{R}^{|X|\cdot|A|}$ 中有一个实现。现在，对于变量集 $Y \subseteq X$ 上的 $\mathcal{X}$ 的任意子句 P，我们也可以验证

$$\mathrm{Mat}(\mathcal{U}_{X,A})|_{(Y\times A)^2} = \frac{1}{|A|^{|Y|}} \sum_{\mathbf{a} \in A^Y} \mathrm{Mat}(\mathbf{a}).$$

因此，对于 $\mathcal{X}$, $\mathcal{U}_X$ 的每个子句，A 与均匀随机赋值一致。因此，$\mathcal{U}_{X,A} \in \mathbb{V}_{\mathcal{X},\mathbf{A}}^M$.

□

给定 $\mathcal{V} \in (\mathbb{S}_A^N)^X$和 $\rho \in [0,1]$，我们令 $\mathcal{U}_{X,A} \oplus_\rho \mathcal{V} \in (\mathbb{S}_A^{M+N})^X$为 ρ-提升 of $\mathcal{V}$。接下来我们使用 ρ-提升，使 (30) 更有可能为真。

6.3.2 提升 δ-修改

我们当前的目标是证明以下引理。

引理 6.15. 设 $\mathcal{X}$ 是一个 部分约束满足问题(**A**,**B**) 的加权实例。对于任意 $\delta > 0$，存在 $\rho = O_{\mathbf{A}}(\sqrt{\delta}) \in [0,1]$，使得对所有 $\mathcal{V} \in \mathbb{V}_{\mathcal{X},\mathbf{A}}^N$ 以及 $\mathcal{W} \in B(\mathcal{V}, \delta)$，都有

(1) $\mathcal{U}_{X,A} \oplus_\rho \mathcal{W} \in \mathbb{V}_{\mathcal{X}}^{|X|\cdot|A|+N}{}_{,\mathbf{A}}$.

(2) $\mathrm{comp}_{\mathcal{X},\mathbf{A}}(\mathcal{U}_{X,A} \oplus_\rho \mathcal{W}) \geq \mathrm{comp}_{\mathcal{X},\mathbf{A}}(\mathcal{V}) - O_{\mathbf{A}}(\sqrt{\delta})$.

为了证明这个引理，我们需要借助凸几何中的一些工具。部分思路受到 Raghavendra–Steurer [RS09] 以及 [BGS25]附录 A 中内容的启发。我们先从一个简单的命题开始。

命题 6.16. 设$\mathbf{u}$、$\mathbf{u}'$、$\mathbf{v}$、$\mathbf{v}' \in \mathbb{R}^N$为长度至多为1的向量，且 $\|\mathbf{u} - \mathbf{u}'\|_2^2 \leq \delta$以及 $\|\mathbf{v} - \mathbf{v}'\|_2^2 \leq \delta$。那么 $|\langle \mathbf{u}, \mathbf{v} \rangle - \langle \mathbf{u}', \mathbf{v}' \rangle| \leq 2\sqrt{\delta}$。

证明。 根据柯西–施瓦茨不等式，注意到

$$\begin{aligned}|\langle \mathbf{u},\mathbf{v}\rangle - \langle \mathbf{u}',\mathbf{v}'\rangle| &\le |\langle \mathbf{u},\mathbf{v}\rangle - \langle \mathbf{u},\mathbf{v}'\rangle| + |\langle \mathbf{u},\mathbf{v}'\rangle - \langle \mathbf{u}',\mathbf{v}'\rangle| \\ &\le \|\mathbf{u}\|_2\|\mathbf{v}-\mathbf{v}'\|_2 + \|\mathbf{u}-\mathbf{u}'\|_2\|\mathbf{v}'\|_2 \\ &\le 2\sqrt{\delta}.\end{aligned}$$

□

接下来，我们固定一个有限（非空）集合 Y。我们令 $K_{Y,A}, K^0_{Y,A} \subseteq \mathbb{R}^{(Y\times A)^2}$ 表示如下两个凸集，它们是 $\mathbb{R}^{(Y\times A)^2}$ 的线性子空间：

$$K_{Y,A} := \left\{ \sum_{\mathbf{a}\in A^Y} \lambda_{\mathbf{a}} \operatorname{Mat}(\mathbf{a}) : \lambda_{\mathbf{a}} \in \mathbb{R} \right\},$$

$$K^0_{Y,A} := \left\{ \sum_{\mathbf{a}\in A^Y} \lambda_{\mathbf{a}} \operatorname{Mat}(\mathbf{a}) : \sum_{\mathbf{a}\in A^Y} \lambda_{\mathbf{a}} = 0 \right\}.$$

我们将需要如下关键引理。它可以直接由超矩阵低维投影的组合刻画导出，该刻画证明于 [CŽ23a]。此外，我们还给出一个涉及对偶空间 $K^*_{Y,A}$ 的 $K_{Y,A}$。两个论证的全部细节均推迟至第 A节。

引理 6.17. 对任意 $\mathcal{V}$、$\mathcal{W} \in (\mathbb{S}^N_A)^Y$，我们有

(1) $\operatorname{Mat}(\mathcal{V}) \in K_{Y,A}$. *(2)* $\operatorname{Mat}(\mathcal{V}) - \operatorname{Mat}(\mathcal{W}) \in K^0_{Y,A}$.

我们只需要再引入一点工具，然后就可以证明引理 6.15。定义集合

$$L_{Y,A} := \{M \in K^0_{Y,A} : \|M\|_\infty \le 1\},$$

其中 $\|M\|_\infty$ 是 M 的最大元素的绝对值。注意 $L_{Y,A}$ 是凸且紧的。再定义函数 $f : K^0_{Y,A} \to \mathbb{R}_{\ge 0}$ 为

$$f(M) := \min_{\substack{\lambda \\ \sum_{\mathbf{a}} \lambda_{\mathbf{a}} = 0 \\ \sum_{\mathbf{a}} \lambda_{\mathbf{a}} \operatorname{Mat}(\mathbf{a}) = M}} \max_{\mathbf{a}\in A^Y} |\lambda_{\mathbf{a}}|.$$

我们现在证明如下结论。

命题 6.18. $\kappa_{Y,A} := \text{上确界}_{M\in L_{Y,A}} f(M)$ 是有限的。

证明。 任取 $M_1, \dots, M_r$ 的一组基 $K^0_{Y,A}$。容易看出，对于所有 $i \in [r]$，都有 $f(M_i) < \infty$。此外，若 $M = \beta_1 M_1 + \cdots + \beta_r M_r$，则

$$f(M) \le \sum_{i=1}^r |\beta_i| f(M_i). \tag{31}$$

令 $g(M)$ 为 (31) 的右端。由于 $M_1, \dots, M_r$ 构成一个基，映射 $M \mapsto (\beta_1, \dots, \beta_r)$ 是连续的。因此， $g(M)$ 是连续的。因此，由于 L 是紧的，$\max_{M\in L_{Y,A}} g(M)$ 存在且为有限值。因此，$\kappa_{Y,A} := \sup_{M\in L_{Y,A}} f(M)$ 也是有限的。 □

我们还需要以下事实。

命题 6.19。 我们有 $\mathcal{U}_{X,\ A} \oplus_\rho \mathcal{V} \in \mathbb{V}_{\mathcal{X}}^{|X|\cdot|A|+N}$，$\mathbf{A}$ 和

$$\operatorname{comp}_{\mathcal{X},\mathbf{A}}(\mathcal{U}_{X,A} \oplus_\rho \mathcal{V}) \geq \operatorname{comp}_{\mathcal{X},\mathbf{A}}(\mathcal{V}) - O_{\mathbf{A}}(\rho). \tag{32}$$

证明。固定 $\mathcal{X}$ 中的一个子句 (Y, P)，其中 $Y \subseteq X$ 且 $P \in \mathbf{A}$。选取一个概率分布 $(p_{\mathbf{a}} : 一个 \in A^Y)$，使得 $\mathsf{Mat}(\mathcal{V}|_Y) = \sum_{\mathbf{a}\in A^Y} p_{\mathbf{a}} \mathsf{Mat}(\mathbf{a})$，且 $\mathsf{comp}_{Y,P}(\mathcal{V}|_Y) = \sum_{\mathbf{a}\in P} p_{\mathbf{a}}$。通过与命题 6.14 类似的方法，我们可以观察到

$$\operatorname{Mat}((\mathcal{U}_{X,A} \oplus_\rho \mathcal{V})|_Y) = \sum_{\mathbf{a}\in A^Y} \left(\frac{\rho}{|A|^{|Y|}} + (1-\rho)p_{\mathbf{a}} \right) \operatorname{Mat}(\mathbf{a}). \tag{33}$$

因此，$\mathcal{U}_{X,\ A} \oplus_\rho \mathcal{V} \in \mathbb{V}_{\mathcal{X}}^{|X|\cdot|A|+N}$，$\mathbf{A}$ 和

$$\begin{aligned}
\operatorname{comp}_{Y,P}((\mathcal{U}_{X,A} \oplus_\rho \mathcal{V})|_Y) &\geq \sum_{\mathbf{a}\in P} \left(\frac{\rho}{|A|^{|Y|}} + (1-\rho)p_{\mathbf{a}} \right) \operatorname{Mat}(\mathbf{a}) \\
&\geq (1-\rho) \operatorname{comp}_{Y,P}(\mathcal{V}|_Y) \\
&\geq \operatorname{comp}_{Y,P}(\mathcal{V}|_Y) - O_{\mathbf{A}}(\rho),
\end{aligned}$$

这里我们用到完备性至多为 1。对 $\mathcal{X}$ 的所有子句，将上述不等式取平均，得到 (32)。

□

引理 *6.15* 的证明。 暂且令 $\rho \in [0,1]$ 任意。固定 $\mathcal{X}$ 中的一个子句 $(Y,\ P,\ Q)$。令 $\mathcal{V}' := (\mathcal{U}_{X,\ A} \oplus_\rho \mathcal{V})|_Y$，且令 $\mathcal{W}' := (\mathcal{U}_{X,\ A} \oplus_\rho \mathcal{W})|_Y$。要证明 (1)，只需证明 $\mathcal{W}'$ 有一个解满足 (30)。回想命题 6.19 和 (33)，可得 $\mathcal{V}' \in \mathbb{V}_{YP}^{|X|\cdot|A|+N}$，和

$$\operatorname{Mat}(\mathcal{V}') = \sum_{\mathbf{a}\in A^Y} \left(\frac{\rho}{|A|^{|Y|}} + (1-\rho)p_{\mathbf{a}} \right) \operatorname{Mat}(\mathbf{a}).$$

由于 $\mathcal{W} \in B(\mathcal{V}, \delta)$，我们有 $\|(\mathcal{U}_{X,A} \oplus_\rho \mathcal{V}) - (\mathcal{U}_{X,A} \oplus_\rho \mathcal{W})\|_2^2 \leq (1-\rho)\delta$。根据命题 6.16，我们有：

$$\|\operatorname{Mat}(\mathcal{V}') - \operatorname{Mat}(\mathcal{W}')\|_\infty \leq 2\sqrt{(1-\rho)\delta}.$$

也就是说，$\frac{1}{2\sqrt{(1-\rho)\delta}}(\mathsf{Mat}(\mathcal{W}') - \mathsf{Mat}(\mathcal{V}')) \in L_{Y,\ A}$。因此，根据引理 6.17 和命题 6.18，存在一种对所有 $\mathbf{a} \in A^Y$ 的 $\lambda_{\mathbf{a}} \in \mathbb{R}$ 选择，使得 $\mathsf{Mat}(\mathcal{W}') - \mathsf{Mat}(\mathcal{V}') = \sum_{\mathbf{a}\in A^Y} \lambda_{\mathbf{a}} \mathsf{Mat}(\mathbf{a})$ 且 $|\lambda_{\mathbf{a}}| \leq 2\kappa_{Y,\ A}\sqrt{(1-\rho)\delta}$。取满足下述条件的最小 ρ

$$2\kappa_{Y,A}\sqrt{(1-\rho)\delta} \leq \frac{\rho}{|A|^{|Y|}}$$

对于 $\mathcal{X}$ 的每个子句 $(Y,\ P,\ Q)$。注意，$\rho = O_{\mathbf{A}}(\sqrt{\delta})$，且 $\rho \in [0,1]$，因为当 $\rho = 1$ 时，左端为 0。因此，我们现在有

$$\operatorname{Mat}(\mathcal{W}') = \sum_{\mathbf{a}\in A^Y} \left(\frac{\rho}{|A|^{|Y|}} + \lambda_{\mathbf{a}} + (1-\rho)p_{\mathbf{a}} \right) \operatorname{Mat}(\mathbf{a}),$$

其中每个系数都非零。因此， $\mathcal{W}'$ 满足（30），所以 $\mathcal{U}_{X,\,A} \oplus_\rho \mathcal{W} \in \mathbb{V}^{|X|\cdot|A|+N}{}_{\mathbf{X},\,\mathbf{A}}$。这证明了（1）。

为证明 (2)，注意，对于 $\mathcal{X}$ 的固定子句 $(Y,\ P,\ Q)$，我们有

$$\begin{aligned}\mathrm{comp}_{Y,P}(\mathcal{U}_{X,A} \oplus_\rho \mathcal{W}) &\geq \sum_{\mathbf{a}\in P}\left(\frac{\rho}{|A|^{|Y|}} + \lambda_{\mathbf{a}} + (1-\rho)p_{\mathbf{a}}\right)\\ &\geq (1-\rho)\sum_{\mathbf{a}\in P} p_{\mathbf{a}}\\ &= (1-\rho)\,\mathrm{comp}_{Y,P}(\mathcal{V})\\ &\geq \mathrm{comp}_{Y,P}(\mathcal{V}) - O_{\mathbf{A}}(\sqrt{\delta}).\end{aligned}$$

对 $\mathcal{X}$ 的所有子句 $(Y,\ P,\ Q)$ 对此不等式取平均，即可得到 (2)，如所需。 □

6.3.3 拉回方案

一般而言，要使半定规划舍入方案具有鲁棒性，我们需要保证彼此接近的半定规划向量在舍入后具有相似的可靠性。先验地，我们并不知道 BCR舍入方案是否具有这一性质。为此，我们将展示如何运用一种称为“拉回方案”的技术来平滑BCR 舍入方案。在第6.5节中，我们还将进一步修改拉回方案，使其具有更强的鲁棒性。

对于固定的 $\theta > 0$ 以及 PCSP(**A**，**B**) 的固定实例 $\mathcal{X}$，根据推论 6.7，存在 N，使得 $\mathrm{BCR}_\theta^{N'}$ 对所有 $N' \geq N$ 都是 $\mathcal{X}$ 的 $(\alpha-\beta,\ \beta+\theta)$-鲁棒方案。特别地，对于任意有限集 Z，$\mathrm{BCR}_\theta^{|Z|\cdot|A|+N}$ 都是 $\mathcal{X}$ 的 $(\alpha-\theta,\ \beta+\theta)$-鲁棒方案。现在，我们对任意 $\delta \in (0,\ 1)$ 定义一个拉回方案 $\widehat{\mathrm{BCR}}_\theta^{N\,Z}{}_{,\,,\rho}$，如下所示。

定义 6.20（拉回方案）。对于任意有限集 Z，我们定义 $\widehat{\mathrm{BCR}}_{\theta\,\delta}^{N\,Z}{}_{,,:}\ \ \mathbb{S}_A^N \times^{\Xi^{\mathrm{BCR}}_{|Z|\cdot|A|+N,}}_{\theta} \to \Delta_B$ 为

$$\widehat{\mathrm{BCR}}_{\theta,\delta}^{N,Z}(\mathbf{V},\xi) = \mathop{\mathbb{E}}_{z\sim Z}\left[\mathrm{BCR}_\theta^{|Z|\cdot|A|+N}(\mathbf{U}_z \oplus_\rho \mathbf{V},\xi)\right],$$

其中 $z \sim Z$ 是均匀分布，$\mathbf{U}_z$ 是 z-*th* 个局部配置，属于 $\mathcal{U}_{Z,A}$，且$\rho = O_{\mathbf{A}}(\sqrt{\delta})$ 根据引理 *6.15*选取。

请注意，我们称之为“拉回”方案，因为我们将高维舍入方案映射到低维。现在证明这个拉回方案具有宽裕鲁棒性。

引理 6.21。若 $\mathrm{BCR}_\theta^{|X|\cdot|A|+N}$ 是实例 $\mathcal{X}$ 上PCSP$(\mathbf{A},\mathbf{B})$的一个$(\alpha-\theta,\beta+\theta)$-鲁棒方案，则 $\widehat{\mathrm{BCR}}_{\theta\,\delta}^{N\,Z}{}_{,,}$是 $\mathcal{X}$的一个$(\delta,\alpha',\beta+\theta+\frac{|X|^2}{|Z|})$-宽裕鲁棒方案，其中$\alpha' = \alpha-\theta-O_{\mathbf{A}}(\sqrt{\delta})$。

证明。设 $\mathcal{V} \in \mathbb{V}^N_{\mathcal{X},\,\mathbf{A}}$ 满足 $\mathrm{comp}_{\mathcal{X},\,\mathbf{A}}(\mathcal{V}) \geq 1-\alpha'$。设 $\mathcal{W} \in B(\mathcal{V},\ \delta)$。根据定义 6.20 与

