arXiv:2304.06664v1 [cs.DS] 13 Apr 2023

约束满足问题的流式近似算法

A DISSERTATION PRESENTED BY NOAH SINGER
TO THE DEPARTMENT OF COMPUTER SCIENCE
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF BACHELOR OF ARTS
IN THE SUBJECTS OF
COMPUTER SCIENCE AND MATHEMATICS
HARVARD UNIVERSITY CAMBRIDGE,
MASSACHUSETTS MARCH 2022

论文导师：Madhu Sudan 教授

Noah Singer

关于约束满足问题的流式近似算法

Abstract

在这篇论文中，我们探讨用于流式计算算法的近似约束满足问题（*CSPs*）。大致设置如下：一台计算机的内存空间有限，接收关于一组变量的局部约束组成的长“数据流”，并尝试估计其中有多少个约束可以同时满足。过去十年中，该领域已经出现了许多研究成果，而这篇论文既包含综述性材料，也包含原创贡献。贯穿全文，我们强调其与更广泛的 CSP 理论、可近似性和流式模型之间的联系，并突出介绍一些有趣的开放问题。

论文的第一部分为综述性内容：我们介绍了以往研究的若干方面，这些研究完全刻画了特定约束满足问题（如最大割和最大有向割）在 $\sqrt{n}$ 空间流式算法（针对 n 变量实例）下的可近似性;¯同时，还刻画了所有约束满足问题在 $\sqrt{n}$ 空间下的可近似性（仅限于“可组合”（即草图化）算法这一特殊情形），以及特定子类的约束满足问题在线性空间 流式算法下的可近似性。

论文的第二部分介绍了我们自己的两项合作研究。首先，我们介绍与 Madhu Sudan 和 Santhoshini Velusamy 合作的一项研究，在其中我们证明，所有排序约束满足问题（*OCSP*）都具有线性空间流式近似抗性；这类“类似约束满足问题”的问题是在排列集合上进行最大化。以往研究考察了最大无环子图 问题（MAS），这是典型的排序约束满足问题；即使对于 MAS，我们也改进了不可近似因子和空间界。

接下来，我们介绍与 Joanna Boyland、Michael Hwang、Tarun Prasad 和 Santhoshini Velusamy 的合作研究，探讨带取反的布尔约束满足问题的 $\sqrt{n}$-空间流式近似性。具体而言，我们给出了若干类约束满足问题的显式 $\sqrt{n}$-空间草图化近似比，包括 Max-kAND；为阈值 谓词开发了更简单的最优草图近似算法；并证明以往的

论文指导教授：Madhu Sudan 教授 Noah Singer

流式下界并不完整，因为它们未能刻画 Max-3AND 的 $\sqrt{n}$-空间流式近似性。

目录

1 Introduction 1
1.1 先前工作的总结.41.2 贡献与概要.51.3 重要主题与动机.7

2 Preliminaries 14
2.1 约束满足问题.152.2 流式计算与草图算法.172.3 超图.182.4 傅里叶分析.192.5 集中不等式.212.6 优势与全变差距离.212.7 下界基础.22

I 已有结果 26

3 Max-Cut is approximation-resistant 27
3.1 布尔划分检测问题.283.2 BPD 很难：证明 定理 3.3 .333.3 混合论证：证明引理 3.5 .383.4 讨论.40

4 Max-DiCut is mildly approximable 43
4.1 基于偏差的算法 Max-2AND .444.2 证明 最大有向割 .484.3 讨论.52

5 Prior results: General CSPs 56
5.1 $\sqrt{n}$-空间算法与草图二分.575.2 线性空间流处理的下界.66

II 贡献 70

6 Ordering constraint satisfaction problems 71
6.1 OCSP：定义、动机、历史.726.2 MAS 的证明概要.746.3 所有 OCSP 的线性空间近似抗性：证明 定理 6.1 . 786.4 粗化分析：证明 引理 6.7 .80

7 Symmetric Boolean predicates 84
7.1 结果.857.2 对称情形的设置.897.3 技术.927.4 λ_S 和 $\gamma_{S,\ k}$的显式公式.967.5 草图近似比分析.987.6 阈值谓词的简单草图算法.1087.7 [CGSV21a]不完整：Max-3AND 的流式下界 Max-3AND? 112

8 Conclusions and future directions 114
8.1 唯一博弈困难性与流式计算困难性.1148.2 随机排序与线性空间流处理.1168.3 流式计算（与草图化）下界.1178.4 多遍下界.118

Glossary 120

References 123

To my parents and grandparents.

编写程序绘制地图，显示数据交换频率：每一千兆字节对应大屏幕上的一个像素。曼哈顿和亚特兰大亮成一片纯白。接着它们开始闪烁，流量之大，仿佛要让你的模拟系统不堪重负。你的地图就要爆发了。冷静下来。调高比例尺。每个像素代表一百万兆字节。每秒一亿兆字节时，你开始看清曼哈顿中城的某些街区，以及环绕亚特兰大旧城区的百年工业园区的轮廓。。。

威廉·吉布森，《神经漫游者》

此外，还破译出了其中的内容：组合分析学的概念，并通过无限重复的排列示例加以说明……他注意到，所有的书无论多么不同，都由相同的元素构成：空格、句点、逗号，以及二十二个字母。

豪尔赫·路易斯·博尔赫斯，《巴别图书馆》

致谢

我由衷感谢 Madhu Sudan，在我于哈佛大学求学期间，他一直是极其支持我的研究导师，也是全方位的良师益友。我很幸运有机会与他共事并向他学习；他对我似乎永无止境的 Slack 消息总是耐心回复、慷慨相助，还源源不断地为我提供建议、反馈和见解，这至今仍让我惊叹不已。

Santhoshini Velusamy 是本论文中两项合作研究的出色合作者 [SSV21；BHP+22]。她建议研究MAS问题的流式算法。这是她本科生研究实习期间留下的一个有趣且尚未解决的问题（参见 [GVV17]），由此开启了我对流式约束满足问题的研究。将近两年后，这项研究已发展成本论文。（第 6 章介绍了与 Madhu [SSV21] 的合作研究，其中解决了她最初提出的问题。）也感谢我合作研究中的其他合著者 [BHP+22]（第 7 章）：Joanna Boyland、Tarun Prasad 和 Michael Hwang；感谢 Sumegha Garg、Chi-Ning Chou、Sasha Golovnev、Ameya Velingker 和 Raghuvansh Saxena 提供宝贵见解并参与讨论；还要感谢哈佛学院研究项目在 2021年秋季为我研究 [BHP+22]提供支持。