由于 $\mathsf{sound}_{\mathcal{X},\mathbf{B}}$ 是多重线性的这一事实，我们有

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\xi\sim\Xi^{\mathrm{BCR}}_{|Z|\cdot|A|+N,\theta}}[\mathrm{sound}_{\mathcal{X},\mathbf{B}}(\widehat{\mathrm{BCR}}^{N,Z}_{\theta,\delta}(\mathbf{W}_x,\xi):x\in X)]\\
&\qquad=\mathop{\mathbb{E}}_{\xi\sim\Xi^{\mathrm{BCR}}_{|Z|\cdot|A|+N,\theta}}\left[\mathrm{sound}_{\mathcal{X},\mathbf{B}}\left(\mathop{\mathbb{E}}_{z\sim Z}\left[\mathrm{BCR}^{|Z|\cdot|A|+N}_{\theta}(\mathbf{U}_z\oplus_\rho\mathbf{W}_x,\xi)\right]:x\in X\right)\right]\\
&\qquad=\mathop{\mathbb{E}}_{\substack{\xi\sim\Xi^{\mathrm{BCR}}_{|Z|\cdot|A|+N,\theta}\\ \mathbf{z}\sim Z^X}}\left[\mathrm{sound}_{\mathcal{X},\mathbf{B}}\left(\mathrm{BCR}^{|Z|\cdot|A|+N}_{\theta}(\mathbf{U}_{z_x}\oplus_\rho\mathbf{W}_x,\xi):x\in X\right)\right],
\end{aligned}$$

其中，$\mathbf{z}\sim Z^X$是均匀随机选取的。对于每个$\mathbf{z}\in Z^X$，令 $\mathcal{W}_{\mathbf{z}}:=(\mathbf{U}_{z_x}\oplus_\rho\mathbf{W}_x:\ x\in X)$。如果 $\mathbf{z}$ 是单射——也就是说，如果 $z_x=z_{x'}$ 蕴含 $x=x'$——那么我们断言

$$\mathrm{Mat}(\mathcal{W}_{\mathbf{z}})=\mathrm{Mat}(\mathcal{U}_{X,A}\oplus_\rho\mathcal{W}).$$

要说明原因，对于所有 $x,x'\in X$ 和 $a,a'\in A$，我们有

$$\begin{aligned}
\mathrm{Mat}(\mathcal{W}_{\mathbf{z}})_{(x,a),(x',a')}&=\rho\langle\mathbf{U}_{z_x,a},\mathbf{U}_{z_{x'},a'}\rangle+(1-\rho)\langle\mathbf{W}_{x,a},\mathbf{U}_{x',a'}\rangle\\
&=\rho\langle\mathbf{U}_{x,a},\mathbf{U}_{x',a'}\rangle+(1-\rho)\langle\mathbf{W}_{x,a},\mathbf{U}_{x',a'}\rangle\qquad(z\text{ injective})\\
&=\mathrm{Mat}(\mathcal{U}_{X,A}\oplus_\rho\mathcal{W})_{(x,a),(x',a')}.
\end{aligned}$$

因此，根据引理 6.15，对于所有单射$\mathbf{z}$，我们有 $\mathcal{W}_{\mathbf{z}}\in\mathbb{V}_{\mathcal{X}}^{|Z|\cdot|A|+N,\mathbf{A}}$ 以及

$$\mathrm{comp}_{\mathcal{X},\mathbf{A}}(\mathcal{W}_{\mathbf{z}})\geq\mathrm{comp}_{\mathcal{X},\mathbf{A}}(\mathcal{V})-O_{\mathbf{A}}(\sqrt{\delta})=1-\alpha+\theta.$$

因此，由于 $\mathsf{BCR}^{|X|\cdot|A|+N}_{\theta}$ 是$(\alpha-\theta,\beta+\theta)$-鲁棒的，我们有

$$\begin{aligned}
1-\beta-\theta&\leq\mathop{\mathbb{E}}_{\substack{\xi\sim\Xi^{\mathrm{BCR}}_{|Z|\cdot|A|+N,\theta}\\ \mathbf{z}\sim Z^X}}\left[\mathrm{sound}_{\mathcal{X},\mathbf{B}}\left(\mathrm{BCR}^{|Z|\cdot|A|+N}_{\theta}(\mathbf{U}_{z_x}\oplus_\rho\mathbf{W}_x,\xi):x\in X\right)\Big|\ \mathbf{z}\text{ injective}\right]\\
&\leq\frac{1}{\Pr_{\mathbf{z}\sim Z^X}[\mathbf{z}\text{ injective}]}\mathop{\mathbb{E}}_{\substack{\xi\sim\Xi^{\mathrm{BCR}}_{|Z|\cdot|A|+N,\theta}\\ \mathbf{z}\sim Z^X}}\left[\mathrm{sound}_{\mathcal{X},\mathbf{B}}\left(\mathrm{BCR}^{|Z|\cdot|A|+N}_{\theta}(\mathbf{U}_{z_x}\oplus_\rho\mathbf{W}_x,\xi):x\in X\right)\right]\\
&=\frac{1}{\Pr_{\mathbf{z}\sim Z^X}[\mathbf{z}\text{ injective}]}\mathop{\mathbb{E}}_{\xi\sim\Xi^{\mathrm{BCR}}_{|Z|\cdot|A|+N,\theta}}[\mathrm{sound}_{\mathcal{X},\mathbf{B}}(\widehat{\mathrm{BCR}}^{N,Z}_{\theta,\delta}(\mathbf{W}_x,\xi):x\in X)].
\end{aligned}$$

最后，我们注意到

$$\Pr_{\mathbf{z}\sim Z^X}[\mathbf{z}\text{ injective}]=\prod_{i=1}^{|X|}\left(1-\frac{i-1}{|Z|}\right)\geq1-\frac{|X|^2}{|Z|},$$

so

$$\mathop{\mathbb{E}}_{\xi\sim\Xi^{\mathrm{BCR}}_{|Z|\cdot|A|+N,\theta}}[\mathrm{sound}_{\mathcal{X},\mathbf{B}}(\widehat{\mathrm{BCR}}^{N,Z}_{\theta,\delta}(\mathbf{W}_x,\xi):x\in X)]\geq(1-\beta-\theta)\cdot(1-\frac{|X|^2}{|Z|})\geq1-\beta-\theta-\frac{|X|^2}{|Z|},$$

如所需。 □

6.4 测度论基础

为了证明定理6.1，我们接下来要做的是将BCR 改为另一种方案（我们将其称为REQ），使相似的输入产生相似的输出。为此，我们首先需要掌握一些测度论基础知识。基础概念可参阅 DiBenedetto 的教材 [DiB16] 。

设 R 是一个可能为无限的集合，并设 $\mathcal{R} := (R, \mu)$ 是定义在 R 上的概率测度。精确定义请参见 [DiB16] 的第 3 章。回顾一下，函数 $f : R \to \mathbb{R}^d$ 是可测的，当且仅当对 f 下 $\mathbb{R}^d$ 的每个可测子集，其原像都是可测的。再令 $\int_R$ 表示在 R 上的勒贝格积分。我们将考虑集合 $L^{2,2}(\mathcal{R}, \mathbb{R}^d)$，它由所有满足 $\int_R \|f(x)\|_2^2 \, d\mu(x) < \infty$ 的可测函数 $f: R \to \mathbb{R}^d$ 构成，并对等价关系“∼”取商；该等价关系定义为： $f \sim g$ 当且仅当 $f - g$ 仅在一个零测度集合上非零。注意， $L^{2,2}(\mathcal{R}, \mathbb{R}^d)$ 是一个赋范空间，其范数为

$$\|f\|_{2,2} = \sqrt{\int_R \|f(x)\|_2^2 \, d\mu(x)}. \tag{34}$$

如果对所有 $\epsilon > 0$，都存在 $N \in \mathbb{N}$ 使得对所有 $i \geq N$，$\|f - f_i\|_{2,2} \leq \epsilon$，我们就称 $f \in L^{2,2}(\mathcal{R}, \mathbb{R}^d)$ 是函数序列 $f_1, f_2, \ldots \in L^{2,2}(\mathcal{R}, \mathbb{R}^d)$ 的极限。显然，每个序列至多有一个极限。柯西序列是一个函数序列$f_1, f_2, \ldots \in L^{2,2}(\mathcal{R}, \mathbb{R}^d)$，满足：对所有 $\epsilon > 0$，都存在 $N \in \mathbb{N}$，使得对任意 $i, j \geq N$，均有$\|f_i - f_j\|_{2,2} \leq \epsilon$。如果每个柯西序列都有极限，我们就称 $L^{2,2}(\mathcal{R}, \mathbb{R}^d)$ 为巴拿赫空间。以下结论是里斯-费歇尔定理的一个简单推论。

定理 6.22 （黎斯–费歇尔定理，参见 [DiB16] 第 6 章定理 5.1）。 $L^{2,2}(\mathcal{R}, \mathbb{R}) = L^2(\mathcal{R})$是一个巴拿赫空间。[18]

推论 6.23。 对于所有 $d \geq 1$, $L^{2,2}(\mathcal{R}, \mathbb{R}^d)$ 都是巴拿赫空间。

证明。任取柯西序列 $f_1, f_2, \ldots, \in L^{2,2}(\mathcal{R}, \mathbb{R}^d)$。对于每个 $i \in [d]$，注意到$f_{1,i}, f_{2,i}, \ldots$ 是 $L^{2,2}(\mathcal{R}, \mathbb{R})$ 中的柯西序列。因此，根据定理 6.22，该序列收敛于 $g_i \in L^{2,2}(\mathcal{R}, \mathbb{R})$。令 $g = (g_1, \ldots, g_d)$。容易验证 $g \in L^{2,2}(\mathcal{R}, \mathbb{R}^d)$。此外，由于 d 是有限的，我们有

$$\begin{aligned} 0 = \sqrt{\sum_{j=1}^{d} 0} &= \sqrt{\sum_{j=1}^{d} \lim_{i\to\infty} \|f_{i,j} - g_j\|_{2,2}^2} \\ &= \lim_{i\to\infty} \sqrt{\sum_{j=1}^{d} \|f_{i,j} - g_j\|_{2,2}^2} \\ &= \lim_{i\to\infty} \|f_i - g\|_{2,2}. \end{aligned}$$

因此， g确实是柯西序列 f_1， f_2，$\ldots$ 的极限，符合预期。 □

[18]严格来说， [DiB16] 允许 f 取值为 $\pm\infty$，但从（34）可以清楚地看出，为了使$\|f\|_{2,2} < \infty$成立，$f^{-1}(\{-\infty, \infty\})$必须是零测度。因此，我们可以假设 f 是有限输出。

如果对于任意 f_1, $f_2 \in K$ 和 $\lambda \in [0,1]$, 都有 $\lambda f_1 + (1-\lambda) f_2 \in K$, 那么我们称 $K \subseteq L^{2,2}(\mathcal{R}, \mathbb{R}^d)$ 是凸的。我们将 $L^{2,2}(\mathcal{R}, \Delta_d) \subseteq L^{2,2}(\mathcal{R}, \mathbb{R}^d)$ 记为值域包含于 Δ_d 的函数子集。注意, $L^{2,2}(\mathcal{R}, \Delta_d)$ 是凸的。

给定 $K \subseteq L^{2,2}(\mathcal{R}, \mathbb{R}^d)$, 我们用 $\overline{K} \subseteq L^{2,2}(\mathcal{R}, \mathbb{R}^d)$ 表示它的（序列）闭包。也就是说, $f \in \overline{K}$ 当且仅当, 对于所有 $\epsilon > 0$, 都存在 $g \in K$, 使得 $\|f - g\|_{2,2} \leq \epsilon$。显然, 如果 K 是凸的, 那么 $\overline{K}$ 也是凸的。下面的事实是众所周知的。为了帮助读者熟悉这些定义, 我们给出一个简单的证明。

命题 6.24。如果 $K \subseteq L^{2,2}(\mathcal{R}, \Delta_d)$, 那么 $\overline{K} \subseteq L^{2,2}(\mathcal{R}, \Delta_d)$。

证明。反设存在 $f \in \overline{K}$, 使得 $f \notin L^{2,2}(\mathcal{R}, \Delta_d)$。令 $S = f^{-1}(\mathbb{R}^d \setminus \Delta_d)$。注意, $\mu(S) > 0$。由于 f 是可测的, 因此必然存在 $\delta > 0$ 和 $T \subseteq S$, 使得 $\mu(T) > 0$, 并且对于所有 $x \in T$, x 与 Δ_d 之间的 ℓ_1 距离大于 d。因此, 对于所有 $g \in L^{2,2}(\mathcal{R}, \Delta_d)$, 我们有

$$\|f - g\|_{2,2}^2 \geq \int_T \|f(x) - g(x)\|_1^2 \, d\mu(x) \geq \delta^2 \mu(T).$$

由于 $\delta^2 \mu(T) > 0$, 这与 $f \in \overline{K}$ 这一事实相矛盾。 □

接下来, 我们观察到一个关于 $L^{2,2}(\mathcal{R}, \mathbb{R}^d)$ 的范数的基本事实。

命题 6.25. 若 $f, g \in L^{2,2}(\mathcal{R}, \mathbb{R}^d)$ 满足 $\|f - g\|_{2,2} \geq \delta$ 则

$$\|(f+g)/2\|_{2,2}^2 \leq \max(\|f\|_{2,2}^2, \|g\|_{2,2}^2) - \delta^2/4.$$

证明. 注意到

$$\begin{aligned}
\|(f+g)/2\|_{2,2}^2 &= \frac{1}{4} \int_R \|f(x) + g(x)\|_2^2 \, d\mu(x) \\
&= \frac{1}{4} \int_R 2\|f(x)\|_2^2 + 2\|g(x)\|_2^2 - \|f(x) - g(x)\|_2^2 \, d\mu(x) \\
&= \frac{1}{4}(2\|f\|_{2,2}^2 + 2\|g\|_{2,2}^2 - \|f - g\|_{2,2}^2) \\
&\leq \max(\|f\|_{2,2}^2, \|g\|_{2,2}^2) - \delta^2/4.
\end{aligned}$$

□

我们现在证明我们可以唯一求解 $L^{2,2}(\mathcal{R}, \Delta_d)$ 上的一个适当优化问题。

引理 6.26. 设 $K \subseteq L^{2,2}(\mathcal{R}, \mathbb{R}^d)$ 非空且为凸集, 则存在唯一的 $f \in K$, 使得 $\|f\|_{2,2}$ 达到最小值。

证明. 首先注意, 若极小化元存在, 则必定唯一。否则, 存在 $f, g \in K$ 使得 $\|f\|_{2,2} = \|g\|_{2,2}$ 为最小值, 但命题 6.25 表明, $(f+g)/2 \in K$ 的范数必定更小, 因为按照不同的定义, 对于 $\|f - g\|_{2,2} > 0$, f 与 g 不同要求 $f \neq g$ 在一个非零测度集合上成立。

因此, 只需证明极小化元存在。令 $\alpha = \text{下确界}\{\|f\|_{2,2}^2 : f \in K\} < \infty$。根据下确界的定义, 对于所有 $n \in \mathbb{N}$, 存在 $f_n \in K$ 使得 $\|f_n\|_{2,2}^2 \leq \alpha + \frac{1}{n}$。现在任取正整数 $n \geq m$, 并根据命题 6.25 注意到

$$\alpha \leq \|(f_n + f_m)/2\|_{2,2}^2 \leq \max(\|f_n\|_{2,2}^2, \|f_m\|_{2,2}^2) - \frac{1}{4}\|f_n - f_m\|_{2,2}^2 \leq \alpha + \frac{1}{m} - \frac{1}{4}\|f_n - f_m\|_{2,2}^2.$$

因此，$\|f_n - f_m\|_{2,2}^2 \le 4/m$。因此 f_1，f_2，.....是一个柯西序列。根据定理 6.22，其极限 f 属于 K。此外，由于$\|f_m\|_{2,2}^2$ 趋近于 α，当 $m \to \infty$时，容易证明$\|f\|_{2,2}^2 = \alpha$。因此，f 是K中范数的唯一极小化元。

□

6.5 定义REQ

回顾一下，在第 6.3.3 节中，我们定义了一族宽松鲁棒舍入方案 BCR。现在，我们希望进一步改造 BCR，得到另一种称为 REQ 的方案，它支持一项额外性质：任意两个足够接近的向量，舍入后在 Δ_B 上得到的分布基本相同。我们通过凸优化来实现这一点。

回顾一下，我们先前将一个舍入方案 定义为函数 $S : \mathbb{S}_A^N \times \Xi \to \Delta_B$（定义6.5）。等价地，我们可以将 S 视为具有签名 $\mathbb{S}_A^N \to L^{2,2}(\Xi, \Delta_B)$。从现在起，我们采用后一种表示方式。

定义 6.27 (δ-扩散)。回顾一下，对于任意 $\mathbf{V} \in \mathbb{S}_A^N$，$B(\mathbf{V}, \delta)$ 表示所有$\mathbf{W} \in \mathbb{S}_A^N$ 的集合，其中 $\|\mathbf{V} - \mathbf{W}\|_2^2 \le \delta$。我们将 $\mathbf{V}$ 的一个 δ-扩散 定义为在 $B(\mathbf{V}, \delta)$ 上的有限支撑概率分布 Λ，使得对于所有 $p \in [0,1]$，都有

$$\Pr_{\mathbf{W} \sim \Lambda}[\|\mathbf{V} - \mathbf{W}\|_2^2 \le p^2 \delta] \ge p.$$

我们称 $S' : \mathbb{S}_A^N \to L^{2,2}(\Xi, \Delta_B)$ 是 $S : \mathbb{S}_A^N \to L^{2,2}(\Xi, \Delta_B)$ 的一个 δ-平滑，如果对所有$\mathbf{V} \in \mathbb{S}_A^N$，存在 $\mathbf{V}$ 的一个 δ-展开 $\Lambda_{\mathbf{V}}$，使得

$$S'(\mathbf{V}) = \mathop{\mathbb{E}}_{\mathbf{W} \sim \Lambda_{\mathbf{V}}}[S(\mathbf{W})].$$

我们令 $B(S, \mathbf{V}, \delta) \subseteq L^{2,2}(\Xi, \Delta_B)$ 表示 $S'(\mathbf{V})$ 的所有可能取值。

命题 6.28. $B(S, \mathbf{V}, \delta)$ 是凸的。

证明。考虑任意 $S', S'' \in B(S, \mathbf{V}, \delta)$，并令 Λ', Λ'' 为 $\mathbf{V}$ 的 δ-展开，使得 $S'(\mathbf{V}) = \mathop{\mathbb{E}}_{\mathbf{W} \sim \Lambda'}[S(\mathbf{W})]$ 且 $S''(\mathbf{V}) = \mathop{\mathbb{E}}_{\mathbf{W} \sim \Lambda''}[S(\mathbf{W})]$。对任意 $\theta \in [0,1]$，令 Λ_θ 为以概率 θ 从 Λ' 抽样、并以概率 $1-\theta$从 Λ'' 抽样的概率分布。不难看出

$$(\theta S' + (1-\theta) S'')(\mathbf{V}) = \mathop{\mathbb{E}}_{\mathbf{W} \sim \Lambda_\theta}[S(\mathbf{W})].$$

还需要验证 Λ_θ 是 $\mathbf{V}$ 的 δ-扩展。为说明这一点，请注意，对于任意 $p \in [0,1]$，我们有

$$\begin{aligned}\Pr_{\mathbf{W} \sim \Lambda_\theta}[\|\mathbf{V} - \mathbf{W}\|_2^2 \le p^2 \delta] &= \theta \Pr_{\mathbf{W} \sim \Lambda'}[\|\mathbf{V} - \mathbf{W}\|_2^2 \le p^2 \delta] + (1-\theta) \Pr_{\mathbf{W} \sim \Lambda''}[\|\mathbf{V} - \mathbf{W}\|_2^2 \le p^2 \delta] \\ &\ge \theta p + (1-\theta) p = p\end{aligned}$$

正如所需。

□

现在我们根据 $\mathrm{BCR}_{\theta,\delta}^{N,Z}$，来定义 $\mathrm{REQ}_{\theta,\delta}^{N,Z}$：$\mathbb{S}_A^N \to L^{2,2}(\Xi_{|Z|\cdot|A|+N,\theta}^{\mathrm{BCR}}, \Delta_B)$，具体如下：$\mathbb{S}_A^N \to L^{2,2}(\Xi_{|Z|\cdot|A|+N,\theta}^{\mathrm{BCR}}, \Delta_B)$。

定义 6.29。 对于所有$\mathbf{V} \in \mathbb{S}_A^N$ 以及集合 Z，我们令

$$\mathrm{REQ}_{\theta,\delta}^{N,Z}(\mathbf{V}) := \operatorname{argmin}\{\|f\|_{2,2} : f \in \overline{B(\widehat{\mathrm{BCR}}_{\theta,\delta}^{N,Z}, \mathbf{V}, \delta)}\}.$$

注意，根据引理6.26，该方案定义良好。直观地说，最小值点会执行$\widehat{\ }$在许多 BCR 舍入方案上进行局部优化。这个最小值对输入的修改具有相当强的鲁棒性。特别地，我们有以下两个引理，它们将在接下来的两个小节中证明。第一个引理表明，与 BCR 相比，$\mathrm{PCSP}(\mathbf{A},\mathbf{B})\widehat{\ }$的 REQ 鲁棒性几乎没有下降。第二个引理表明，REQ 会将邻近向量舍入为相似的分布。

引理 *6.30*。设 $\mathcal{X}$ 是 *PCSP(A, B)* 的一个加权实例。假设 $\mathit{BCR}_\theta^{|Z|\cdot|A|+N}$ 对于 $\mathcal{X}$ 是 $(\alpha - \theta, \beta + \theta)$-鲁棒的。那么 $\mathit{REQ}_{\theta\,\delta}^{N\,Z}{}_{,,}$，对于 $\mathcal{X}$ 是 $(\alpha - \theta - O_{\mathbf{A}}(\sqrt{\delta})\ \beta \mp \theta + \frac{|X|^2}{|Z|})$-鲁棒的，其中$O_{\mathbf{A}}(\sqrt{\delta})$ 来自引理 *6.21*。

引理 6.31。 假设 $\mathbf{V},\mathbf{W} \in \mathbb{S}_A^N$满足 $\|\mathbf{V} - \mathbf{W}\|_2^2 \le \delta \cdot \eta^2$，其中 $\eta > 0$。那么，$\|\mathrm{REQ}_{\theta\,\delta}^{N\,Z}{}_{,,}(\mathbf{V}) - \mathrm{REQ}_{\theta\,\delta}^{N\,Z}{}_{,,}(\mathbf{W})\|_{2,2} \le 8\sqrt{\eta}$。

6.5.1 稳健性得以保持：引理 6.30

证明引理 6.30相对直接。由于，$\widehat{\mathrm{BCR}}_{\theta\,\delta}^{N\,Z}{}_{,,}$已经具有宽松鲁棒性，因此只需证明 $\mathrm{REQ}_{\theta\,\delta}^{N\,Z}{}_{,,}$可能选取的任意 δ-扩展都具有类似的可靠性。

引理 *6.30* 的证明。 根据引理6.26，$\mathrm{REQ}_{\theta\,\delta}^{N\,Z}{}_{,,}$的定义是良定义的。因此，对于所有$\epsilon > 0$，存在一个 δ-平滑化 S，它来自 $\widehat{\mathrm{BCR}}_{\theta\,\delta}^{N\,Z}{}_{,,}$，使得对于所有 $\mathbf{V} \in \mathbb{S}_A^N$，我们有

$$\|\mathrm{REQ}_{\theta,\delta}^{N,Z}(\mathbf{V}) - S(\mathbf{V})\|_{2,2} = \sqrt{\mathop{\mathbb{E}}_{\xi \in \Xi_{|Z|\cdot|A|+N,\theta}^{\mathrm{BCR}}} [(\mathrm{REQ}_{\theta,\delta}^{N,Z}(\mathbf{V},\xi) - S(\mathbf{V},\xi))^2]} < \epsilon.$$

设 $\alpha' = \alpha - \theta - O_{\mathbf{A}}(\sqrt{\delta})$。固定 $\mathcal{V} \in \mathbb{V}_{\mathcal{X},\,\mathbf{A}}^N$使得 $\mathrm{comp}_{\mathcal{X},\,\mathbf{A}}(\mathcal{V}) \ge 1 - \alpha'$。对于每个 $x \in X$，令Λ_x 为定义在 $B(\mathbf{V}_x,\ \delta)$ 上的概率分布，使得

$$S(\mathbf{V}) = \mathop{\mathbb{E}}_{\mathbf{W}\sim\Lambda_x} \left[\widehat{\mathrm{BCR}}_{\theta,\delta}^{N,Z}(\mathbf{W})\right]. \tag{35}$$

令 $\mathbb{W}$ 为定义在 $B(\mathcal{V},\ \delta)$上的有限概率分布，其中对于每个 $x \in X$，分布$\mathbf{W}_x$ (满足 $\mathcal{W} \sim \mathbb{W}$) 是从 Λ_x中独立抽取的样本。注意，每个 $\mathcal{W} \in \operatorname{supp}\mathbb{W}$ 都是δ-对 $\mathcal{V}$的修改，因此由引理 6.21 可得

$$\mathop{\mathbb{E}}_{\substack{W\sim\mathbb{W}\\ \xi\sim\Xi_{|Z|\cdot|A|+N,\theta}^{\mathrm{BCR}}}} \left[\mathrm{sound}_{\mathcal{X},\mathbf{B}}(\widehat{\mathrm{BCR}}_{\theta,\delta}^{N,Z}(\mathbf{W},\xi) : x \in X)\right] \ge 1 - \beta - \theta - \frac{|X|^2}{|Z|}.$$

与引理 6.21 的证明类似，我们利用 $\mathrm{sound}_{\mathcal{X},\,\mathbf{B}} \colon \Delta_B^X \to [0,1]$ 是一个多重线性函数这一事实。因此，由于 $\mathbb{W}$ 是一个乘积分布，我们有

$$\begin{aligned} 1 - \beta - \theta - \frac{|X|^2}{|Z|} &\le \mathop{\mathbb{E}}_{\xi\sim\Xi_{|Z|\cdot|A|+N,\theta}^{\mathrm{BCR}}} \left[\mathrm{sound}_{\mathcal{X},\mathbf{B}}(\mathbb{E}_{\mathbf{W}_x\sim\Lambda_x}[\widehat{\mathrm{BCR}}_{\theta,\delta}^{N,Z}(\mathbf{W}_x,\xi)] : x \in X)\right] \\ &= \mathop{\mathbb{E}}_{\xi\sim\Xi_{|Z|\cdot|A|+N,\theta}^{\mathrm{BCR}}} [\mathrm{sound}_{\mathcal{X},\mathbf{B}}(S(\mathbf{W}_x,\xi) : x \in X)], \end{aligned}$$

其中，最后一个等式用到了（35）。由于 $\mathsf{sound}_{\mathcal{X},\mathbf{B}}$，$\mathbf{B}$：$\Delta_B^X \to [0,1]$ 是有界的多重线性函数，对于任意 $\mathbf{p}$，$\mathbf{q} \in \Delta_B^X$，我们有如下粗略界

$$\mathrm{sound}_{\mathcal{X},\mathbf{B}}(\mathbf{p}) - \mathrm{sound}_{\mathcal{X},\mathbf{B}}(\mathbf{q}) \le \sum_{x\in X} |p_x - q_x| \le \sqrt{|X| \sum_{x\in X} (p_x - q_x)^2},$$

其中格　　不等式由柯西–施瓦茨不等式得出。因此，由于 $\sqrt{\cdot}$ 是凹函数，

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\xi\sim\Xi^{\mathrm{BCR}}_{|Z|\cdot|A|+N,\theta}} \left[\mathrm{sound}_{\mathcal{X},\mathbf{B}}(S(\mathbf{V}_x,\xi) : x\in X) - \mathrm{sound}_{\mathcal{X},\mathbf{B}}(\mathrm{REQ}^{N,Z}_{\theta,\delta}(\mathbf{V}_x,\xi) : x\in X)\right] \\
&\qquad \le \sqrt{|X|} \mathop{\mathbb{E}}_{\xi\sim\Xi^{\mathrm{BCR}}_{|Z|\cdot|A|+N,\theta}} \left[\sqrt{\sum_{x\in X} (S(\mathbf{V}_x,\xi) - \mathrm{REQ}^{N,Z}_{\theta,\delta}(\mathbf{V}_x,\xi))^2}\right] \\
&\qquad \le \sqrt{|X| \cdot \sum_{x\in X} \mathop{\mathbb{E}}_{\xi\in\Xi^{\mathrm{BCR}}_{|Z|\cdot|A|+N,\theta}} [(S(\mathbf{V},\xi) - \mathrm{REQ}^{N,Z}_{\theta,\delta}(\mathbf{V},\xi))^2]} \\
&\qquad < \sqrt{|X| \cdot \sum_{x\in X} \epsilon^2} = |X|\epsilon.
\end{aligned}$$

因此，

$$\mathop{\mathbb{E}}_{\xi\sim\Xi^{\mathrm{BCR}}_{|Z|\cdot|A|+N,\theta}} \left[\mathrm{sound}_{\mathcal{X},\mathbf{B}}(\mathrm{REQ}^{N}_{\theta,\delta,x}(\mathbf{V}_x,\xi) : x\in X)\right] \ge 1 - \beta - \theta - |X|\epsilon.$$

令 $\epsilon \to 0$ 趋于极限可得，REQ^N_θ，δ 对于 $\mathcal{X}$ 是 $(\alpha - \theta - O_{\mathbf{A}}(\sqrt{\delta})\ \bar{\beta} + \theta)$-鲁棒的。 □

6.5.2 $\mathrm{REQ}^N_{\theta,\delta}$ 的平滑性：引理 6.31

现在我们证明引理 6.31。直观而言，我们希望论证，对于两个邻近向量 $\mathbf{V}$、$\mathbf{W} \in \mathbb{S}^N_A$，定义 6.29 中的优化会给出相似的答案。我们通过“策略窃取”论证来证明这一点：对于任意一个 δ-扩展，其对应于 $\mathbf{V}$，都存在一个相似的 δ-扩展，对应于 $\mathbf{W}$。具体做法是，取 δ-扩展，对应于 $\mathbf{V}$，并尽可能少地修改它，使其成为一个合法的 δ-扩展，对应于 $\mathbf{W}$。由此得到以下命题。

命题 6.32. 设 S：$\mathbb{S}^N_A \times \Xi \to \Delta_B$ 是一个舍入方案。考虑 $\mathbf{V},\mathbf{W} \in \mathbb{S}^N_A$，其中 $\|\mathbf{V} - \mathbf{W}\|_2^2 \le \delta \cdot \eta^2$ 满足 $\eta \in (0,1)$。对于任意 $f \in B(S, \mathbf{V}\ \delta)$，存在 $g \in B(S, \mathbf{W}\ \delta)$ 使得 $\|f - g\|_{2,2} \le 2\eta$。

证明。设 Λ 是 $\mathbf{V}$ 的一个 δ-扩展，使得

$$\forall p \in [0,1],\ p \le \Pr_{\mathbf{V}'\sim\Lambda}[\|\mathbf{V} - \mathbf{V}'\|_2^2 \le p^2\delta]$$
$$f = \mathop{\mathbb{E}}_{\mathbf{V}'\sim\Lambda} \left[S(\mathbf{V}')\right].$$

回顾一下，Λ 是一个离散概率分布。令 $\mathbf{V}'_1,\ldots,\mathbf{V}'_k \in B(\mathbf{V}\ \delta)$ 为该分布的支撑集，$p_1,\ldots,p_k \in [0,1]$ 为相应的概率。我们假设 $\|\mathbf{V} - \mathbf{V}'_1\|_2^2 \le \cdots \le \|\mathbf{V} - \mathbf{V}'_k\|_2^2$。选取满足 $p_1 + \cdots + p_\ell \ge 1 - \eta$ 的最小 $\ell \in [k]$。

令 Λ' 为支撑在 $\{\mathbf{W}, \mathbf{V}'_1, \ldots, \mathbf{V}'_\ell\}$ 上的概率分布：以概率 η 取样 $\mathbf{W}$，对于 $i \in [\ell - 1]$，以概率 p_i 取样 $\mathbf{V}'_i$，否则（概率为 $p'_\ell := 1 - \eta - p_1 - \cdots - p_{\ell-1}$）取样 $\mathbf{V}'_\ell$。我们利用以下事实：

$$(p_\ell - p'_\ell) + \sum_{i=\ell+1}^{k} p_i \le \eta. \tag{36}$$

以概率 η， Λ' 从$\mathbf{W}$ 中采样；否则，从与$\mathbf{V}$距离最近的$1-\eta$比例的 Λ 中随机采样。

We n我们解释为何 Λ' 是$\mathbf{W}$的 δ-扩展。首先注意，若 $\|\mathbf{V} - \mathbf{V}'\|_2^2 \le p^2\delta$，则

$$\|\mathbf{W} - \mathbf{V}'\|_2^2 \le (\|\mathbf{W} - \mathbf{V}\|_2 + \|\mathbf{V} - \mathbf{V}'\|_2)^2 \le (\eta\sqrt{\delta} + p\sqrt{\delta})^2 = (p + \eta)^2\delta.$$

因此，对于任意 $p \in [0, 1]$，我们有

$$\Pr_{\mathbf{V}' \sim \Lambda}\left[\|\mathbf{W} - \mathbf{V}'\|_2^2 \le p^2\delta\right] \ge \Pr_{\mathbf{V}' \sim \Lambda}\left[\|\mathbf{V} - \mathbf{V}'\|_2^2 \le \max(p - \eta, 0)^2\delta\right] \ge \max(p - \eta, 0).$$

因此，

$$\Pr_{\mathbf{V}' \sim \Lambda'}\left[\|\mathbf{W} - \mathbf{V}'\|_2^2 \le p^2\delta\right] \ge \max(p - \eta, 0) + \eta \ge p.$$

因此， Λ' 是$\mathbf{W}$ 的 δ-扩展，因而支撑于 $B(\mathbf{W}\ \delta)$。令 $g = \mathop{\mathbb{E}}_{\mathbf{V}' \sim \Lambda'}[S(\mathbf{V}')]$. 我们有

$$\begin{aligned}
\|f - g\|_{2,2} &= \left\| \mathop{\mathbb{E}}_{\mathbf{V}' \sim \Lambda}\left[S(\mathbf{V}')\right] - \mathop{\mathbb{E}}_{\mathbf{V}' \sim \Lambda'}\left[S(\mathbf{V}')\right] \right\|_{2,2} \\
&= \left\| \sum_{i \in [k]} p_i S(\mathbf{V}'_i) - \eta S(\mathbf{W}) - \sum_{i \in [\ell-1]} p_i S(\mathbf{V}'_i) - p'_\ell S(\mathbf{V}'_\ell) \right\|_{2,2} \\
&\le (p_\ell - p'_\ell)\|S(\mathbf{V}_\ell)\|_{2,2} + \sum_{i=\ell+1}^{k} p_i \|S(\mathbf{V}'_i)\|_{2,2} + \eta\|S(\mathbf{W})\|_{2,2} \\
&\le 2\eta \max_{\mathbf{V}' \in B(\mathbf{V},\delta) \cup B(\mathbf{W},\delta)} \|S(\mathbf{V}')\|_{2,2} \qquad \text{(by (36))} \\
&\le 2\eta,
\end{aligned}$$