感谢 Salil Vadhan 担任我的第二位论文审阅人；感谢 Boaz Barak 多年来给予我的建议和鼓励——从他热情友善地发来一系列关于哈佛大学计算机科学的邮件开始，这些邮件在很大程度上坚定了我前往哈佛大学就读的决定；也感谢 Eric Allender 在 2021年夏季我参加罗格斯大学的 DIMACS本科生研究体验项目期间，给予我出色的指导。此外，我也十分感激自己曾担任 Madhu、Boaz、Adam Hesterberg、James Mickens 和 Michael Mitzenmacher 所授课程的本科教学助理（TF），这段经历对我影响深远。

最后，我要感谢我的父母 Mindy Weinstein 和 Joel Singer、我的兄弟 Ethan、其他家人，以及许多朋友，包括 Braxton Marion、Clara Li、James Roney、Joshua Doolan、Jyotsna Rao、Nari Johnson、Shuvom Sadhuka 和 Sahana Srinivasan，感谢他们在我大学期间一路走向科研和研究生院的旅程中给予我无比的支持。

1 引言

This thesis sits at the intersection 计算机科学的两个主要分支：组合优化 和 大数据。前者是一个统称，指目标是在有限且具有一定“结构”的解集合中找出“最佳”解的计算问题，包括路由、装箱、调度和资源分配等任务。后者涵盖了类似广泛的计算场景，涉及“海量”输入数据，因此需要“极高效”地使用资源（以内存、时间、能耗等衡量），进而催生了在线、分布式、并行和次线性时间算法等。

在本论文中，更具体地说，我们考虑一类特定的组合优化问题，称为约束满足问题（*CSP*），以及一类用于大数据的特定算法，称为流式算法。大致而言，CSP 的目标是找到一个满足尽可能多“局部约束”的“全局解”。更准确地说，固定一个有限集合 Σ，称为字母表。一个 k元谓词 是一个函数 $\Sigma^k \to \{0,1\}$。由一组 $\mathcal{F}$个 k元谓词定义的 CSP 记为 Max-CSP($\mathcal{F}$)。Max-CSP($\mathcal{F}$) 的一个实例 由 n 变量定义，每个变量都可以赋值 为从字母表Σ中取出的一个值；此外还有 m 约束，每个约束都将 $\mathcal{F}$ 中的一个谓词应用于 k 个变量的某个子集。Max-CSP($\mathcal{F}$) 问题的目标是找到一个将变量赋值为各个值的赋值。

尽可能满足更多约束。（正式定义见下文 §2.1。）例如，考虑最大割问题（Max-Cut），可以说是最简单的 CSP。它定义在布尔字母表 $\Sigma = \{0,1\}$ 上，由二元谓词 Cut$(a,b) = a \oplus b$ 给出（即，Cut$(a,b) = 1$ 当且仅当 $a \neq b$）。因此，在一个最大割实例中，我们有 n 个变量，可赋值为两个值（0 或 1）之一，以及 m 个约束，每个约束都表示“变量 i 和变量 j 应取不同的值”。最大割在电路设计和统计物理等领域有实际应用 [BGJR88]；一个简单的应用示例是，在校外活动中根据一份彼此不和的儿童名单，将孩子分成两组，以尽量减少冲突。CSP 框架还涵盖许多其他在理论和实践中都得到广泛研究的问题，例如 Max-kSAT 和 Max-qCut。

现在，假设我们要解决如下约束满足问题：最大割 ——也就是说，找到一个较好的赋值，或者至少判断是否存在较好的赋值——针对的是以下意义上“规模很大”的实例：约束按某种序列生成，数量多到无法存储。例如，我们可以设想这样一种场景：许多客户端向服务器传送大量约束，而服务器试图尽可能多地满足这些约束。流式算法 的理论模型旨在刻画这些挑战：算法接收一系列输入，内存空间有限，并且只能按顺序对输入进行一次遍历。*† （§2.2 给出了该模型的形式化定义。）流式算法由 Alon、Matias 和 Szegedy 提出， [AMS99], 它们对网络流量和科学数据的实时分析等实际场景进行了建模。有关流式算法的更多内容，请参阅综述 [Mut05；Cha20]。

具体而言，一个“流式约束满足问题算法”会接收输入实例 Ψ 的约束，并负责 估计 约束的 值 ，即 Ψ，记作val_Ψ，它是通过对变量进行任意赋值所能满足的约束的最大比例。‡ 下一页的 图 1.1以图示方式呈现了这一概念。准确地说，我们采用以下关于 CSP 值“估计”的标准概念：对于 $\alpha \in [0,1]$，我们称 $\widetilde{v}$ α-近似 val_Ψ ，如果

*也就是说，该算法无法对输入进行随机访问——它只能依次看到第一个输入 C_1，然后是 C_2，等等，无法访问序列中位于当前位置之前或之后的输入 C_j。当然，它可以选择在看到输入 C_j 后存储它，但可用存储空间非常有限。

†这种特定的流式计算模型可以通过多种方式放宽，例如允许对数据流进行多遍扫描，或随机排列数据流中的内容。参见 §1.3.3。

‡我们通常并不要求算法实际输出一个良好的赋值，因为即使只是写下这样的赋值，也可能占用过多空间。

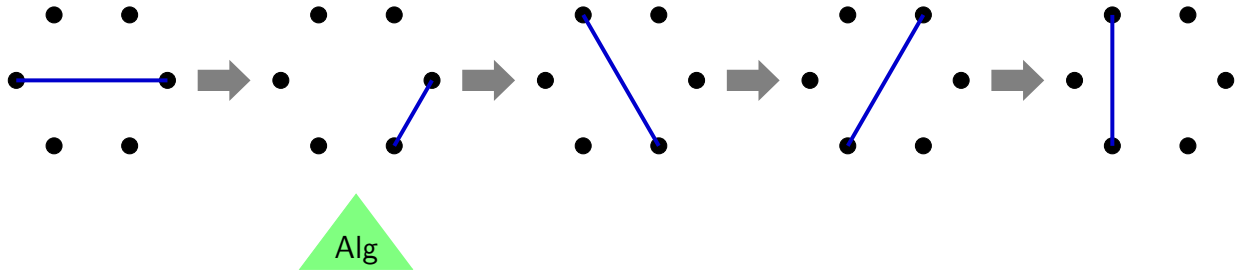


图 1.1: 在 $n = 6$ 个变量（“顶点”）上最大割实例的示意图，其中包含 $m = 5$ 个约束（“边”）。流式算法 Alg 对约束列表进行一次线性遍历，并尝试判断是否能够找到一种顶点划分，使大多数边都跨越该划分。

$\alpha \mathrm{val}_\Psi \leq \widetilde{v} \leq \mathrm{val}_\Psi$。换句话说，$\widetilde{v}$ 是 val_Ψ的一个低估值，但低估幅度不会超过因子 α。

每个最大割实例的值都至少为 1 2；事实上，随机赋值在期望意义下满足一半的约束。因此，估计值 1 2 始终是 val_Ψ 的一个 1 2-近似。反过来，在许多变量上具有许多均匀随机约束的最大割实例，其值可以任意接近 1 2（见 §3.1）。因此，1 2 是所有最大割实例 Ψ 的 val_Ψ 下确界，也是最优的“平凡”-（即与输入无关）估计值。因此，最大割的非平凡近似是某个 $\frac{1}{2} + \epsilon$-近似，其中 $\epsilon > 0$。对于其他约束满足问题，我们也类似地将一种 α-近似称为非平凡近似，条件是 α 超过所有实例的值 [CGSV21b] 的下确界。如果某个约束满足问题无法获得非平凡近似，则称其具有近似抗性。

现在的核心问题是：

对于哪些谓词族、哪些期望的近似比 α，以及哪些类别的流式算法，我们能够为最大约束满足问题$(\mathcal{F})$证明正面（即算法方面）或负面（即困难性方面）的结果？

值得注意的是，直到 2015 年，尽管约束满足问题和流式算法这两个领域各自都已得到广泛研究，却还没有研究探索二者的交集。但此后，基于 2011 年 Bertorino 次线性算法研讨会上提出的开放问题 [IMNO11，问题 10]，推动了针对约束满足问题的流式算法研究蓬勃发展 [KK15；KKS15；GVV17；KKSV17；KK19；CGV20；CGSV21a；CGSV21b；SSV21；BHP+22；CGS+22] 这项研究既解决了不少最初提出的问题，也引出了许多新的、有趣的问题。

1.1 Summary of prior work

Kogan 和 Krauthgamer [KK15] 以及 Kapralov、Khanna 和 Sudan [KKS15] 研究了最大割的流式近似；后者证明，对于任意 $\epsilon > 0$，在含有 n 个变量的实例上，对最大割进行流式 $(\frac{1}{2} + \epsilon)$ 近似需要 $\Omega(\sqrt{n})$ 空间（见下文定理 3.1）。[§] 他们的结果实际上适用于比我们迄今描述的模型更强的模型，在该模型中，实例 Ψ的约束是“随机排序”的。Guruswami、Vel-ingker 和 Velusamy [GVV17] 给出了一个针对最大有向割（Max-DiCut）问题的 $(\frac{2}{5} - \epsilon)$ 近似流式算法，所需空间为 $O(\log n)$；他们还通过从最大割归约，证明了 $(\frac{1}{2} + \epsilon)$ 近似需要 $\Omega(\sqrt{n})$ 空间。Chou、Golovnev 和 Velusamy [CGV20] 弥合了这一差距：他们证明，对于任意 $\epsilon > 0$，最大有向割可以在 $O(\log n)$ 空间内获得 $(\frac{4}{9} - \epsilon)$ 近似，但 $(\frac{4}{9} + \epsilon)$ 近似需要 $\Omega(\sqrt{n})$ 空间（见下文定理 4.1）。[CGV20] 还分析了其他若干问题的可近似性，包括 Max-kSAT。

在 [CGV20], 针对每个 Max-CSP($\mathcal{F}$) 问题的结果基础上，Chou、Golovnev、Sudan 和 Velusamy [CGSV21b] 证明了草图算法的二分定理。草图算法是一类“可组合”的流式算法（定义见 §2.2）。他们的定理指出，对于每个谓词族 $\mathcal{F}$，都存在一个草图近似性阈值$\alpha(\mathcal{F}) \in [0,1]$，使得对每个 $\epsilon > 0$，Max-CSP($\mathcal{F}$) 都可以在 $O(\text{polylog } n)$ 空间内达到 $(\alpha(\mathcal{F}) - \epsilon)$-近似，而要达到 $(\alpha(\mathcal{F}) + \epsilon)$-近似则需要 $\Omega(\sqrt{n})$ 空间。在更早的一篇论文中，[CGSV21a], 在所谓的“带否定的布尔约束满足问题”这一特殊情形下证明了相同的结果：对于一个布尔谓词 $f : \{0,1\}^k \to \{0,1\}$，考虑由对 f 的输入取反子集所对应的 2^k 个谓词组成的谓词族$\mathcal{F}_{\neg f}$，这些谓词定义了一个约束满足问题 Max-BCSP(f) def $=$Max-CSP($\mathcal{F}_{\neg f}$)。[CGSV21a] 为 Max-BCSP(f) 给出了草图二分定理，从而得到草图近似性阈值 $\alpha(f)$ def $=$ $\alpha(\mathcal{F}_{\neg f})$。然而，[CGSV21a; CGSV21b] 都没有提供计算这些阈值的显式方法；事实上，事先甚至无法确定它们是否存在闭式表达式。另一方面，[CGSV21a; CGSV21b]还包含许多其他结果，尤其是关于二分定理中的下界在何种条件下可推广至流式算法的结果。[CGSV21a] 结果的正式描述见下文 §5.1。

[§]请注意，$\Omega(\cdot)$记号中的隐含常数可能取决于所需的近似因子常数，即取决于 ϵ。为简化表述，我们将其称为“$\sqrt{n}$-空间不可近似性结果”，但在定理陈述中会谨慎地明确量词。

另一项研究工作 [KKSV17；KK19；CGS+22]将上述一些不可近似性结果推广到线性空间算法的情形。特别地，Kapralov 和 Krachun [KK19] 证明，对于 $\frac{1}{2}+\epsilon$-近似，流式计算 最大割 需要 $\Omega(n)$ 空间；Chou、Golovnev、Sudan、Velingker 和 Velusamy [CGS+22]则将这一紧确的不可近似性推广到了某些其他“线性”约束满足问题（见下文的 推论 5.14，位于 §5.2）。