正如所需。 □

引理 *6.31* 的证明。 若 $\eta \ge 1$，则 $\|\mathrm{REQ}^{N\,Z}_{\theta\,\delta}{}_{,,}(\mathbf{V}) - \mathrm{REQ}^{N\,Z}_{\theta\,\delta}{}_{,,}(\mathbf{W})\|_{2,2} \le \sqrt{2} < 8\sqrt{\eta}$, −如所需。因此，假设 $\eta \in (0,1)$。

固定 $x \in X$，并令 $f = \mathrm{REQ}^{N\,Z}_{\theta\,\delta}$，(V) 和 $g = \mathrm{REQ}^{N\,Z}_{\theta\,\delta}$，(W)。由命题 6.32 可知，存在 $f' \in B(\widehat{\ \ \ }\mathrm{BCR}^{N\,Z}_{\theta\,\delta}$，V δ) 和 $g' \in B(\widehat{\ \ \ }\mathrm{BCR}^{N\,Z}_{\theta\,\delta}$，W δ)，使得 $\|f' - g\|_{2、\ 2} \le 2\eta$ 以及 $\|g' - f\|_{2、\ 2} \le 2\eta$。令 $g'' = (g + g')/2$ 和 $f'' = (f + f')/2$。不失一般性，假设 $\|f\|_{2、\ 2} \ge \|g\|_{2、\ 2}$。

由命题 6.25 以及 $\|f\|_{2,2} \le 1$ 这一事实可知，

$$\begin{aligned}\|f''\|_{2,2}^2 &\le \max(\|f\|_{2,2}^2, \|f'\|_{2,2}^2) - \frac{\|f-f'\|_{2,2}^2}{4} \\ &\le \max(\|f\|_{2,2}^2, (\|g\|_{2,2}+2\eta)^2) - \frac{(\|f-g\|_{2,2}-2\eta)^2}{4} \\ &\le (\|f\|_{2,2}+2\eta)^2 - \frac{(\|f-g\|_{2,2}-2\eta)^2}{4} \\ &\le \|f\|_{2,2}^2 + 8\eta - \frac{(\|f-g\|_{2,2}-2\eta)^2}{4}.\end{aligned}$$

由于 $f'' \in B(\widehat{\ }\mathrm{BCR}_{\theta\ \delta}^{N\ Z}{}_{,}\ ,\ \mathbf{V}\ \delta)$ 和 $f = \mathrm{REQ}_{\theta\ \delta}^{N\ Z}{}_{,}(\mathbf{V})$，我们有 $\|f''\|_{2,\ 2}^2 \ge \|f\|_{2,\ 2}^2$。因此，

$$8\eta \ge \frac{(\|f-g\|_{2,2}-2\eta)^2}{4}.$$

因此，$\|f-g\|_{2,\ 2} \le \sqrt{32\eta+2\eta} \le 8\sqrt{\eta}$，如所期望的那样。 □

6.6 相关舍入

证明定理 6.1 所需的最后一个要素，是将 BCR 的独立舍入转换为相关舍入。更具体地说，根据引理 6.31，我们知道 REQ 会将相似的向量映射为相似的概率分布。然而，BCR 算法中独立舍入的最后一步破坏了这一性质。例如，对于 $A = \{0,1\}$，考虑 Δ_A 中的点 $p_x =$ (0.5, 0.5) 和 $p_y =$ (0.51, 0.49)。这两个分布高度相似，但采用独立舍入时，x 和 y 被舍入为不同值的概率为 $1/2$。我们可以通过采样一个公共随机实数 $r \sim [0,1]$，并根据 $r < 0.5$ 对 x 进行舍入，以及根据 $r < 0.51$ 对 y 进行舍入，使这些分布相关起来。这样，x 和 y 有 99% 的概率被舍入为相同的值。

一般来说，我们可以执行类似的相关舍入（其中 ξ_{COR} 对应变量 r）。令 plur：$\mathbb{R}^B \to B$ 为满足以下性质的任意函数：对所有 $q \in \Delta_B$，q（plur(q)）$\ge q$（b）。对所有 $b \in B$ 均成立。也就是说，plur 是一个在平票时任意打破平局的多数函数（参见第 5 节）。

定义 6.33。令 S：$\mathbb{S}_A^N \to L^2{}_{,\ 2}(\Xi, \Delta_B)$ 为一个舍入方案。令 $\Xi_{\mathrm{COR},\ B}$ 为 $[0, {}_{2|B|}^{1}]^B$上的均匀分布。于是，我们将 $\mathbb{S}_{\mathrm{COR}}$：$\mathbb{S}_A^N \to L^2{}_{,\ 2}(\Xi \times \Xi_{\mathrm{COR},\ B}, \Delta_B)$ 定义如下：

$$S_{\mathrm{COR}}(\mathbf{V}, \xi, \xi_{\mathrm{COR}}) = \mathrm{plur}(S(\mathbf{V}, \xi) + \xi_{\mathrm{COR}}). \tag{37}$$

注意，在 S_{COR} 处仅输出 B的元素，我们将其与 Δ的顶点对应起来 $_B$.

我们要证明关于（37）的两个事实：首先，如果 S 是鲁棒的，那么 S_{COR} 是鲁棒的；其次，如果$\|S$（$\mathbf{V}$）$-S$（$\mathbf{W}$）$\|_{2,\ 2}$很小，那么 S_{COR}（$\mathbf{V}$）和 S_{COR}（$\mathbf{W}$）的输出大多相同。

引理 6.34。假设 S：$\mathbb{S}_A^N \times \Xi \to \Delta_B$ 是一种针对加权实例 $\mathcal{X}$（属于 部分约束满足问题(**A**，**B**)）的舍入方案，且该方案是(α，β)-鲁棒的。那么，S_{COR} 对 $\mathcal{X}$ 是(α，$O_{\mathbf{B}}(\beta)$-鲁棒的。

证明。令 $\mathcal{V} \in \mathbb{V}^N_{\mathcal{X},\mathbf{A}}$ 为一个满足 $\mathrm{comp}_{\mathcal{X},\mathbf{A}}(\mathcal{V}) \geq 1-\alpha$ 的半定规划解。根据定义 6.6，我们有

$$\mathop{\mathbb{E}}_{\xi\sim\Xi}[\mathrm{sound}_{\mathcal{X},\mathbf{B}}(S(\mathbf{V}_x,\xi):x\in X)] \geq 1-\beta. \tag{38}$$

令 (Y,P,Q) 为 $\mathcal{X}$ 的任意子句，并固定 $\xi \in \mathrm{supp}\ \Xi$。假设 $\mathrm{sound}_{Y,Q}(S(\mathbf{V}y,\xi):y\in Y) \geq 1-\gamma$。我们断言

$$\mathop{\mathbb{E}}_{\mathbf{p}\sim[0,1/(2|B|)]^B}[\mathrm{sound}_{Y,Q}(S_{\mathrm{COR}}(\mathbf{V}_y,\xi,\mathbf{p}):y\in Y)] \geq 1-(2|B|)^{|Y|}\gamma. \tag{39}$$

为方便记号，令 $\mathbf{r} := (S(\mathbf{V}y,\xi): \ y \in Y) \in \Delta_B^Y$。假设 $\mathrm{sound}_{Y,Q}(\mathbf{q}) \geq 1-\gamma$ 等价于

$$\sum_{\mathbf{q}\in B^Y\setminus Q}\prod_{y\in Y} r_{y,q_y} \leq \gamma. \tag{40}$$

我们要证明

$$\Pr_{\mathbf{p}\sim[0,1/(2|B|)]^B}[(\mathrm{plur}(\mathbf{r}_y+\mathbf{p}):y\in Y)\in Q] \geq 1-(2|B|)^{|Y|}\gamma.$$

任取 $\mathbf{q} \in B^Y \setminus Q$ 使得存在 $\mathbf{p} \in [0,1/(2|B|)]^B$ 满足 $(\mathrm{plur}(\mathbf{r}_y+\mathbf{p}):y\in Y) = \mathbf{q}$。若不存在这样的 $\mathbf{q}$，则（38）的左端等于 1。

对于每个 $y \in Y$，要使 $\mathrm{plur}(\mathbf{r}_y+\mathbf{p}) = q_y$，必须满足 $r_{y,q_y} + \frac{1}{2|B|} \geq r_{y,b}$ 对所有 $b \in B$。由于 $\sum_{b\in B} r_{y,b} \geq 1$，这意味着 $r_{y,q_y} \geq \frac{1}{2|B|}$。因此，由（40），可得

$$\gamma \geq \prod_{y\in Y} r_{y,q_y} \geq \frac{1}{(2|B|)^{|Y|}}.$$

因此，（39）的右端至多为零，所以该不等式成立。最后，我们应用（39）和（38）如下。

$$\begin{aligned}
&\mathop{\mathbb{E}}_{\xi\sim\Xi}[\mathrm{sound}_{\mathcal{X},\mathbf{B}}(S_{\mathrm{COR}}(\mathbf{V}_x,\xi):x\in X)] \\
&\quad= \mathop{\mathbb{E}}_{\substack{\xi\sim\Xi\\(Y,P,Q)\sim\mathcal{X}}}[\mathrm{sound}_{Y,Q}(S_{\mathrm{COR}}(\mathbf{V}_y,\xi):y\in Y)] \\
&\quad\geq 1-\mathop{\mathbb{E}}_{\substack{\xi\sim\Xi\\(Y,P,Q)\sim\mathcal{X}}}[|B|^{|Y|}(1-\mathrm{sound}_{Y,Q}(S(\mathbf{V}_y,\xi):y\in Y))] && \text{by (39)} \\
&\quad\geq 1-\mathop{\mathbb{E}}_{\substack{\xi\sim\Xi\\(Y,P,Q)\sim\mathcal{X}}}[O_{\mathbf{B}}(1)(1-\mathrm{sound}_{Y,Q}(S(\mathbf{V}_y,\xi):y\in Y))] && \mathbf{B}\text{ has bounded arity} \\
&\quad= 1-O_{\mathbf{B}}(1)\mathop{\mathbb{E}}_{\xi\sim\Xi}[1-\mathrm{sound}_{\mathcal{X},\mathbf{B}}(S(\mathbf{V}_x,\xi):x\in X)] \\
&\quad\geq 1-O_{\mathbf{B}}(\beta), && \text{by (38)}
\end{aligned}$$

如所需。 □

接下来，我们证明 S_{COR} 轮会将相似的局部配置映射为近乎相同的输出。

引理 6.35. 设$\mathbf{V}$、$\mathbf{W} \in \mathbb{S}_A^N$满足 $\|S(\mathbf{V}) - S(\mathbf{W})\|_{2,2} \leq \eta$。那么，

$$\Pr_{\substack{\xi \sim \Xi \\ \mathbf{p} \sim \Xi_{\mathrm{COR},B}}} [S_{\mathrm{COR}}(\mathbf{V}, \xi, \mathbf{p}) \neq S_{\mathrm{COR}}(\mathbf{W}, \xi, \mathbf{p})] \leq O_{\mathbf{B}}(\eta).$$

证明. 我们有

$$\begin{aligned}
&\Pr_{\substack{\xi \sim \Xi \\ \mathbf{p} \sim \Xi_{\mathrm{COR},B}}} [S_{\mathrm{COR}}(\mathbf{V}, \xi, \mathbf{p}) \neq S_{\mathrm{COR}}(\mathbf{W}, \xi, \mathbf{p})] \\
&\quad = \Pr_{\substack{\xi \sim \Xi \\ \mathbf{p} \sim \Xi_{\mathrm{COR},B}}} [\mathrm{plur}(S(\mathbf{V}, \xi) + \mathbf{p}) \neq \mathrm{plur}(S(\mathbf{W}, \xi) + \mathbf{p})] \\
&\quad = \sum_{b \neq b' \in B} \Pr_{\substack{\xi \sim \Xi \\ \mathbf{p} \sim \Xi_{\mathrm{COR},B}}} [\mathrm{plur}(S(\mathbf{V}, \xi) + \mathbf{p}) = b \wedge \mathrm{plur}(S(\mathbf{W}, \xi) + \mathbf{p}) = b'] \\
&\quad \leq \sum_{b \neq b' \in B} \Pr_{\substack{\xi \sim \Xi \\ \mathbf{p} \sim \Xi_{\mathrm{COR},B}}} [S(\mathbf{V}, \xi)_b + p_b \geq S(\mathbf{V}, \xi)_{b'} + p_{b'} \wedge S(\mathbf{W}, \xi)_{b'} + p_{b'} \geq S(\mathbf{W}, \xi)_b + p_b] \\
&\quad = \sum_{b \neq b' \in B} \Pr_{\substack{\xi \sim \Xi \\ \mathbf{p} \sim [0, 1/(2|B|)]^B}} [S(\mathbf{V}, \xi)_b - S(\mathbf{V}, \xi)_{b'} \geq p_{b'} - p_b \geq S(\mathbf{W}, \xi)_b - S(\mathbf{W}, \xi)_{b'}] \\
&\quad \leq \sum_{b \neq b' \in B} \mathbb{E}_{\xi \sim \Xi} [2|B| \cdot |S(\mathbf{V}, \xi)_b - S(\mathbf{V}, \xi)_{b'} - (S(\mathbf{W}, \xi)_b - S(\mathbf{W}, \xi)_{b'})|] \qquad (*) \\
&\quad \leq 2|B|^3 \mathbb{E}_{\xi \sim \Xi} [\|S(\mathbf{V}, \xi) - S(\mathbf{W}, \xi)\|_1] \qquad (**) \\
&\quad \leq 2|B|^3 \|S(\mathbf{V}) - S(\mathbf{W})\|_{2,2} = O_{\mathbf{B}}(\eta),
\end{aligned}$$

其中，**(*)** 是因为分布 $p_b - p_{b'}$ 的累积分布函数处处有界于 $2|B|$，而 **(**)** 则由霍尔德不等式（以及 $\mathbb{E}_{\xi \sim \Xi}[1] = 1$）得出。 □

6.7 定理6.1的证明

现在，我们终于 具备了证明定理6.1所需的全部要素，现为方便起见重述如下。

定理 6.1。 假设唯一博弈猜想成立。若 部分约束满足问题**(A, B)** 对某个 $0 < \alpha < \beta < 1$ 是(α, β)-鲁棒的，那么部分约束满足问题**((A, B)** + 等式约束**)** 是$(\alpha_{\mathrm{EQ}}, \beta_{\mathrm{EQ}})$-鲁棒的

$$\alpha_{\mathrm{EQ}} = \Omega_{\mathbf{A}}(\alpha^2 \beta^4), \tag{27}$$

$$\beta_{\mathrm{EQ}} = O_{\mathbf{B}}(\beta). \tag{28}$$

证明。 根据定理 6.4，只需证明，对于每个实例 $\mathcal{X}$，若它属于 部分约束满足问题**((A,B)** + 等式约束**)**且半定规划值至少为 $1 - 2\alpha_{\mathrm{EQ}}$，就存在一个整数赋值 $\mathcal{X} \to \mathbf{B}$，其可靠性至少为 $1 - \beta_{\mathrm{EQ}}/2$。特别地，我们无需给出高效算法，因为根据 Raghavendra 定理，这一点会自动成立。

设 $\mathcal{X}$ 为 PCSP**((A, B)** + EQ**)** 的任意实例，并设 $\mathcal{V} \in \mathbb{V}^N_{\mathcal{X}, \mathbf{A}+\mathrm{EQ}}$ 的完备性至少为 $1 - 2\alpha_{\mathrm{EQ}}$。将 $\mathcal{X}$ 分成两部分：$\mathcal{X}_{\mathbf{A},\mathbf{B}}$ 作为 PCSP**(A,B)** 的实例，以及 $\mathcal{X}_{\mathrm{EQ}}$ 作为 PCSP**(EQ)** 的实例。设 $p \in [0, 1]$ 为落在 $\mathcal{X}_{\mathbf{A},\mathbf{B}}$ 上的权重比例。

注意，对变量的任意赋值，只要将所有变量都设为同一值，就能满足 $\mathcal{X}_{EQ}$ 中的每一个约束。因此， $\mathcal{X}$ 的最优整数赋值的值至少为 $1-p$。若$1-p \geq 1-\beta$，则已完成，因此可以假设 $1-p < 1-\beta$ （即 $p > \beta > \alpha$）。进一步注意，

$$1 - 2\alpha_{\mathrm{EQ}} \leq \mathrm{comp}_{\mathcal{X},\mathbf{A}+\mathrm{EQ}}(\mathcal{V}) = p\,\mathrm{comp}_{\mathcal{X}_{\mathbf{A},\mathbf{B}},\mathbf{A}}(\mathcal{V}) + (1-p)\,\mathrm{comp}_{\mathcal{X}_{\mathrm{EQ}},\mathrm{EQ}}(\mathcal{V}).$$