1.2 Contributions and outline

第2章给出了约束满足问题和流式算法的形式化定义，以及一些其他的预备材料。

Expositions of prior work. 在本文第一部分中，我们介绍了若干关于约束满足问题流式算法的奠基性研究。本文旨在让更广泛的理论研究读者能够理解这些结果，并借鉴后续论文提出的新视角；在某些情况下，这些新视角大幅简化了早期的构造。

第3章首次对以下结果作了完整且自成一体的阐述：由 [KKS15],所蕴含的结论，即要对最大割进行非平凡近似，需要 $\Omega(\sqrt{n})$ 的流式空间。请注意， [KKS15]还针对约束的“随机排序”数据流给出了这一结论的更强版本；证明这一更强结论还需要一些额外步骤，而这些步骤与最大割可近似性的根本问题略有关系偏离。我们的证明整合并简化了 [GKK+08、KKS15、CGSV21a]中的部分内容。随后，我们将讨论最大割的困难性在 [KKS15、KK19]中得到加强的多种方式。

在第 4 章中，我们介绍 [CGV20]的证明，说明最大有向割的流式近似性阈值（对于对数 n 与 $\sqrt{n}$ 空间）为 $4/9$。我们的阐述与 [CGV20]的原文有两处重要不同。首先，我们描述了一种大幅简化的算法，该算法基于我们与 [BHP+22]的合作研究所得的观察（我们将在第 7 章进一步探讨）。其次，我们强调了（$\frac{4}{9}-\epsilon$）近似算法与（$\frac{4}{9}+\epsilon$）近似的困难性证明之间的结构相似性，即二者都使用了所谓的模板分布；这后来成为所有由 [CGSV21a；CGSV21b]提出的约束满足问题二分定理。

我们将在 [CGS+22]线性空间下界以及第 5 章中讨论这些二分定理。我们会对这些研究进行概述，其技术性不如我们在

前两章中的讨论。[¶] 不过，对于我们在第二部分中开展自己的研究所需的结果，我们会谨慎地加以表述。

Ordering CSPs. 在 第 6 章 （该章开始于 第二部分）中，我们介绍与 Sudan 和 Velusamy 合作完成的主要结果 [SSV21], ，该成果发表于 APPROX'21。此结果（下文的 定理 6.1 ）指出，对于一类称为 排序约束满足问题（*OCSPs*）的"类似 CSP"问题，所有非平凡的流式近似都需要 $\Omega(n)$ 空间。回顾一下，在约束满足问题中，解空间是从变量到字母表值的赋值集合；而在 OCSP 中，解空间则是变量上的排列集合（详见下文 §6.1），因此，OCSP 是调度问题的良好模型。

我们的结果在 [SSV21] 中是"三重最优"的：它排除了所有 非平凡近似，适用于所有 OCSP，且 $\Omega(n$ 空间界是紧的（在多对数因子范围内，见下文的 备注 3.19）。先前的工作 [GVV17；GT19] 研究了最大无环子图（*MAS*）问题——一种由谓词"变量 i 排在变量 j之前"定义的简单 OCSP——并证明某些近似算法需要 $\Omega(\sqrt{n})$ 空间；因此，我们在 [SSV21]中的结果在这三个"参数"上都有改进。

此外，我们针对有序约束满足问题的不可近似性证明，依赖于 [CGS+22]中关于（非排序）约束满足问题的线性空间不可近似性结果；我们将在§5.2节提前介绍这些结果。在此背景下，我们在第 6 章 给出了一个比最初发表于 [SSV21]中的证明更模块化的版本。

Symmetric Boolean CSPs. 在第 7 章中，我们介绍与 Boyland、Hwang、Prasad 和 Velusamy 的合作成果 [BHP+22] ，该成果研究了布尔字母表上的特定类型约束满足问题的流式算法 $\{0,1\}$，具体而言，是具有对称谓词的约束满足问题（即谓词仅取决于输入中 1 的数量，也称为汉明重量）。这些约束满足问题是一个有趣的"透镜"，我们借此考察 Chou 等人的工作 [CGSV21a；CGSV21b]留下的若干未解问题。

本研究的主要目标是发现并利用[CGSV21a] 二分定理的"结构性"性质，从而给出草图化的显式表达式

¶在第 3 章和第 4 章中，为了聚焦于更重要的定量方面，我们有时会在证明中省略集中界；这些地方都已仔细标注。

若干类谓词 f 的可近似性阈值 $\alpha(f)$。例如，令$\alpha'_k \stackrel{\text{def}}{=} 2^{-(k-1)}(1-k^{-2})^{(k-1)/2}$，我们证明：对于奇数 k，$\alpha(k\text{AND}) = \alpha'_k$；对于偶数 k，$\alpha(k\text{AND}) = 2\alpha'_{k+1}$（见下文定理 7.2）；对于奇数 k，$\alpha(\text{Th}_k^{k-1}) = \frac{k}{2}\alpha'_{k-1}$（见下文定理 7.4）。我们还确定了另外十五个特定函数的阈值（见下文 §7.5.4）。

我们还基于对对称布尔谓词的研究给出另外两项结果。首先，对于阈值谓词（当且仅当其输入的汉明重量至少为t某个常数 t时取值为 1；又称单调对称谓词），我们设计了大幅简化的草图算法，并且同样达到了 [CGSV21a] 给出的最优近似阈值（见下文定理 7.7）。其次，我们证明，[CGSV21a] 中用于证明流式计算困难性结果的判据并不“完备”，也就是说，它们无法为Max-3AND确立精确的可近似性阈值。

第 7 章中的大多数证明和讨论第 7 章均以少量修改的形式摘录自我们的论文 [BHP+22]。

Open questions. 最后，在 第 8 章中，我们汇总了一些有趣的开放问题，以及进一步研究约束满足问题流式算法的方向。其中一些问题已在先前的工作中提出，另一些则是在我们与合作者开展研究时产生的，并首次在此提出。

1.3 Important themes and motivations

所有这些关于 CSP 近似的流式算法的研究，在理论上意味着什么？与流式算法不同，关于经典算法的 CSP 可近似性已经形成了一套丰富的理论，其性能要求仅为运行时间是 poly(n)；例如，参见综述 [Tre04]。然而，这一理论依赖于诸如$\mathbf{P} \neq \mathbf{NP}$这样的复杂性理论猜想。相比之下，正如我们将要看到的，本论文讨论的流式约束满足问题的困难性结果都是无条件的，也就是说，它们不依赖于任何尚未得到证明的猜想！

从某种意义上说，我们能够得到无条件的困难性结果，与其说是流式计算模型的“特性”，不如说是一个“缺陷”。事实上，经典约束满足问题领域中几乎所有有用的算法似乎都无法实现为流式算法；因此，可以证明针对剩余算法的困难性结果，应该说并不令人意外。

算法（不过，当我们反而成功开发出流式算法时，这确实令人兴奋！）。

在本节中，我们将论证，流式CSP理论的价值并不止于其技术性论述本身。具体而言，我们将重点介绍三个主题，它们似乎与CSP或流式模型的更广泛领域相关，并且有助于读者在阅读论文余下部分时牢记于心。对于不熟悉第2章所述预备知识的读者，可以放心跳过本节（也希望之后能再回来阅读！）。

1.3.1 Parallels to classical hardness-of-approximation

许多关于CSP以及其他组合优化问题的早期经典近似困难性结果，都是借助概率可检验证明（PCP） [AS98; ALM+98]的工具证明的。事实上，借助PCP技术，许多问题的经典可近似性已得到精确刻画，例如CSP中的最大 3SAT [H˚as01] as，以及集合覆盖 [Fei98], 、色数 [FK98], 和最大团[H˚as99]等非CSP问题。基于PCP的困难性结果通常只假设 P $\neq$NP 猜想。后来，Khot [Kho02] 提出了一种新的复杂性理论假设（强于 P $\neq$NP），称为唯一博弈猜想（UGC），旨在进一步理解组合优化问题的经典可近似性。‖ 如今已知，UGC能够推出CSP的一些紧确可近似性结果，包括最大割 [KKMO07],、最大2可满足性 [Aus07], 以及 Max-kAND（达到常数因子） [ST09; CMM09] ；对于其他组合优化问题也能推出此类结果，包括排序约束满足问题 [GHM+11]、值为 $\frac{1}{2}+\epsilon$ [KO09], 的实例上的最大割，以及顶点覆盖 [KR08]。

考虑一位程序员希望近似求解组合优化问题时面临的两个“世界”：World U 中，UGC 为真，程序员可以使用多项式时间算法；World S 中，程序员只能使用多对数空间流式算法。我们对这两个世界中的可近似性所知的情况，存在一些令人惊讶的相似之处：

- 定理　　等人 [CGSV21b] 的 $\sqrt{n}$空间草图化二分定理,¯适用于世界

‖UGC 大致断言，对于 Max-UG 这一约束满足问题，其困难性是最优的。Max-UG 允许使用二元谓词，且这些谓词具有如下性质：固定一个变量后，另一个变量便被唯一确定；其字母表可以任意大 Σ。换言之，Max-UG $=$ Max-CSP($\{f_\pi : \pi$ 是 $\Sigma\}$上的一个双射)，其中 $f_\pi : \Sigma^2 \to \{0,1\}$ 定义为$f_\pi(a, b) = 1$ 当且仅当 $b = \pi(a)$。

S，发表于§5.1，与 Raghavendra 在 [Rag08]中提出的二分定理类似。前者表明，在世界 S 中，基于偏差的线性草图算法 `遵循 [GVV17] 的思路，对每个约束满足问题都是最优的；后者则表明，在 World U 中，最优算法是半定规划（*SDP*）“先松弛再舍入”算法 `遵循[GW95]针对最大割（参见 [MM17] 的最新综述）。**

• 在世界S中， [CGSV21b] 还表明，任何满足一种称为“支撑单变量独立性”的自然性质的约束满足问题，都是在$\sqrt{n}$ 空间下具有流式近似抗性的（见下文的例 5.6 ）。Austrin 和 Mossel [AM09]证明了一个类似的世界 U 中的结果：满足一种称为“支撑二变量独立性”的高阶条件的约束满足问题具有近似抗性。

• 对于世界 S 中的排序约束满足问题，我们与他人合作得出的线性空间近似抗性结果 [SSV21], 见第 6 章，与 Guruswami、H˚astad、Manokaran、Raghavendra 和 Charikar [GHM+11] 的一条定理类似。该定理指出，世界 U 中的有序约束满足问题具有近似抗性。正如我们将在第 6 章看到的，这两项结果的证明方法有着显著的相似之处——两者都依赖于从有序约束满足问题的“粗粒度”变体的不可近似性结果进行归约。

• Max-kAND 是最“可近似”的 Max-BCSP(f) 问题（见下文备注 7.9），直观地说，这是因为它的约束最“有信息量”——每个约束都能准确告知我们其变量需要赋什么值。因此，我们很幸运能够在两个世界中都解决其可近似性问题：在世界 S 中，我们与 [BHP+22] 的合作成果（见第 7 章）表明，Max-kAND 问题在 $\sqrt{n}$-空间下的草图化可近似性为 $(2-o(1))2^{-k}$（下文定理 7.2）。在世界 U 中，Max-kAND 是 $\Theta(k2^{-k})$-可近似的 [ST09；CMM09]。†† 此外，就第一条要点中讨论的算法方面而言，对于 Max-k AND，我们来自 [BHP+22] 的最优草图算法与来自[Has05；CMM09] 的最优半定规划舍入算法具有惊人相似的结构：找到一个好的“猜测”赋值——

**约束满足问题还有许多其他“经典二分定理”，具体涉及精确计算（即，判定$\mathsf{val}_\Psi = 1$是否） [Sch78；FV98；Bul17；Zhu20] 以及所谓的粗略近似（见 [KSTW01] 和著作 [CKS01]）。

††事实上， [ST09]甚至证明了 $O(k2^{-k})$-近似是 **NP**-困难的，不过在假设唯一博弈猜想成立的情况下，他们的结果更强。

ment $\mathbf{x} \in \mathbb{Z}_2^n$ 然后以某个小常数概率，独立地随机扰动其中的每一位。然而，我们的算法选择 $\mathbf{x}$ 完全基于组合方法——依据某个变量以正极性还是负极性出现得更频繁——而 [Has05；CMM09] 算法则通过对半定规划进行随机舍入来生成它。