由于 comp 的值域为 $[0,1],$ ，我们可以推出

$$\mathrm{comp}_{\mathcal{X}_{\mathbf{A},\mathbf{B}},\mathbf{A}}(\mathcal{V}) \geq 1 - \frac{2\alpha_{\mathrm{EQ}}}{p} \geq 1 - \frac{2\alpha_{\mathrm{EQ}}}{\alpha}, \tag{41}$$

$$\mathrm{comp}_{\mathcal{X}_{\mathrm{EQ}},\mathrm{EQ}}(\mathcal{V}) \geq 1 - \frac{2\alpha_{\mathrm{EQ}}}{1-p}. \tag{42}$$

根据推论 6.7，我们可以选取 $\theta = \alpha/2$ ，使得对任意有限集 Z，$\mathrm{BCR}_{\theta}^{|Z|\cdot|A|+N}$ 对 $\mathcal{X}$ 是 $(\alpha/2, \beta + \alpha/2)$-鲁棒的（当 N充分大时）。选取 $|Z| \geq 2|X|^2/\alpha$ 和 $\delta = \Theta_{\mathbf{A}}(\alpha^2)$ 。根据引理 6.30，舍入方案集合 $\mathrm{REQ}_{\theta,\delta}^{N,Z},,$ 是 $(\alpha/2 - O_{\mathbf{A}}(\sqrt{\delta})\ \beta + \alpha/2 + \frac{|X|^2}{|Z|})$-鲁棒的，其中我们选取充分小的 $\bar{\delta}$，使得 $\mathrm{REQ}_{\theta,\delta}^{N,Z},,$ 是 $(\alpha/4, 2\beta)$-鲁棒的。由于由 (41) 可知 $\mathrm{comp}_{\mathcal{X}_{\mathbf{A},\mathbf{B}},\mathbf{A}}(\mathcal{V}) \geq 1 - 2\alpha_{\mathrm{EQ}}/\alpha \geq 1 - \alpha/4$, 因此将 $\mathrm{REQ}_{\theta,\delta}^{N,Z},,$ 应用于 V，至少满足 $\mathcal{X}_{\mathbf{A},\mathbf{B}}$的约束中 $1-2\beta$ 的比例。

特别地，当 $\mathrm{REQ}_{\theta,\delta}^{N,Z},,$应用于 $\mathbf{V}$ 时，我们平均满足 $\mathcal{X}_{\mathbf{A},\mathbf{B}}$ 的约束的 $1-2\beta$ 比例。此外，由引理 6.34，$\mathrm{REQ}_{\theta,\delta}^{N,Z},,,\mathrm{COR}$ 对于 $\mathcal{X}$ 是 $(\alpha/4, \Theta_{\mathbf{B}}(\beta))$-鲁棒的。因此，$\mathrm{REQ}_{\theta,\delta}^{N,Z},,,\mathrm{COR}$ 应用于 $\mathcal{V}$ 时满足 $\mathcal{X}_{\mathbf{A},\mathbf{B}}$ 的约束的 $1 - O_{\mathbf{B}}(\beta)$ 比例。

现在，我们评估 $\mathrm{REQ}_{\theta,\delta}^{N,Z},,,\mathrm{COR}$ 舍入 $\mathcal{V}$ 对于 $\mathcal{X}_{\mathrm{EQ}}$ 的性能。固定一个约束 (x,y)，并假设 $\mathrm{comp}_{\{x,y\},\mathrm{EQ}}(\mathcal{V}) = 1-\gamma$。注意到

$$\mathrm{comp}_{\{x,y\},\mathrm{EQ}}(\mathcal{V}) = 1 - \frac{\|\mathbf{V}_x - \mathbf{V}_y\|_2^2}{2},$$

因此 $\|\mathbf{V}_x - \mathbf{V}_y\|_2^2 = 2\gamma$。由引理 6.31 取 $\eta = \sqrt{2\gamma/\delta}$，我们有

$$\|\,\mathrm{REQ}_{\theta,\delta}^{N,Z}(\mathbf{V}_x) - \mathrm{REQ}_{\theta,\delta}^{N,Z}(\mathbf{V}_y)\|_{2,2} \leq 8\sqrt[4]{\frac{2\gamma}{\delta}} \leq 10\sqrt[4]{\frac{\gamma}{\delta}}.$$

因此，由引理6.35，我们有

$$\Pr_{\substack{\xi\sim\Xi_{|Z|\cdot|A|+N,\theta}^{\mathrm{BCR}} \\ \mathbf{p}\sim\Xi_{\mathrm{COR},B}}}[\mathrm{REQ}_{\theta,\delta,\mathrm{COR}}^{N,Z}(\mathbf{V}_x,\xi,\mathbf{p}) \neq \mathrm{REQ}_{\theta,\delta,\mathrm{COR}}^{N,Z}(\mathbf{V}_y,\xi,\mathbf{p})] \leq O_{\mathbf{B}}((\gamma/\delta)^{1/4}) = O_{\mathbf{B}}(\gamma^{1/4}\alpha^{-1/2}).$$

换言之，将 $\mathrm{REQ}_{\theta,\delta}^{N,Z},,,$COR 应用于 $\mathcal{V}$ 后， x 和 y 被舍入为相同值的概率为 $1 - O_{\mathbf{B}}(\gamma^{1/4}\alpha^{-1/2})$。由于该可靠性是 γ的凸函数，因此若 $\mathrm{comp}_{\mathcal{X}_{\mathrm{EQ}},\mathrm{EQ}}(\mathcal{V}) = 1-\lambda$，则 $\mathrm{REQ}_{\theta,\delta}^{N,Z},,,$ COR 平均满足 $1 - O_{\mathbf{B}}(\lambda^{1/4}\alpha^{-1/2})$ 比例的等式约束。由 (42) 可得 $\lambda \leq \frac{2\alpha_{\mathrm{EQ}}}{1-p}$ ，因此期望数量

通过将 $\mathrm{REQ}_{\theta\,\delta}^{N\,Z}$,,,COR 应用于 $\mathcal{V}$，满足的约束数量至少为

$$
\begin{aligned}
p(1-O_{\mathbf{B}}(\beta))+(1-p)(1-O_{\mathbf{B}}(\lambda^{1/4}\alpha^{-1/2})) &\geq 1-p\cdot O_{\mathbf{B}}(\beta)-(1-p)O_{\mathbf{B}}\left(\frac{(2\alpha_{EQ})^{1/4}}{(1-p)^{1/4}\sqrt{\alpha}}\right)\\
&\geq 1-O_{\mathbf{B}}\left(p\beta+(1-p)^{3/4}\frac{\alpha_{\mathrm{EQ}}^{1/4}}{\sqrt{\alpha}}\right)\\
&\geq 1-O_{\mathbf{B}}\left(\beta+\frac{\alpha_{\mathrm{EQ}}^{1/4}}{\sqrt{\alpha}}\right),
\end{aligned}
$$

其中，最后一行的界对任意 $p\in[0,1]$ 均满足 $p\leq 1$ 和 $(1-p)^{3/4}\leq 1$。特别地，对于 $\alpha_{\mathrm{EQ}}=\Theta_{\mathbf{B}}(\alpha^2\beta^4)$，我们得到 $1-O_{\mathbf{B}}(\beta)=1-\beta_{\mathrm{EQ}}$ 比例的约束得到满足，正如所期望的那样。

□

7 结论

本文证明了关于鲁棒承诺约束满足问题本质的一系列新结果。首先，我们针对 $(1\text{-IN-}3\text{-SAT},\mathrm{NAE\text{-}SAT})$ 得出的整数间隙表明，Brakensiek–Guruswami–Sandeep 提出的 $(\epsilon,O(\log\log(1/\epsilon)/\log(1/\epsilon)))$- 鲁棒算法对于交替阈值AT 多态性 [BGS25] 而言几乎是紧的。其次，我们针对多数、相对多数和可分多态性的算法表明，Charikar–Makarychev–Makarychev 提出的鲁棒算法 [CMM06,CMM09]可以扩展到相当一般的情形。最后，我们针对添加了等式约束的鲁棒 PCSP 模板设计的鲁棒算法表明，PCSP 之间丰富的构件归约理论可以作为黑箱应用于鲁棒 CSP 理论。未来还有许多值得进一步探索的方向。

- 在第 3 节中，我们给出了 fiPCSP(1-IN-3-SAT，NAE-SAT) 的一个整数间隙。更一般地，对于 fiPCSP(a-IN-b-SAT，NAE-SAT)，我们能否得到具有类似渐近性质的整数间隙？在 $b=2a$ 的情形下，MAJ 是多态性，因此一般来说，我们考虑 $a/b\in(0,\ 1)\setminus\{1/2\}$。据我们所知，无法仅使用构件归约来确立这一更广泛的间隙族。

- 回想一下，Brakensiek、Guruswami 和 Sandeep [BGS25] 为所有具有 MAJ 或交替阈值多态运算的布尔承诺约束满足问题构造了鲁棒算法。在第4 节和第5节中，我们大幅改进了 BGS 的 MAJ 算法的分析和适用范围。对于交替阈值，这样的推广会是什么样子？一个可能的方向是移除定理 α 中关于映射 ρ 的“5.3-保守”假设。

- 能否推广第6节中的分析，从而彻底解决问题1.4？鉴于采用了 $\epsilon^{1/2}$ -空间的几何性质（例如，命题6.32），以现有技术而言，至少需要 L^2的损失。或许可以通过直接构造针对 $\Gamma\cup\{$等式约束$\}$的拟随机近似多态性，获得更精确的渐近结果。

致谢

作者感谢美国数学研究所（AIM）SQuaRE 项目为此次合作提供部分资助并促成合作，也感谢 AIM 的热情款待。作者还感谢 Marcin Kozik 分享了许多有益的讨论。

参考文献

[AFO+25] Sergey Avvakumov、Marek Filakovský、Jakub Oprsal、Gianluca Tasinato 和 Uli Wagner。k-可着色图的四色着色困难性。载于 第*57*届*ACM*计算理论年会（*STOC'25*）论文集，第72–83页。ACM，2025年。[AGH17] Per Austrin、Venkatesan Guruswami 和 Johan Håstad。$(2+\epsilon)$-SAT 是 NP-困难的。*SIAM*计算杂志，46(5):1554–1573，2017年。[BBB21] Libor Barto、Diego Battistelli 和 Kevin M. Berg。对称承诺约束满足问题：超越布尔情形。载于 第*38*届国际计算机科学理论方面研讨会（*STACS'21*）论文集，*LIPIcs*第187卷，第10:1–10:16页，2021年。[BBKO21] Libor Barto、Jakub Bulín、Andrei A. Krokhin 和 Jakub Opršal。承诺约束满足的代数方法。*ACM* 杂志，68(4):28:1–28:66，2021年。[BD06] Andrei A. Bulatov 和 Víctor Dalmau。Mal'tsev 约束的简单算法。*SIAM*计算杂志，36(1):16–27，2006年。[BG19] Joshua Brakensiek 和 Venkatesan Guruswami。用于承诺约束满足问题的线性规划松弛与环方程的算法融合。载于 第三十届*ACM-SIAM*离散算法年会论文集，第436–455页。SIAM，2019年。[BG21a] Joshua Brakensiek 和 Venkatesan Guruswami。承诺约束满足：代数结构与对称布尔二分性。*SIAM*计算杂志，50(6):1663–1700，2021年。[BG21b] Joshua Brakensiek 和 Venkatesan Guruswami。追求具有完美完备性的强不可近似性结果。*ACM Trans. Algorithms*，17(3):27:1–27:35，2021年。[BGS23] Joshua Brakensiek、Venkatesan Guruswami 和 Sai Sandeep。布尔有序承诺约束满足问题的条件二分性。*TheoretiCS*，第2卷：8967，2023年1月。[BGS25] Joshua Brakensiek、Venkatesan Guruswami 和 Sai Sandeep。半定规划与承诺约束满足的鲁棒可满足性。*Discrete Anal.*，（14）：80，2025年。[BGWŽ20] Joshua Brakensiek、Venkatesan Guruswami、Marcin Wrochna 和 Stanislav Živný。基本线性规划与仿射松弛相结合对承诺约束满足问题的作用。*SIAM*计算杂志，49(6):1232–1248，2020年。

[BJK05] Andrei A. Bulatov、Peter Jeavons 和 Andrei A. Krokhin。使用有限代数对约束复杂性进行分类。SIAM计算杂志，34(3):720–742，2005年。[BK14] Libor Barto 和 Marcin Kozik。可通过局部一致性方法求解的约束满足问题。ACM 杂志，61(1)，2014年。[BK16] Libor Barto 和 Marcin Kozik。鲁棒可解的约束满足问题。SIAM计算杂志，45(4):1646–1669，2016年。[BK22] Libor Barto 和 Marcin Kozik。组合间隙定理与承诺约束满足问题之间的归约。载于第2022年ACM-SIAM离散算法研讨会（SODA'22）论文集，第1204–1220页。SIAM，2022年。[BK24] Demian Banakh 和 Marcin Kozik。承诺约束满足问题的单射困难性条件。载于 Pawel Sobocinski、Ugo Dal Lago 和 Javier Esparza 编，第39届ACM/IEEE计算机科学逻辑研讨会论文集，LICS 2024，爱沙尼亚塔林，2024年7月8日至11日，第8:1–8:10页。ACM，2024年。[BKM21] Mark Braverman、Subhash Khot 和 Dor Minzer。关于丰富的2对1游戏。载于第12届理论计算机科学创新会议（ITCS'21）论文集，LIPIcs第185卷，第27:1–27:20页。Schloss Dagstuhl - Leibniz信息学中心，2021年。[BR16] Jonah Brown-Cohen 和 Prasad Raghavendra。约束满足问题的相关性衰减与可处理性。载于第43届自动机、语言与编程国际研讨会（ICALP'16）论文集，LIPIcs第55卷，第79:1–79:13页。Schloss Dagstuhl - Leibniz信息学中心，2016年。[Bul17] Andrei A. Bulatov。非一致约束满足问题的二分定理。载于第58届IEEE计算机科学基础研讨会（FOCS'17）论文集，第319–330页，美国，2017年。IEEE。[BV04] Stephen P Boyd 和 Lieven Vandenberghe。凸优化。剑桥大学出版社，2004年。[BWŽ21] Alex Brandts、Marcin Wrochna 和 Stanislav Živný。非布尔域上承诺可满足性问题的复杂性。ACM计算理论汇刊，13(4):26:1–26:20，2021年。[BŽ22] Alex Brandts 和 Stanislav Živný。超越 PCSP(1-in-3,NAE)。信息与计算，2022年。[CKK+25] Lorenzo Ciardo、Marcin Kozik、Andrei A. Krokhin、Tamio-Vesa Nakajima 和 Stanislav Živný。1-in-3与非全相等：一个破裂承诺的二分性。ACM计算逻辑汇刊，26(2):10:1–10:22，2025年。[CMM06] Moses Charikar、Konstantin Makarychev 和 Yury Makarychev。唯一博弈的近似最优算法。载于第三十八届ACM

计算理论研讨会，第205–214页，美国华盛顿州西雅图，2006年5月。ACM。[CMM09] Moses Charikar、Konstantin Makarychev 和 Yury Makarychev。最大约束满足问题的近似最优算法。*ACM*计算算法汇刊，5(3):32:1–32:14，2009年。[CŽ23a] Lorenzo Ciardo 和 Stanislav Živný。近似图着色与晶体。载于*2023*年 *ACM-SIAM* 离散算法研讨会论文集（*SODA*），第2256–2267页。SIAM，2023年。[CŽ23b] Lorenzo Ciardo 和 Stanislav Živný。近似图着色与空心影。载于 Barna Saha 和 Rocco A. Servedio（编），第*55*届 *ACM* 计算理论年会论文集（*STOC 2023*），美国佛罗里达州奥兰多，*2023*年*6*月*20*日至*23*日，第623–631页。ACM，2023年。[CŽ23c] Lorenzo Ciardo 和 Stanislav Živný。CLAP：一种新的承诺约束满足问题算法。*SIAM*计算杂志，52(1):1–37，2023年。[CŽ23d] Lorenzo Ciardo 和 Stanislav Živný。通过张量构建 PCSP 的 minion 检验层级。载于*2023*年 *ACM-SIAM* 离散算法研讨会论文集（*SODA'23*），第568–580页，2023年。[CŽ24] Lorenzo Ciardo 和 Stanislav Živný。半定规划与线性方程对比同态问题。载于 Bojan Mohar、Igor Shinkar 和 Ryan O'Donnell（编），第*56*届 *ACM* 计算理论年会论文集（*STOC 2024*），加拿大不列颠哥伦比亚省温哥华，*2024*年*6*月*24*日至*28*日，第1935–1943页。ACM，2024年。[DiB16] Emmanuele DiBenedetto。实分析。Birkhäuser高级教材丛书《巴塞尔教科书》。Springer纽约，纽约州纽约市，2016年。[DK13] Víctor Dalmau 和 Andrei A. Krokhin。约束满足问题的鲁棒可满足性：困难性与算法结果。*ACM*计算理论汇刊，5(4):15:1–15:25，2013年。[FKOS19] Miron Ficak、Marcin Kozik、Miroslav Olšák 和 Szymon Stankiewicz。对称布尔承诺约束满足问题的二分定理。载于第*46*届自动机、语言与编程国际研讨会论文集（*ICALP'19*），第132卷，第57:1–57:12页。Schloss Dagstuhl – Leibniz-Zentrum für Informatik，2019年。[FNO+24] Marek Filakovský、Tamio-Vesa Nakajima、Jakub Opršal、Gianluca Tasinato 和 Uli Wagner。可3着色的3一致超图的线性序4着色之困难性。载于第*41*届国际计算机科学理论方面研讨会论文集（*STACS'24*），第289卷莱布尼茨信息学国际论文集（*LIPIcs*），第34:1–34:19页，2024年。[GJ76] M. R. Garey 和 David S. Johnson。近似最优图着色的复杂性。*ACM* 杂志，23(1):43–49，1976年。