这些相似之处或许表明，World U 的困难性结果并非空穴来风，至少对于弱算法类别而言是如此。

1.3.2 Random instances of CSPs (and average-case hardness)

在经典情形中，人们也对用于 CSP“随机*3SAT* 实例”的算法 [Fei02] 颇感兴趣；一个典型例子是，通过均匀分布地采样变量和谓词来采样约束。Feige 著名的随机最大 3SAT假设 $\frac{m}{n}$ 指出，对于任意常数约束与变量之比，经典算法都无法“反驳”随机实例；粗略地说，我们将“反驳”定义为“将实例与完全可满足的实例区分开来”。Feige 的猜想及相关猜想在近似困难性、密码学和学习领域有许多应用（综述见 [KMOW17，§1。2]）。另一方面，当约束与变量之比更大时，针对各种 CSP，算法方面已取得显著进展 [BKPS98；FGK05；CGL07；FO07；AOW15；BM16；RRS17；GKM22]。

相比之下，在流式算法的设置中，我们所有的下界都来自随机实例！具体来说，我们将展示，流式算法无法区分“**否**”实例（这些实例完全随机采样得到）与“**是**”实例（这些实例是在随机“植入”赋值上具有较高值的条件下随机采样得到）。我们将在 最大割 的简单情形中探讨这一范式，详见第3章。

经典情形中的算法结果，以及流式设置中的困难性结果，都依赖于对随机图进行细致的组合分析。同样，流式计算中的困难性也可能为例如 Feige 随机 3SAT 假设的正确性提供启发式证据，至少对于较弱的算法类别而言。

1.3.3 Subtleties of streaming models

二元约束满足问题的一个实例可以视为一张（有向）图，其中的边标有谓词；更广义地说，k元约束满足问题是所谓的“k均匀超图”，

或 k-超图，简而言之，其中谓词为超边标记。因此，我们所讨论的约束满足问题的流式近似算法属于“图流”算法的范畴；这类问题的输入是一张（超）图中带标签的（超）边所组成的数据流（参见例如综述 [McG14]）。

在“**小空间、单遍**”这一基本图流模型上，有许多有趣的变体。本小节将重点讨论两种弱化该模型的方式，即随机排序输入或允许多遍，以及一种强化该模型的方式，即要求算法具有可组合性 （从而得到所谓的“草图算法”）。对于这些变体，我们将列举已知的各种近似组合优化问题的分离结果。

Input ordering. 当我们要求流式算法仅在输入流为随机排序时（以高概率）取得成功，而不是在所有输入排序下都取得成功时，会发生什么？直观来看，这可能会减轻算法的负担，因为算法从长远来看对其输入具有很强的“遗忘性”，一小段连续的劣质输入就可能导致灾难性的失败；而在随机排序的数据流中，这类序列出现的可能性可能较低。这一现象已在“大数据”算法相关文献中得到广泛研究；关于在线算法计算列表中最大元素这一简单情形的启发性阐述，请参见§该综述的第 1 节 [GS21] 。在更直接的图流式计算场景中，Peng 和 Sohler [PS18] 证明了图问题中“随机顺序”设置与“对抗性顺序”设置之间存在可证明的分离，这些问题包括近似计算连通分量数量以及近似计算最小生成树权重。关于 CSP 流式算法场景下的相关讨论，请参见第 3.4.2 节和第 8.2 节。

Sketching vs. streaming. 草图化算法是一类特殊的流式算法，大致具有以下“可组合性”性质：我们可以选择将输入流拆分成若干部分，而算法必须能够“支持”在每个部分上独立运行，然后合并结果；形式化定义见§2.2 Kapralov、Kallaugher 和 Price [KKP18;KP20]证明了，对于图中的近似三角形计数问题，草图化算法与流式算法之间存在分离。

Multiple passes. 最后，我们可以考虑允许流式算法对输入数据进行多遍扫描。即使只进行两遍，要证明流式算法的下界通常也非常困难，除非是在高度结构化的情境中，例如沿着图中的路径进行遍历（这是一类所谓的“指针追逐”问题，参见例如[GO16]）。对于估计矩阵范数 [BCK+18;BKKS20] 以及近似计数子图（见 [BC17]），已知单遍与多遍流式算法之间存在可证明的分离。近期，Assadi、Kol、Saxena 和 Yu [AKSY20] 以及 Assadi 和 N [AN21] 证明了图中环计数（及其变体）的近似问题的多遍下界，这排除了一些 针对约束满足问题的非平凡近似（不过，要排除两遍算法对最大割 的所有非平凡近似，我们似乎还相距甚远）。

此外，正如我们将在§2.7中看到的，流式计算问题的下界通常是通过从通信问题归约得到的。在这些问题中，多个参与者各自获得输入流的一个“片段”；在相应的通信到流式归约中，每位参与者都会在自己的输入片段上运行流式算法，然后将该算法的当前状态传递给下一位参与者。因此，空间占用小的流式算法能够构成高效的通信协议（而我们的目标就是证明高效通信协议的下界）。

这些通信问题定义中的细节，会对我们能够证明其下界的流式模型产生关键影响。下面我们简要说明其中的原因。首先，要证明随机排序算法的下界，通常需要玩家之间具有对称性：他们应当接收来自相同来源的输入，并以相同的方式处理这些输入。否则，他们在归约中构造出的数据流就会与随机排序相去甚远。另一方面，要证明草图算法的下界，只需考虑玩家以并行而非顺序方式进行通信的通信博弈，因为可组合性意味着每位玩家都可以独立地在自己的“数据块”上运行算法。最后，证明多遍下界的难点在于，通信问题包含多个“轮次”（分别对应每一遍），在每一轮中，每位玩家都能再次查看自己的数据块。这些细节意味着，即使不考虑其在流式下界中的应用，研究约束满足问题流式近似时所产生的通信问题也颇为有趣。最后，还有一个动

机是，这些通信问题与傅里叶分析和随机图组合学有着引人注目的联系。

2 预备知识

We begin with tools and definitions这是论文其余部分所必需的背景知识。本章回顾的主题包括 CSP（§2.1）、流式计算与草图算法（§2.2）、随机（超）图（§2.3）、关于 $\mathbb{Z}_q^n$ （§2.4）的傅里叶分析，以及尤为重要的单向通信下界和傅里叶分析在证明流式下界中的应用（§2.7）。

我们用 $[n]$ 表示自然数集合 $\{1,\ldots,n\}$，用 $\mathbb{Z}_q$ 表示模 q 的整数。*我们通常用粗体表示向量，但不表示其分量，例如，$\mathbf{b} = (b_1,\ldots,b_k)$。向量序列用圆括号标记索引（例如，$\mathbf{b}(\ell) = (b(\ell)1,\ldots,b(\ell)_k)$）。对于向量 $\mathbf{b} \in \mathbb{Z}_q^n$，我们将其汉明重量（又称零范数）$\|\mathbf{b}\|_0 \stackrel{\text{def}}{=} |\{i \in [n] \text{ 定义为: } b_i \neq 0\}|$其非零项的数量。对于有限字母表 Σ，我们用 Σ^k、$\Sigma^{\leq k}$ 和 Σ^* 分别表示长度为 k、长度至多为 k 和任意长度的 Σ 上的字符串。令 $\mathbb{1}_S$ 表示事件 S 的指示变量/函数；对于任意有限集合 Ω，令 $\Delta(\Omega)$ 表示 Ω 上概率分布构成的空间。

我们通常用花体字母表示分布和某些集合（例如函数族）。例如，$\mathcal{U}_S$ 表示 S上的均匀分布，$\mathcal{B}_p$ 表示伯努利分布

* $[q]$ 与 $\mathbb{Z}_q$ 之间的主要区别在于其隐含的加法运算。

，其取值为 0 的概率是 p，取值为 1 的概率是 $1-p$，而且 $\mathcal{P}_X$表示离散随机变量 X的概率分布。我们用函数记号表示分布概率，即 $\mathcal{D}(\omega) \overset{\text{定义为}}{=} \Pr_{\omega' \sim \mathcal{D}}[\omega = \omega']$。分布 $\mathcal{D} \in \Delta(\Omega)$ 的支撑集 是集合 $\mathrm{supp}(\mathcal{D}) \overset{\text{定义为}}{=} \{\omega \in \Omega : \mathcal{D}(\omega) \neq 0\}$。类似地，对于函数 $f : \Omega \to \mathbb{C}$，我们定义 $\mathrm{supp}(f) \overset{\text{定义为}}{=} \{\omega \in \Omega : f(\omega) \neq 0\}$；对于向量 $\mathbf{v} \in \mathbb{Z}_q^n$，定义 $\mathrm{supp}(\mathbf{v}) \overset{\text{定义为}}{=} \{i \in [n] : v_i \neq 0\}$（因此 $\|\mathbf{v}\|_0 = |\mathrm{supp}(\mathbf{v})|$）。

2.1 Constraint satisfaction problems

约束满足问题 Max-CSP($\mathcal{F}$) 由 $2 \leq q$、$k \in \mathbb{N}$ 和一个带标签的谓词集合 $\mathcal{F} = \{f_b$ 定义：$\mathbb{Z}_q^k \to \{0,1\}\}_{b \in B_\mathcal{F}}$对于某个有限标签集合 $B_\mathcal{F}$。[†]一个涉及 $n \in \mathbb{N}$ 个变量的约束 C 由三元组 $(b, \mathbf{j}, w)$ 给出，该三元组由一个标签 $b \in B_\mathcal{F}$、一个 k 元组 $\mathbf{j} = (j_1, \ldots, j_k) \in [n]^k$（其中各索引互不相同）以及一个权重 $w \geq 0$ 组成。Max-CSP($\mathcal{F}$) 的一个实例 Ψ 由一列 m 个约束 $(C_\ell = (b(\ell), \mathbf{j}(\ell), w(\ell)))_{\ell \in [m]}$ 组成。我们有时会省略约束的权重，此时将其统一取为 1；同样，如果 $|\mathcal{F}| = 1$，我们会省略约束的标签。

两个 Max-CSP($\mathcal{F}$) 实例 Ψ_1 和 Ψ_2 的并集，记作 $\Psi_1 \cup \Psi_2$，是将 Ψ_1 和 Ψ_2的约束列表拼接而成的实例。

对于赋值 $\mathbf{x} \in \mathbb{Z}_q^n$，令 $\mathbf{x}|_\mathbf{j} \overset{\text{def}}{=} (x_{j_1}, \ldots, x_{j_k}) \in \mathbb{Z}_q^k$表示 $\mathbf{x}$在索引 $\mathbf{j}$上的“限制”。当且仅当 $f_b(\mathbf{x}|_\mathbf{j}) = 1$时，赋值 $\mathbf{x}$ 满足 $C = (b, \mathbf{j}, w)$。实例 Ψ上赋值 $\mathbf{x} \in \mathbb{Z}_q^n$ 的值 记作 $\mathrm{val}_\Psi(\mathbf{x})$，即 $\mathbf{x}$满足的约束的（分数）权重，也就是，

$$\mathrm{val}_\Psi(\mathbf{x}) \overset{\text{def}}{=} \frac{1}{W_\Psi} \sum_{\ell=1}^{m} w(\ell) f_{b(\ell)}(\mathbf{x}|_{\mathbf{j}(\ell)})$$

其中 $W_\Psi \overset{\text{def}}{=} \sum_{\ell=1}^m w(\ell)$ 是 Ψ中的总权重。最后，Ψ的值 记作 val_Ψ，是任意赋值可取得的最大值，也就是，

$$\mathrm{val}_\Psi \overset{\text{def}}{=} \max_{\mathbf{x} \in \mathbb{Z}_q^n} (\mathrm{val}_\Psi(\mathbf{x})) .$$

从计算角度看，最大约束满足问题($\mathcal{F}$)的目标是“近似” val_Ψ。更

[†]严格来说，约束满足问题仅由谓词族定义；为方便记号起见，我们加入标签。

确切地说，对于 $\alpha \in (0,1]$，如果一个随机化算法 Alg α-近似 最大约束满足问题($\mathcal{F}$)，那么 $\alpha \mathsf{val}_\Psi \le \mathsf{Alg}(\Psi) \le \mathsf{val}_\Psi$ 的概率至少为（例如）$\frac{2}{3}$，其中概率是针对随机性的选择而言。对于 $\beta < \gamma \in [0,1]$，我们还考虑密切相关的 (β,γ)-最大约束满足问题($\mathcal{F}$)间隙问题，其目标是区分 $\mathsf{val}_\Psi \le \beta$ 和 $\mathsf{val}_\Psi \ge \gamma$ 两种情况，同样以至少 $\frac{2}{3}$ 的概率作出区分，其中概率是针对随机性的选择而言。[‡]