[GLS93] Martin Grötschel、László Lovász 和 Alexander Schrijver。《几何算法与组合优化》，《算法与组合学》第2卷。Springer Berlin Heidelberg，德国海德堡，1993年。[GM12] Bernd Gärtner 和 Jiri Matousek。近似算法与半定规划。Springer Science & Business Media，2012年。[Gro75] Leonard Gross。对数 Sobolev 不等式。《美国数学杂志》，97(4):1061–1083，1975年。[GS20] Venkatesan Guruswami 和 Sai Sandeep。用 O(1) 种颜色为可3着色图着色的 d 对 1 的困难性。载于第47届自动机、语言与编程国际研讨会论文集（ICALP'20），第168卷 LIPIcs，第62:1–62:12页。Schloss Dagstuhl – Leibniz-Zentrum für Informatik，2020年。[GZ12] Venkatesan Guruswami 和 Yuan Zhou。近乎可满足的 Horn SAT 与精确击中集可近似性的紧确界。《理论计算》，8(1):239–267，2012年。[Hås01] Johan Håstad。一些最优不可近似性结果。《ACM 杂志》，48(4):798–859，2001年。[HMNŽ24] Johan Håstad、Björn Martinsson、Tamio-Vesa Nakajima 和 Stanislav Živný。线性有序着色的对数近似。载于 Amit Kumar 和 Noga Ron-Zewi（编），《近似、随机化与组合优化：算法与技术》，APPROX/RANDOM 2024，2024年8月28日至30日，伦敦政治经济学院，英国伦敦，第317卷 LIPIcs，第7:1–7:6页。Schloss Dagstuhl - Leibniz信息学中心，2024年。[IMM+10] Pawel M. Idziak、Petar Markovic、Ralph McKenzie、Matthew Valeriote 和 Ross Willard。少子幂代数带来的可处理性与可学习性。SIAM计算杂志，39(7):3023–3037，2010年。[Kho02] Subhash Khot。论唯一 2 证明者 1 轮游戏的威力。载于 STOC'02：第34届 ACM 计算理论研讨会论文集，第767–775页。ACM，纽约，2002年。[KKMO07] Subhash Khot、Guy Kindler、Elchanan Mossel 和 Ryan O'Donnell。最大割及其他二变量约束满足问题的最优不可近似性结果？SIAM计算杂志，37(1):319–357，2007年。[KOWŽ23] Andrei Krokhin、Jakub Opršal、Marcin Wrochna 和 Stanislav Živný。承诺约束满足中的拓扑与伴随。SIAM计算杂志，52(1):37–79，2023年。[LM00] Beatrice Laurent 和 Pascal Massart。通过模型选择自适应估计二次泛函。《统计年鉴》，第1302–1338页，2000年。[LŽ25] Alberto Larrauri 和 Stanislav Živný。在幺半群与群上求解承诺方程。ACM计算逻辑汇刊，26(1):3:1–3:24，2025年。

[MOO10] Elchanan Mossel、Ryan O'Donnell 和 Krzysztof Oleszkiewicz。低影响布尔函数的噪声稳定性：不变性与最优性。数学年刊 *(2)*，171(1):295–341，2010年。[Mot25] Antoine Mottet。承诺约束满足问题与无限域约束满足问题之间的代数与算法协同。载于第*40*届 *ACM/IEEE*计算机科学逻辑研讨会论文集，*LICS 2025*，2025年。[NVWŽ25] Tamio-Vesa Nakajima、Zephyr Verwimp、Marcin Wrochna 和 Stanislav Živný。近似冲突自由着色、线性有序着色及非单色超图着色的复杂性。载于 Keren Censor-Hillel、Fabrizio Grandoni、Joël Ouaknine 和 Gabriele Puppis 编，第*52*届自动机、语言与编程国际研讨会，*ICALP 2025*，*2025*年*7*月*8*日至*11*日，丹麦奥胡斯，第334卷，*LIPIcs*，第169:1–169:10页。Schloss Dagstuhl - Leibniz信息学中心，2025年。[NŽ22] Tamio-Vesa Nakajima 和 Stanislav Živný。超图的线性有序着色。*ACM*计算理论汇刊，13(3–4)，2022年。[NŽ24] Tamio-Vesa Nakajima 和 Stanislav Živný。关于对称与函数型部分约束满足问题的复杂性。*ACM*算法汇刊，20(4):33:1–33:29，2024年。[O'D14] Ryan O'Donnell。布尔函数分析。剑桥大学出版社，2014年。[Rag08] Prasad Raghavendra。每个约束满足问题都有最优算法和不可近似性结果吗？载于第*40*届 *ACM* 年度计算理论研讨会论文集（*STOC'08*），第245–254页，2008年。[RS09] Prasad Raghavendra 和 David Steurer。如何对任意约束满足问题进行舍入。载于*2009*年第*50*届年度 *IEEE*计算机科学基础研讨会，第586–594页。IEEE，2009年。[Sch78] Thomas Schaefer。可满足性问题的复杂性。载于第*10*届 *ACM* 年度计算理论研讨会论文集（*STOC'78*），第216–226页，1978年。[Ver18] Roman Vershynin。高维概率：数据科学应用导论，第47卷，剑桥统计与概率数学丛书。剑桥大学出版社，2018年。[Zhu20] Dmitriy Zhuk。约束满足问题二分猜想的证明。*ACM* 杂志，67(5):30:1–30:78，2020年。[Zwi98] Uri Zwick。寻找近似满足赋值。载于第*13*届 *ACM* 年度计算理论研讨会论文集（*STOC'98*），第551–560页。ACM，1998年。

A 省略的证明

本节将证明论文前几节中陈述的一些技术性结果。

A.1 第 3 节中省略的证明

我们首先正式证明以下定理中的第一个陈述（参见第3.3节中给出的证明概要）。

定理 3.7。 对于所有 $\epsilon > 0$，如果 $d \geq \frac{80000000}{\epsilon^3}$ 比上述整数间隙实例（第*3.3*节）

1. 存在一个半定规划解，使每个未被舍弃的约束都至少获得 $1 - \epsilon$ 的值。*2.* 被采样的约束中，至多有 $6e^{-\frac{10}{\epsilon}}$ 被舍弃。*3.* 所有赋值都至少违反 $10^{60}\lceil log(\frac{1}{\epsilon})\rceil$ 个被采样的 *NAE-SAT* 约束（包括被舍弃的约束）。

我们将使用一些技术引理。

引理 A.1。 若 $\mathbf{v}_1, \mathbf{v}_2$，和 $\mathbf{v}_3$ 是单位向量，且 $\mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3 = -\mathbf{v}_0$，则存在一个概率分布 D，其支撑集为赋值 $\{(-1,-1,1),(-1,1,-1),(1,-1,-1)\}$，使得

1. 对所有 $i \in [3]$，$\mathbb{E}_D[x_i] = \mathbf{v}_i \cdot \mathbf{v}_0$。*2.* 对所有互不相同的 $i, j \in [3]$，$\mathbb{E}_D[x_i x_j] = \mathbf{v}_i \cdot \mathbf{v}_j$。

证明。 令 D 为如下概率分布：以概率 $\frac{1+\mathbf{v}_3\cdot\mathbf{v}_0}{2}$，取赋值 $(-1,-1,1)$，以概率 $\frac{1+\mathbf{v}_2\cdot\mathbf{v}_0}{2}$，取赋值 $(-1,1,-1)$，并以概率 $\frac{1+\mathbf{v}_1\cdot\mathbf{v}_0}{2}$ 取赋值 $(1,-1,-1)$。现在我们作出以下观察：

1. $\mathbb{E}_D[x_1] = \frac{1+\mathbf{v}_1\cdot\mathbf{v}_0}{2} - \frac{1+\mathbf{v}_2\cdot\mathbf{v}_0}{2} - \frac{1+\mathbf{v}_3\cdot\mathbf{v}_0}{2} = \mathbf{v}_1\cdot\mathbf{v}_0 - \frac{(\mathbf{v}_1+\mathbf{v}_2+\mathbf{v}_3)\cdot\mathbf{v}_0}{2} = \mathbf{v}_1\cdot\mathbf{v}_0$。

2.
$$\begin{aligned}\mathbb{E}_D[x_1x_2] &= -\frac{1+\mathbf{v}_1\cdot\mathbf{v}_0}{2} - \frac{1+\mathbf{v}_2\cdot\mathbf{v}_0}{2} + \frac{1+\mathbf{v}_3\cdot\mathbf{v}_0}{2} = \frac{-1+(\mathbf{v}_1+\mathbf{v}_2-\mathbf{v}_3)\cdot(\mathbf{v}_1+\mathbf{v}_2+\mathbf{v}_3)}{2} \\ &= \frac{-1+\mathbf{v}_1\cdot\mathbf{v}_1+2\mathbf{v}_1\cdot\mathbf{v}_2+\mathbf{v}_2\cdot\mathbf{v}_2-\mathbf{v}_3\cdot\mathbf{v}_3}{2} = \mathbf{v}_1\cdot\mathbf{v}_2\end{aligned}$$

其余情形由对称性可得。 □

引理 A.2。 给定单位向量 $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}'_1, \mathbf{v}'_2$ 和 $\mathbf{v}'_3$，使得

1. 对所有 $i \in [3]$，$\mathbf{v}'_i \cdot \mathbf{v}_0 = \mathbf{v}_i \cdot \mathbf{v}_0 + \Delta_i$。*2.* 对所有互不相同的 i、$j \in [3]$，$\mathbf{v}'_i \cdot \mathbf{v}'_j = \mathbf{v}_i \cdot \mathbf{v}_j + \Delta_{ij}$。

对于某些 Δ_1、Δ_2、Δ_3、Δ_{12}、Δ_{13}、$\Delta_{23} \in \mathbb{R}$，如果存在概率分布 D 使得

1. 对所有 $i \in [3]$，$\mathbb{E}_D[x_i] = \mathbf{v}_i \cdot \mathbf{v}_0$。

2. 对所有互不相同的 $i, j \in [3]$, $\mathbb{E}_D[x_i x_j] = \mathbf{v}_i \cdot \mathbf{v}_j$。

那么存在一个伪分布 D'（也就是说，D' 可能会给某些事件赋予负概率，但概率总和仍应为1），使得

1. 对所有 $i \in [3]$，$\mathbb{E}_{D'}[x_i] = \mathbf{v}'_i \cdot \mathbf{v}_0$。2. 对所有互不相同的 i、$j \in [3]$、$\mathbb{E}_{D'}[x_i x_j] = \mathbf{v}'_i \cdot \mathbf{v}'_j$。3. 对每个赋值 $(x_1, x_2, x_3) \in \{-1, 1\}^3$，该赋值在 D' 和 D 下的（伪）概率之差至多为 $\frac{|\Delta_1|+|\Delta_2|+|\Delta_3|+|\Delta_{12}|+|\Delta_{13}|+|\Delta_{23}|}{8}$。

这可由以下命题推出。

命题 *A.3.* 若 v_1, v_2, 和 v_3 是单位向量，且 $p_{-1,-1,-1}$、$p_{-1,-1,1}$、$p_{-1,1,-1}$、$p_{-1,1,1}$、$p_{1,-1,-1}$、$p_{1,-1,1}$、$p_{1,1,-1}$、$p_{1,1,1}$ 以及 $p_{1,1,1}$ 均为实数，且满足

1. $p_{1,-1,-1} + p_{1,-1,1} + p_{1,1,-1} + p_{1,1,1} + p_{-1,-1,-1} + p_{-1,-1,1} + p_{-1,1,-1} + p_{-1,1,1} = 1$
2. $v_1 \cdot v_0 = p_{1,-1,-1} + p_{1,-1,1} + p_{1,1,-1} + p_{1,1,1} - p_{-1,-1,-1} - p_{-1,-1,1} - p_{-1,1,-1} - p_{-1,1,1}$.
3. $v_2 \cdot v_0 = p_{-1,1,-1} + p_{-1,1,1} + p_{1,1,-1} + p_{1,1,1} - p_{-1,-1,-1} - p_{-1,-1,1} - p_{1,-1,-1} - p_{1,-1,1}$.
4. $v_3 \cdot v_0 = p_{-1,-1,1} + p_{-1,1,1} + p_{1,-1,1} + p_{1,1,1} - p_{-1,-1,-1} - p_{-1,1,-1} - p_{1,-1,-1} - p_{1,1,-1}$.
5. $v_1 \cdot v = p_{-1,-1,-1} + p_{-1,-1,1} + p_{1,1,-1} + p_{1,1,1} - p_{-1,1,-1} - p_{-1,1,1} - p_{1,-1,-1} - p_{1,-1,1}$.
6. $v_1 \cdot v = p_{-1,-1,-1} + p_{-1,1,-1} + p_{1,-1,1} + p_{1,1,1} - p_{-1,-1,1} - p_{-1,1,1} - p_{1,-1,-1} - p_{1,1,-1}$.
7. $v_2 \cdot v = p_{-1,-1,-1} + p_{1,-1,-1} + p_{-1,1,1} + p_{1,1,1} - p_{-1,-1,1} - p_{1,-1,1} - p_{-1,1,-1} - p_{1,1,-1}$.

并且$\mathbf{v}'_1$、$\mathbf{v}'_2$和$\mathbf{v}'_3$ 是单位向量，使得

1. 对所有 $i \in [3]$，$\mathbf{v}'_i \cdot \mathbf{v}_0 = \mathbf{v}_i \cdot \mathbf{v}_0 + \Delta_i$。2. 对所有不同的 i、$j \in [3]$，$\mathbf{v}'_i \cdot \mathbf{v}'_j = \mathbf{v}_i \cdot \mathbf{v}_j + \Delta_{ij}$。

对于某些 $\Delta_1, \Delta_2, \Delta_3, \Delta_{12}, \Delta_{13}, \Delta_{23} \in \mathbb{R}$，那么如果我们取

1. $p'_{-1,-1,-1} = p_{-1,-1,-1} + \frac{-\Delta_1-\Delta_2-\Delta_3+\Delta_{12}+\Delta_{13}+\Delta_{23}}{8}$
2. $p'_{-1,-1,1} = p_{-1,-1,1} + \frac{-\Delta_1-\Delta_2+\Delta_3+\Delta_{12}-\Delta_{13}-\Delta_{23}}{8}$
3. $p'_{-1,1,-1} = p_{-1,1,-1} + \frac{-\Delta_1+\Delta_2-\Delta_3-\Delta_{12}+\Delta_{13}-\Delta_{23}}{8}$
4. $p'_{1,-1,-1} = p_{1,-1,-1} + \frac{\Delta_1-\Delta_2-\Delta_3-\Delta_{12}-\Delta_{13}+\Delta_{23}}{8}$
5. $p'_{-1,1,1} = p_{-1,1,1} + \frac{-\Delta_1+\Delta_2+\Delta_3-\Delta_{12}-\Delta_{13}+\Delta_{23}}{8}$
6. $p'_{1,-1,1} = p_{1,-1,1} + \frac{\Delta_1-\Delta_2+\Delta_3-\Delta_{12}+\Delta_{13}-\Delta_{23}}{8}$
7. $p'_{1,1,-1} = p_{1,1,-1} + \frac{\Delta_1+\Delta_2-\Delta_3+\Delta_{12}-\Delta_{13}-\Delta_{23}}{8}$

8. $p'_{1,1,1} = p_{1,1,1} + \frac{\Delta_1+\Delta_2+\Delta_3+\Delta_{12}+\Delta_{13}+\Delta_{23}}{8}$

我们将得到

1. $p'_{1,-1,-1} + p'_{1,-1,1} + p'_{1,1,-1} + p'_{1,1,1} + p'_{-1,-1,-1} + p'_{-1,-1,1} + p'_{-1,1,-1} + p'_{-1,1,1} = 1$
2. $\mathbf{v}'_1 \cdot \mathbf{v}_0 = p'_{1,-1,-1} + p'_{1,-1,1} + p'_{1,1,-1} + p'_{1,1,1} - p'_{-1,-1,-1} - p'_{-1,-1,1} - p'_{-1,1,-1} - p'_{-1,1,1}$.
3. $\mathbf{v}'_2 \cdot \mathbf{v}_0 = p'_{-1,1,-1} + p'_{-1,1,1} + p'_{1,1,-1} + p'_{1,1,1} - p'_{-1,-1,-1} - p'_{-1,-1,1} - p'_{1,-1,-1} - p'_{1,-1,1}$.
4. $\mathbf{v}'_3 \cdot \mathbf{v}_0 = p'_{-1,-1,1} + p'_{-1,1,1} + p'_{1,-1,1} + p'_{1,1,1} - p'_{-1,-1,-1} - p'_{-1,1,-1} - p'_{1,-1,-1} - p'_{1,1,-1}$.
5. $\mathbf{v}'_1 \cdot \mathbf{v}'_2 = p'_{-1,-1,-1} + p'_{-1,-1,1} + p'_{1,1,-1} + p'_{1,1,1} - p'_{-1,1,-1} - p'_{-1,1,1} - p'_{1,-1,-1} - p'_{1,-1,1}$.
6. $\mathbf{v}'_1 \cdot \mathbf{v}'_3 = p'_{-1,-1,-1} + p'_{-1,1,-1} + p'_{1,-1,1} + p'_{1,1,1} - p'_{-1,-1,1} - p'_{-1,1,1} - p'_{1,-1,-1} - p'_{1,1,-1}$.
7. $\mathbf{v}'_2 \cdot \mathbf{v}'_3 = p'_{-1,-1,-1} + p'_{1,-1,-1} + p'_{-1,1,1} + p'_{1,1,1} - p'_{-1,-1,1} - p'_{1,-1,1} - p'_{-1,1,-1} - p'_{1,1,-1}$.

证明。 这由以下观察可知:

1. $\pm\frac{\Delta_i}{8}$项对$\mathbf{v}'_i \cdot \mathbf{v}_0$ 的求和贡献 Δ_i，并在其他求和中相互抵消。

2. 同理， $\pm\frac{\Delta_{ij}}{8}$ 项对$\mathbf{v}'_i \cdot \mathbf{v}'_j$ 的求和贡献 Δ_{ij}，并在其他求和中相互抵消。

□

引理 A. 4. 若$\mathbf{v}'_1$、$\mathbf{v}'_2$和$\mathbf{v}'_3$ 是单位向量，且 D' 是伪分布，使得

1. 对所有 $i \in [3]$、 $\mathbb{E}_{D'}[x_i] = \mathbf{v}'_i \cdot \mathbf{v}_0$。2. 对所有互不相同的 i、 $j \in [3]$、 $\mathbb{E}_{D'}[x_i x_j] = \mathbf{v}'_i \cdot \mathbf{v}'_j$。

那么，如果我们取$\mathbf{v}''_1 = \sqrt{1-\epsilon'^2}\mathbf{v}'_1 + \epsilon'\mathbf{z}_1$, $\mathbf{v}''_2 = \sqrt{1-\epsilon'^2}\mathbf{v}'_2 + \epsilon'\mathbf{z}_2$, 以及$\mathbf{v}''_3 = \sqrt{1-\epsilon'^2}\mathbf{v}'_3 + \epsilon'\mathbf{z}_3$，其中$\mathbf{z}_1$, $\mathbf{z}_2$, 和$\mathbf{z}_3$ 与$\mathbf{v}'_1$、$\mathbf{v}'_2$、$\mathbf{v}'_3$彼此正交，对某个 $\epsilon' > 0$ 成立，并取 D''为如下伪分布：在 D'' 下每个赋值出现的概率为$(1-\epsilon')$ 乘以该赋值在 D' 下出现的概率，再加上 $\frac{\epsilon'}{8}$，那么

−

1. 对所有 $i \in [3]$, $\mathbb{E}_{D''}[x_i] = \mathbf{v}''_i \cdot \mathbf{v}_0$均成立。2. 对所有互不相同的 $i, j \in [3]$, $\mathbb{E}_{D''}[x_i x_j] = \mathbf{v}''_i \cdot \mathbf{v}''_j$均成立。

这由以下命题得出。

命题 A.5. 若 v'_1、v'_2 和 v'_3 为单位向量，且 p'_{-1}、-1、-1、 p'_{-1}、-1、1、 p'_{-1}、1、-1、 p'_{-1}、1、1、p'_1、-1、-1、 p'_1、-1、1、p'_1、1、-1 和 p'_1、1、1 为实数（不必非负），使得

1. $p'_{1,-1,-1} + p'_{1,-1,1} + p'_{1,1,-1} + p'_{1,1,1} + p'_{-1,-1,-1} + p'_{-1,-1,1} + p'_{-1,1,-1} + p'_{-1,1,1} = 1$ 2. $v'_1 \cdot v$
$0 = p'_{1,-1,-1} + p'_{1,-1,1} + p'_{1,1,-1} + p'_{1,1,1} - p'_{-1,-1,-1} - p'_{-1,-1,1} - p'_{-1,1,-1} - p'_{-1,1,1}$. 3. $v'_2 \cdot v$
$0 = p'_{-1,1,-1} + p'_{-1,1,1} + p'_{1,1,-1} + p'_{1,1,1} - p'_{-1,-1,-1} - p'_{-1,-1,1} - p'_{1,-1,-1} - p'_{1,-1,1}$. 4. $v'_3 \cdot v$
$0 = p'_{-1,-1,1} + p'_{-1,1,1} + p'_{1,-1,1} + p'_{1,1,1} - p'_{-1,-1,-1} - p'_{-1,1,-1} - p'_{1,-1,-1} - p'_{1,1,-1}$.

5. $\mathbf{v}_1' \cdot \mathbf{v}_2' = p'_{-1,-1,-1} + p'_{-1,-1,1} + p'_{1,1,-1} + p'_{1,1,1} - p'_{-1,1,-1} - p'_{-1,1,1} - p'_{1,-1,-1} - p'_{1,-1,1}$.

6. $\mathbf{v}_1' \cdot \mathbf{v}_3' = p'_{-1,-1,-1} + p'_{-1,1,-1} + p'_{1,-1,1} + p'_{1,1,1} - p'_{-1,-1,1} - p'_{-1,1,1} - p'_{1,-1,-1} - p'_{1,1,-1}$.

7. $\mathbf{v}_2' \cdot \mathbf{v}_3' = p'_{-1,-1,-1} + p'_{1,-1,-1} + p'_{-1,1,1} + p'_{1,1,1} - p'_{-1,-1,1} - p'_{1,-1,1} - p'_{-1,1,-1} - p'_{1,1,-1}$.

那么如果我们取$\mathbf{v}_1'' = \sqrt{1-\epsilon'^2}\mathbf{v}_1' + \epsilon' z_1, \mathbf{v}_2'' = \sqrt{1-\epsilon'^2}\mathbf{v}_2' + \epsilon' z_2$, 与$\mathbf{v}_3'' = \sqrt{1-\epsilon'^2}\mathbf{v}_3' + \epsilon' z_3$，其中$z_1$，$z_2$，与$z_3$ 正交于$\mathbf{v}_1'$, $\mathbf{v}_2'$, $\mathbf{v}_3'$且彼此正交，那么如果我们取$p''_{-1,-1,-1} = (1-\epsilon')p'_{-1,-1,-1} + \frac{\epsilon'}{8}$, $p''_{-1,-1,1} = (1-\epsilon')p'_{-1,-1,1} + \frac{\epsilon'}{8}$, $p''_{-1,1,-1} = (1-\epsilon')p'_{-1,1,-1} + \frac{\epsilon'}{8}$, $p''_{-1,1,1} = (1-\epsilon')p'_{-1,1,1} + \frac{\epsilon'}{8}$, $p''_{1,-1,-1} = (1-\epsilon')p'_{1,-1,-1} + \frac{\epsilon'}{8}$, $p''_{1,-1,1} = (1-\epsilon')p'_{1,-1,1} + \frac{\epsilon'}{8}$, $p''_{1,1,-1} = (1-\epsilon')p'_{1,1,-1} + \frac{\epsilon'}{8}$, 与$p''_{1,1,1} = (1-\epsilon')p'_{1,1,1} + \frac{\epsilon'}{8}$ 则

1. $p''_{1,-1,-1} + p''_{1,-1,1} + p''_{1,1,-1} + p''_{1,1,1} + p''_{-1,-1,-1} + p''_{-1,-1,1} + p''_{-1,1,-1} + p''_{-1,1,1} = 1$

2. $\mathbf{v}_1'' \cdot \mathbf{v}_0 = p''_{1,-1,-1} + p''_{1,-1,1} + p''_{1,1,-1} + p''_{1,1,1} - p''_{-1,-1,-1} - p''_{-1,-1,1} - p''_{-1,1,-1} - p''_{-1,1,1}$.

3. $\mathbf{v}_2'' \cdot \mathbf{v}_0 = p''_{-1,1,-1} + p''_{-1,1,1} + p''_{1,-1,1} + p''_{1,1,1} - p''_{-1,-1,-1} - p''_{-1,-1,1} - p''_{1,-1,-1} - p''_{1,-1,1}$.

4. $\mathbf{v}_3'' \cdot \mathbf{v}_0 = p''_{-1,-1,1} + p''_{-1,1,1} + p''_{1,-1,1} + p''_{1,1,1} - p''_{-1,-1,-1} - p''_{-1,1,-1} - p''_{1,-1,-1} - p''_{1,1,-1}$.

5. $\mathbf{v}_1'' \cdot \mathbf{v}_2'' = p''_{-1,-1,-1} + p''_{-1,-1,1} + p''_{1,1,-1} + p''_{1,1,1} - p''_{-1,1,-1} - p''_{-1,1,1} - p''_{1,-1,-1} - p''_{1,-1,1}$.

6. $\mathbf{v}_1'' \cdot \mathbf{v}_3'' = p''_{-1,-1,-1} + p''_{-1,1,-1} + p''_{1,-1,1} + p''_{1,1,1} - p''_{-1,-1,1} - p''_{-1,1,1} - p''_{1,-1,-1} - p''_{1,1,-1}$.

7. $\mathbf{v}_2'' \cdot \mathbf{v}_3'' = p''_{-1,-1,-1} + p''_{1,-1,-1} + p''_{-1,1,1} + p''_{1,1,1} - p''_{-1,-1,1} - p''_{1,-1,1} - p''_{-1,1,-1} - p''_{1,1,-1}$.

证明。 这可由以下观察得出：

1. 对所有 $i \in [3]$, $\mathbf{v}_i'' \cdot \mathbf{v}_0 = (1-\epsilon')\mathbf{v}_i' \cdot \mathbf{v}_0$。

2. 对所有互不相同的 $i, j \in [3]$, $\mathbf{v}_i'' \cdot \mathbf{v}_j'' = (1-\epsilon')\mathbf{v}_i' \cdot \mathbf{v}_j'$。

3. 在上述每个求和中， $\frac{\epsilon'}{8}$ 项会相互抵消，因为为每个可能的赋值分配概率 $\frac{\epsilon'}{8}$ 不会对偏差或成对偏差产生任何贡献。 □

定理 3.7的第一条结论的证明： 为证明定理3.7的第一条结论，我们注意到，对于从 T_x' 或 T_{-x}' 中采样且未被舍弃的每组三个向量 $\mathbf{v}_1', \mathbf{v}_2', \mathbf{v}_3'$，都存在一组三个单位向量 $\mathbf{v}_1, \mathbf{v}_2$, 和$\mathbf{v}_3$，使得$\mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3 = \pm\mathbf{v}_0$，且对所有 $i \in [3]$, $\left\| \frac{\mathbf{v}}{\|\mathbf{v}\|} - \frac{\mathbf{v}_i'}{\|\mathbf{v}_i'\|} - \mathbf{v}_i \right\| \le \frac{\epsilon}{100}$。

为此，注意到当我们从 $\mathcal{N}(0, 1/d)^d$ 中采样 $\mathbf{w}$ 和 $\mathbf{u}$ 时，我们可以取

1. $\mathbf{v}_1 = bx\mathbf{v}_0 + \sqrt{1-x^2}\left(-\frac{\sqrt{1-(2|x|-1)^2}}{2\sqrt{1-x^2}} \frac{\mathbf{w}}{\|\mathbf{w}\|} + \sqrt{1 - \frac{1-(2|x|-1)^2}{4(1-x^2)}} \frac{\mathbf{u}}{\|\mathbf{u}\|} \right)$,

2. $\mathbf{v}_2 = bx\mathbf{v}_0 + \sqrt{1-x^2}\left(-\frac{\sqrt{1-(2|x|-1)^2}}{2\sqrt{1-x^2}} \frac{\mathbf{w}}{\|\mathbf{w}\|} - \sqrt{1 - \frac{1-(2|x|-1)^2}{4(1-x^2)}} \frac{\mathbf{u}}{\|\mathbf{u}\|} \right)$,

3. $\mathbf{v}_3 = b(1-2x)\mathbf{v}_0 + \sqrt{1-(2|x|-1)^2}\frac{\mathbf{w}}{\|\mathbf{w}\|}$,

其中 $b \in \{-1, 1\}$。我们需要进行以下调整，将 $\mathbf{v}_i$ 移至 $\frac{\mathbf{v}_i'}{\|\mathbf{v}_i'\|}$： —

1. $||w||$ 和 $||u||$ 与 1 的差最多可达 $\frac{\epsilon}{1000}$。2. 我们需要将基于 $\mathbf{w}$ 和 $\mathbf{u}$获得的向量移至其所在区域的中心$\mathbf{v}_1'$、$\mathbf{v}_2'$和$\mathbf{v}_3'$。3. 我们需要重新缩放 $\mathbf{v}_1'$、$\mathbf{v}_2'$和 $\mathbf{v}_3'$。

不难证明，这些调整的总长度至多为 $\frac{\epsilon}{100}$。

对于向量三元组 $(\mathbf{v}_0,\mathbf{v}_0,\mathbf{v}')$（其中 $\mathbf{v}'$ 从 A'_{-x_0} 中采样）以及向量三元组 $(-\mathbf{v}0,-\mathbf{v}_0,\mathbf{v}')$（其中 $\mathbf{v}'$ 从 A'_{x_0} 中采样），也适用类似的论证。对于这些三元组，我们分别使用 $(\mathbf{v}_1,\mathbf{v}_2,\mathbf{v}_3) = (\mathbf{v}_0,\mathbf{v}0,-\mathbf{v}_0)$ 和 $(\mathbf{v}_1,\mathbf{v}_2,\mathbf{v}_3) == (-\mathbf{v}0,-\mathbf{v}_0,\mathbf{v}_0)$。

第一个结论现在可通过应用引理 A.1、A.2 和A.4 得出。对于每个未被舍弃的三元组，令 $\mathbf{v}_1$，$\mathbf{v}_2$，和 $\mathbf{v}_3$ 为上述论证中的向量。根据引理A.1，存在一个分布 D，其支撑集由满足赋值构成，使得

1. 对所有 $i \in [3]$, $\mathbb{E}_D[x_i] = \mathbf{v}_i \cdot \mathbf{v}_0$。2. 对所有互不相同的 $i,j \in [3]$, $\mathbb{E}_D[x_i x_j] = \mathbf{v}_i \cdot \mathbf{v}j$。

根据引理A.2，存在一个伪分布 D' 使得

1. 对所有 $i \in [3]$, $\mathbb{E}_{D'}[x_i] = \frac{\mathbf{v}_i}{||\mathbf{v}'_i||} \cdot \mathbf{v}_0$。2. 对所有互不相同的 $i,\ j \in [3]$, $\mathbb{E}_{D'}[x_i x_j] = \frac{\mathbf{v}_i}{||\mathbf{v}'_i||} \cdot \frac{\mathbf{v}_j}{||\mathbf{v}'_j||}$。

3. 对于每个赋值 $(x_1,\ x_2,\ x_3) \in \{-1,1\}^3$，该赋值在 D 和 D' 下的（伪）概率之差至多为 $\frac{\epsilon}{50}$。

根据引理A.4，令 D'' 为如下概率分布：若某赋值在 D' 下的伪概率为 p $(1-\frac{\epsilon}{4})p + \frac{\epsilon}{32}$ 下的概率为 D''，则我们有

1. 对所有 $i \in [3]$, $\mathbb{E}_{D''}[x_i] = \left(\sqrt{1-\frac{\epsilon}{4}\mathbf{v}_i} \frac{\mathbf{v}'_i}{||\mathbf{v}'_i||} + \frac{\sqrt{\epsilon}}{2}\mathbf{z}_{\mathbf{v}'_i}\right) \cdot \mathbf{v}_0$。

2. 对所有互不相同的 $i,\ j \in [3]$, $\mathbb{E}_{D''}[x_i x_j] = \left(\sqrt{1-\frac{\epsilon}{4}\mathbf{v}_i} \frac{\mathbf{v}'_i}{||\mathbf{v}'_i||} + \frac{\sqrt{\epsilon}}{2}\mathbf{z}_{\mathbf{v}'_j}\right) \cdot \left(\sqrt{1-\frac{\epsilon}{4}\mathbf{v}_j} \frac{\mathbf{v}'_j}{||\mathbf{v}'_j||} + \frac{\sqrt{\epsilon}}{2}\mathbf{z}_{\mathbf{v}'_j}\right)$。

□

现在我们证明引理 3.9。

引理 3.9. 以下尾界成立：

1. 对所有 $t \in [0,1]$，如果 $\mathbf{w} \sim \mathcal{N}(0,1/d)^d$，那么 $P\left(|(||\mathbf{w}||^2 - 1)| \geq t\right) \leq 2e^{-\frac{dt}{8}}$。*2.* 给定一个向量 $\mathbf{w}$，对于所有 $t \geq 0$，如果 $\mathbf{u} \sim \mathcal{N}(0,1/d)^d$ 与 $\mathbf{w}$ 相互独立，那么 $P(|\mathbf{w} \cdot \mathbf{u}| \geq \frac{dt}{2}t) \leq 2e^{-\frac{2}{2||\mathbf{w}||^2}}$。

证明。对于第一个陈述，写作 $||\mathbf{w}||^2 - 1 = \sum_{j=1}^{d}(w_j^2 - \frac{1}{d})$，其中每个 w_j 都独立地从 $N(0, \frac{1}{d})$ 中抽取，因为

$$\mathbb{E}\left[e^{\beta(w_j^2-\frac{1}{d})}\right] = \int_{-\infty}^{\infty}\frac{\sqrt{d}}{\sqrt{2\pi}}e^{-\frac{dw^2}{2}}e^{\beta(w^2-\frac{1}{d})}dw = \sqrt{\frac{d}{d-2\beta}}e^{-\frac{\beta}{d}}\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi}}e^{-\frac{z^2}{2}}dz = \sqrt{\frac{d}{d-2\beta}}e^{-\frac{\beta}{d}}$$

每当 $|\beta| < \frac{d}{2}$ 时，若令 $\beta' = \frac{\beta}{d}$，则有

$$P\left(\sum_{j=1}^{d}\left({w_j}^2 - \frac{1}{d}\right) \geq t\right) \leq \frac{\mathbb{E}\left[e^{\beta\sum_{j=1}^{d}({w_j}^2-\frac{1}{d})}\right]}{e^{\beta t}} \leq e^{-d(\beta' t+\beta'+\frac{1}{2}ln(1-2\beta'))}$$

and

$$P\left(\sum_{j=1}^{d}\left({w_j}^2 - \frac{1}{d}\right) \leq -t\right) \leq \frac{\mathbb{E}\left[e^{\beta\sum_{j=1}^{d}({w_j}^2-\frac{1}{d})}\right]}{e^{-\beta t}} \leq e^{-d(-\beta' t+\beta'+\frac{1}{2}ln(1-2\beta'))}.$$

每当 $|\beta'| < \frac{1}{2}$ 时。由于 $\ln(1-x) = -\sum_{j=1}^{\infty}\frac{x^j}{j}$，若 $|x| \leqq \frac{1}{2}$，则 $\ln(1-x) \geq -x - x^2$。因此令 $\beta' = \frac{t}{4}$，可得 $P\left(\sum_{j=1}^{d}\left({w_j}^2 - \frac{1}{d}\right) \geq t\right) \leq e^{-\frac{dt^2}{8}}$。类似地，令 $\beta' = -\frac{t}{4}$，可得 $P\left(\sum_{j=1}^{d}\left({w_j}^2 - \frac{1}{d}\right) \leq -t\right) \leq e^{-\frac{dt^2}{8}}$。

对于第二个结论，注意到对所有 $\beta \geq 0$，由于 $\mathbf{w}\cdot\mathbf{u} = \sum_{j=1}^{d} w_j u_j$ 且

$$\mathbb{E}\left[e^{\beta w_j u_j}\right] = \int_{-\infty}^{\infty}\frac{\sqrt{d}}{\sqrt{2\pi}}e^{-\frac{du^2}{2}}e^{\beta w_j u}du = e^{\frac{\beta^2 w_j^2}{2d}}\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi}}e^{-\frac{\left(z-\frac{\beta w_j}{\sqrt{d}}\right)^2}{2}}dz = e^{\frac{\beta^2 w_j^2}{2d}}$$

我们有，对于所有的 $t \geq 0$, $P(\mathbf{w}\cdot\mathbf{u} \geq t) \leq \frac{\mathbb{E}\left[e^{\beta\sum_{j=1}^{d} w_j u_j}\right]}{e^{\beta t}} = e^{\frac{\beta^2||w||^2}{2d} - \beta t}$。代入 $\beta = \frac{td}{||w||^2}$，$e^{\frac{dt^2}{}}$，得到 $P(\mathbf{w}\cdot\mathbf{u} \geq t) \leq 2e^{-2||\mathbf{w}||^2}$。根据对称性，$P(\mathbf{w}\cdot\mathbf{u} \leq -t) \leq 2e^{-2||\mathbf{w}||^2}$。 □

A.2 第 6 节中省略的证明

我们将证明以下结论。

引理 6.17. 对于任意 $\mathcal{V}, \mathcal{W} \in (\mathbb{S}_A^N)^Y$，我们有

(1) $\mathrm{Mat}(\mathcal{V}) \in K_{Y,\,A}$。 *(2)* $\mathrm{Mat}(\mathcal{V}) - \mathrm{Mat}(\mathcal{W}) \in K^0_{Y,\,A}$。

证明。首先我们证明 (1) 蕴含 (2)。为说明这一点，由 (1) 可知，对所有 $\mathbf{a} \in A^Y$，存在 $\lambda_{\mathbf{a}} \in \mathbb{R}$ 使得

$$\mathrm{Mat}(\mathcal{V}) - \mathrm{Mat}(\mathcal{W}) = \sum_{\mathbf{a}\in A^Y}\lambda_{\mathbf{a}}\,\mathrm{Mat}(\mathbf{a}). \tag{43}$$

注意到，利用(29)，$\mathsf{Tr}(\mathsf{Mat}(\mathcal{V})) = \mathsf{Tr}(\mathsf{Mat}(\mathcal{W})) = \mathsf{Tr}(\mathsf{Mat}(\mathbf{a})) = |Y|$ 对所有 $\mathbf{a} \in A^Y$ 成立。因此，(43) 的迹蕴含 $\sum_{\mathbf{a}\in A^Y} \lambda_{\mathbf{a}} = 0$。故 $\mathsf{Mat}(\mathcal{V}) - \mathsf{Mat}(\mathcal{W}) \in K^0_{Y,A}$，即为所求。

接下来我们着重证明 (1)。我们先给出一个自洽证明，然后说明如何根据关于超矩阵投影的一个结果推导出相同结论。

令 $K^*_{Y,\,A} : \mathbb{R}^{(Y\times A)^2} \to \mathbb{R}$ 为 $K_{Y,\,A}$ 的对偶线性空间。只需证明，对于每个 $M \in K^*_{Y,\,A}$，都有 $M(\mathsf{Mat}(\mathcal{V})) = 0$。我们可以将每个元素 $M \in K_{Y,\,A}$ 参数化为一个由 $|Y|^2$ 个矩阵组成的列表 $(M^{y,\,y'} \in \mathbb{R}^{A\times A} : y,\ y' \in Y)$，使得对于所有 $\mathbf{a} \in A$，条件 $M(\mathsf{Mat}(\mathbf{a}))$ 等价于

$$\sum_{y,y'\in Y} M^{y,y'}_{a_y,a_{y'}} = 0. \tag{44}$$

我们现在尝试将 (44) 推广如下。

Claim A.6. 对于任意向量列表 $(\mathbf{u}_y \in \mathbb{R}^A : y \in Y)$，若存在 $c \in \mathbb{R}$，使得对于所有 $y \in Y$，$\sum_{a\in A} u_{y,\,a} = c$，则

$$\sum_{\substack{y\in Y\\ a\in A}} M^{y,y'}_{a,a} u_{y,a} + \sum_{y\neq y'\in Y} \mathbf{u}_y^T M^{y,y'} \mathbf{u}_{y'} = 0. \tag{45}$$

证明。暂且假设 $c = 1$。对于每个 $a \in A$，令 $\mathbf{e}_a \in \mathbb{R}^A$ 为满足以下条件的向量 $\mathbf{e}_{a,\,a'} = \mathbf{1}[a = a']$ 对所有 $a' \in A$ 均成立。于是，对所有 $\mathbf{a} \in A^Y$，式（44）可重新表述为

$$\sum_{y\in Y} M^{y,y}_{a_y,a_y} + \sum_{y\neq y'\in Y} \mathbf{e}_{a_y}^T M^{y,y'} \mathbf{e}_{a_{y'}} = 0.$$

对于每个 $y \in Y$，注意到 $\mathbf{u}_y = \sum_{a\in A} u_{y,\,a}\mathbf{e}_a$。现在，对于所有 $\mathbf{a} \in A^Y$，令 $\lambda_{\mathbf{a}} = \prod_{y\in Y} u_{y,\,a_y}$。于是我们可以看出

$$\begin{aligned}
0 &= \sum_{\mathbf{a}\in A^Y} \prod_{z\in Y} u_{z,a_z} \left(\sum_{y\in Y} M^{y,y}_{a_y,a_y} + \sum_{y\neq y'\in Y} \mathbf{e}_{a_y}^T M^{y,y'} \mathbf{e}_{a_{y'}} \right) \\
&= \sum_{\substack{y\in Y\\ a\in A}} M^{y,y}_{a,a} \sum_{\substack{\mathbf{a}\in A^Y\\ a_y=a}} \prod_{z\in Y} u_{z,a_z} + \sum_{\substack{y\neq y'\in Y\\ a,a'\in A}} \mathbf{e}_a^T M^{y,y'} \mathbf{e}_{a'} \sum_{\substack{\mathbf{a}\in A^Y\\ a_y=a\\ a_{y'}=a'}} \prod_{z\in Y} u_{z,a_z} \\
&= \sum_{\substack{y\in Y\\ a\in A}} M^{y,y}_{a,a} u_{y,a} \cdot \prod_{z\in Y\setminus\{y\}} \sum_{a_z\in A} u_{z,a_z} + \sum_{\substack{y\neq y'\in Y\\ a,a'\in A}} \mathbf{e}_a^T M^{y,y'} \mathbf{e}_{a'} \cdot u_{y,a} u_{y',a'} \cdot \prod_{z\in Y\setminus\{y,y'\}} \sum_{a_z\in A} u_{z,a_z} \\
&= \sum_{\substack{y\in Y\\ a\in A}} M^{y,y}_{a,a} u_{y,a} + \sum_{\substack{y\neq y'\in Y\\ a,a'\in A}} \mathbf{e}_a^T M^{y,y'} \mathbf{e}_{a'} \cdot u_{y,a} u_{y',a'} \qquad (c = 1) \\
&\sum_{\substack{y\in Y\\ a\in A}} M^{y,y'}_{a,a} u_{y,a} + \sum_{y\neq y'\in Y} \mathbf{u}_y^T M^{y,y'} \mathbf{u}_{y'},
\end{aligned}$$

如所需。现在考虑 $c \neq 1$。如果 $c \neq 0$，我们可以对 $(\mathbf{u}_y \in \mathbb{R}^A : y \in Y)$ 重新缩放，使得 $c = 1$。如果 $c = 0$，我们可以构造一个序列的序列 $\{(\mathbf{u}^{(i)}_y \in \mathbb{R}^A : y \in Y) : i \in \mathbb{N}\}$，使其趋近于

$(\mathbf{u}^y\colon\ y\in Y)$ 在 ℓ_2 范数下，但每个 $c_i\colon=\sum_{a\in A}u_y^{(i)},\ a$ 都非零。于是，我们在极限下得到 (45)。 □

对于所有 $i\in[N]$ 和 $y\in Y$，令 $\mathbf{z}^{i,y}\in\mathbb{R}^A$ 满足 $z^{i,y}_a=v_{y,a,i}$。回想一下，$\mathbf{v}_{y,a}$ 是定义 $\mathbf{V}_y\in\mathbb{S}_A^N$ 的第 a 个向量。由于对于所有 $y\in Y$，$\sum_{a\in A}\mathbf{v}_{y,a}=\mathbf{v}_0$，因此对于所有 $y\in Y$ 和 $i\in[N]$，我们有 $\sum_{a\in A}z^{i,y}_a=v_{0,i}$。假设对于所有 $i\in[N]$，$v_{0,i}\neq 0$。然后，对所有 $i\in[N]$，应用 Claim A.6，其中 $(z^{i,y}/v_{0,i}\colon\ y\in Y)$，可得

$$\begin{aligned}
0&=\sum_{i=1}^N v_{i,0}^2\left(\sum_{\substack{y\in Y\\ a\in A}}M^{y,y'}_{a,a}\frac{z^{i,y}_a}{v_{0,i}}+\sum_{y\neq y'\in Y}\frac{1}{v_{i,0}^2}(\mathbf{z}^{i,y})^TM^{y,y'}\mathbf{z}^{i,y'}\right)\\
&=\sum_{\substack{y\in Y\\ a\in A}}M^{y,y'}_{a,a}\sum_{i=1}^N v_{y,a,i}v_{0,i}+\sum_{y\neq y'\in Y}\sum_{i=1}^N(\mathbf{z}^{i,y})^TM^{y,y'}\mathbf{z}^{i,y'}\\
&=\sum_{\substack{y\in Y\\ a\in A}}M^{y,y'}_{a,a}\langle\mathbf{v}_{y,a},\mathbf{v}_0\rangle+\sum_{y\neq y'\in Y}\sum_{a,a'\in A}M^{y,y'}_{a,a'}\sum_{i=1}^N v_{y,a,i}v_{y',a',i}\\
&=\sum_{\substack{y\in Y\\ a\in A}}M^{y,y'}_{a,a}\langle\mathbf{v}_{y,a},\mathbf{v}_{y,a}\rangle+\sum_{y\neq y'\in Y}\sum_{a,a'\in A}M^{y,y'}_{a,a'}\langle\mathbf{v}_{y,a},\mathbf{v}_{y',a'}\rangle\\
&=\sum_{y,y'\in Y}\sum_{a,a'\in A}M^{y,y'}_{a,a'}\langle\mathbf{v}_{y,a},\mathbf{v}_{y',a'}\rangle\\
&=M(\mathrm{Mat}(\mathcal{V})),
\end{aligned}$$

如所需，因此 $\mathcal{V}\in K_{Y,\ A}$。 □

引理的另一种证明 *6.17 (1)*。我们将使用 [CŽ23a]证明的一个关于超矩阵投影的结果。对于 $n,\ q\in\mathbb{N}$，考虑集合 $\mathcal{M}=\{M^{y,y'}\colon\ 1\le y<y'\le q\}$ 由 $n\times n$ 个具有整数项的矩阵组成。我们称 $\mathcal{M}$ 为一个可实现的 系统，如果 $\mathcal{M}$ 中的矩阵是某个唯一超矩阵的二维投影；形式化地说，若存在一个超矩阵 $\Lambda\in\mathbb{Z}^{\overbrace{n\times n\times\cdots\times n}^{q}}$ 使得

$$M^{y,y'}_{a,b}=\sum_{\substack{\mathbf{z}\in[n]^q\\ z_y=a,\,z_{y'}=b}}\Lambda_{\mathbf{z}}$$

对于每个 $M^{y,\ y'}\in\mathcal{M}$ 以及每个 $a,\ b\in[n]$。如果 $\mathcal{M}$ 是一个现实的 系统，意味着其矩阵在以下意义下局部兼容：对于每个 $1\le y_1<y_2\le q$、每个 $1\le w_1<w_2\le q$ 以及每个 $r,\ s\in[2]$ 使得 $y_r=w_s$，都有

$$(M^{y_1,y_2})^{\circ r}\mathbf{1}=(M^{w_1,w_2})^{\circ s}\mathbf{1},$$

其中我们 使用记号 $M^{\circ 1}\coloneqq M$ 和 $M^{\circ 2}\coloneqq M^\top$。我们将使用以下结果。

定理 A.7（[CŽ23a]）。一个系统 $\mathcal{M}$ 是现实的当且仅当它是可实现的。[19]

现在取某个全局配置 $\mathcal{V} \in (\mathbb{S}_A^N)^Y$，并令 $\mathrm{Mat}(\mathcal{V}) \in \mathbb{R}^{(Y\times A)^2}$ 为相应的格拉姆矩阵。首先假设 $\mathrm{Mat}(\mathcal{V})$ 的项均为有理数，并令 N 为公分母。记 $M^{y,y'}$ 为 $N\cdot\mathrm{Mat}(\mathcal{V})$ 的第 (y,y') 个块（大小为 $A\times A$），并注意到该量

$$(M^{y,y'}\mathbf{1})_a = N\sum_{b\in A}\langle \mathbf{v}_{y,a}, \mathbf{v}_{y',b}\rangle = N\langle \mathbf{v}_{y,a}, \mathbf{v}_0\rangle$$

对每个 $a\in A$ 都独立于 y'。因此，系统 $\mathcal{M} = \{M^{y,y'} : 1\le y < y' \le |Y|\}$ 是现实的。根据定理 A.7，可知 $\mathcal{M}$ 是可实现的。设 Λ 为其实现超矩阵。我们断言 $\frac{1}{N}\Lambda$ 见证了 $\mathrm{Mat}(\mathcal{V})$ 位于 $K_{Y,A}$ 中。即，我们断言 $\mathrm{Mat}(\mathcal{V}) = \sum_{\mathbf{z}\in A^Y}\frac{1}{N}\Lambda_{\mathbf{z}}\,\mathrm{Mat}(\mathbf{z})$。事实上，对每个 $1\le y<y'\le|Y|$ 以及每个 a，$b\in A$，我们有

$$N\cdot\mathrm{Mat}(\mathcal{V})_{(y,a),(y',b)} = M^{y,y'}_{a,b} = \sum_{\substack{\mathbf{z}\in A^{|Y|}\\ z_y=a,\, z_{y'}=b}}\Lambda_{\mathbf{z}} = \sum_{\mathbf{z}\in A^{|Y|}}\Lambda_{\mathbf{z}}\,\mathrm{Mat}(\mathbf{z})_{(y,a),(y',b)} = \left(\sum_{\mathbf{z}\in A^{|Y|}}\Lambda_{\mathbf{z}}\,\mathrm{Mat}(\mathbf{z})\right)_{(y,a),(y',b)}$$

如所需。由于 $M^{y',\,y} = (M^{y,\,y'})^\top$，并且由于任意全局配置的格拉姆矩阵的对角块完全由其非对角块决定，因此该结果对每个 $y,\ y'\in Y$ 成立，从而证明了该断言。最后，$(\mathbb{S}_A^N)^Y$ 中全局配置的格拉姆矩阵的有理数子集是稠密的，因此同一结果对非有理的 $\mathrm{Mat}(\mathcal{V})$ 也必然成立，从而完成证明。

□

[19] 这一结果由 [CŽ23a] 在投影维度任意、且超矩阵不一定是立方的情形下证明（也就是说，其各模的长度可能不同）。这里我们只需要上述受限情形。