Approximation resistance

对于一个 CSP 最大约束满足问题($\mathcal{F}$)，定义

$$\rho(\mathcal{F}) \stackrel{\text{def}}{=} \inf_{\Psi} \mathsf{val}_\Psi.$$

$\rho(\mathcal{F})$ 有如下显式公式：

命题 2.1 ([CGSV21b，命题 2。12])。 对于任意 $\mathcal{F}$，

$$\rho(\mathcal{F}) = \min_{\mathcal{D} \in \Delta(\mathcal{F})} \max_{\mathcal{D}' \in \Delta(\mathbb{Z}_q)} \left(\mathop{\mathbb{E}}_{f \sim \mathcal{D}, \mathbf{a} \sim (\mathcal{D}')^k} [f(\mathbf{a})] \right).$$

在典型情形下，$|\mathcal{F}| = 1$, $\rho(\mathcal{F})$ 表示对 f 的任意概率赋值所能达到的最大值；这种赋值是对称的，即每个变量都独立地从同一分布中取值。

根据定义，只需在每个输入上输出 $\rho(\mathcal{F})$，就能得到 Max-CSP($\mathcal{F}$) 的 $\rho(\mathcal{F})$-近似；我们称之为平凡近似。如果对于某个算法类 $\mathcal{S}$，任意 $\epsilon > 0$ 下，$\mathcal{S}$ 中都不存在能够以 $(\rho(F) + \epsilon)$-近似 Max-CSP($\mathcal{F}$) 的算法，那么我们称 Max-CSP($\mathcal{F}$) 是近似抗性的。否则，我们称 Max-CSP($\mathcal{F}$) 对于$\mathcal{S}$是可近似的。

CSPs of interest

我们在这篇论文中研究的具体约束满足问题包括以下内容。对于 $k = q = 2$ 的情形，我们令割(x_1, x_2) def $= x_1 + x_2 = \mathbb{1}_{x_1 \neq x_2}$，并考虑问题最大割 def $=$

[‡]这种“密切联系”的一个方向是：如果 Alg α-近似 最大约束满足问题($\mathcal{F}$)，并且 $\frac{\beta}{\gamma} < \alpha$，那么 Alg 也能求解 (β, γ)-最大约束满足问题($\mathcal{F}$) 问题。关于另一个方向，参见下文推论 5.3 的证明概要。

最大约束满足问题({割})。类似地，我们令有向割$(x_1, x_2) \stackrel{\text{def}}{=} x_1(x_2 + 1) = \mathbb{1}_{x_1=1,x_2=0}$，并考虑问题最大有向割 $\stackrel{\text{def}}{=}$ 最大约束满足问题({有向割})。

在 $q = 2$ 的情况下，对于谓词 $f\colon \mathbb{Z}_2^k \to \{0,1\}$，我们将问题 Max-BCSP($f$) 定义为 Max-CSP($\{f_{\mathbf{b}}\colon \mathbb{Z}_2^k \to \{0,1\}\}_{\mathbf{b}\in\mathbb{Z}_2^k}$)，其中 $f_{\mathbf{b}}(\mathbf{x}) = f(\mathbf{b} + \mathbf{x})$；该约束满足问题的谓词对应于“带取反的 f ”。例如，对于 $k = 2$，我们令 2AND(x_1, x_2) 定义为 $x_1x_2 = \mathbb{1}_{x_1=x_2=1}$。那么，Max-2AND 定义为 Max-BCSP(2AND)，包含四个谓词 $\text{2AND}_{b_1,b_2}(x_1, x_2) = (x_1 + b_1)(x_2 + b_2)$，其中 $b_1, b_2 \in \mathbb{Z}_2$。（注意，$\text{2AND}_{0,0} = 2$ 是 AND，$\text{2AND}_{0,1} =$ 是有向割。）更一般地，我们定义 $k\text{AND}(x_1, \ldots, x_k) = \prod_{i=1}^k x_i$，并考虑 Max-$k$AND。

读者可以验证，Max-Cut、Max-DiCut 和 Max-BCSP(f) 的平凡近似比 $\rho(\mathcal{F})$ 分别为 $\frac{1}{2}$、$\frac{1}{4}$和 $\overline{\rho}(f) \stackrel{\text{def}}{=} \mathbb{E}_{\mathbf{a}\sim\mathcal{U}_{\mathbb{Z}_2^k}}[f(\mathbf{a})]$,。

2.2 Streaming and sketching algorithms

对于谓词族 $\mathcal{F}$，我们考虑尝试在 $s(n)$-空间流式设置中求解近似问题 Max-CSP($\mathcal{F}$) 或区分问题 (β, γ)-Max-CSP($\mathcal{F}$) 的算法，其中 $s(n)$ 通常很小（例如 polylog(n)）。首先，我们给出一个非正式定义。对于输入 Ψ （含有 n 个变量），流式算法的空间限制为 $s(n)$，且只能通过按某种顺序单次遍历 Ψ 的约束来访问这些约束；该顺序可以由对手决定，也可以随机（均匀地）选取。（若未特别说明，我们假设输入按对抗性顺序排列。）另一方面，算法可以使用随机性，且不受时间或一致性限制。我们还考虑一类称为草图化算法的流式算法子类，其特点是算法可以分别在输入流的两半上运行，并将所得状态合并。若算法的状态编码了向量空间中的一个元素，且合并对应于向量加法，则该草图化算法称为线性算法。

更形式化一些，我们如下定义流式计算和草图算法。令 Σ 表示数据流的输入空间（例如，包含 n 个变量的最大约束满足问题($\mathcal{F}$)实例中的约束）。一个确定性空间-s 流式算法 Alg 由一对函数 NextState : $\{0,1\}^s \times \Sigma \to \{0,1\}^s$ 和 Output : $\{0,1\}^s \to \{0,1\}^*$ 指定。对于输入流 $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_m) \in \Sigma^*$，我们将 FinalState($\boldsymbol{\sigma}$) $\in \{0,1\}^s$ 定义为：初始化状态 $S \leftarrow 0^s$，然后对 $\ell \in [m]$ 迭代执行 $S \leftarrow$ NextState(S, σ_ℓ)；接着

Alg 输出 Output(FinalState($\boldsymbol{\sigma}$))。此外，如果存在另一个函数 Compose : $\{0,1\}^s \times \{0,1\}^s \to \{0,1\}^s$，使得对于任意两个输入流$\boldsymbol{\sigma}$，$\boldsymbol{\sigma}' \in \Sigma^*$，都有，Alg 就是一个草图算法 。

$$\text{最终状态}(\boldsymbol{\sigma}\boldsymbol{\sigma}') = \text{组合}(\text{最终状态}(\boldsymbol{\sigma}), \text{最终状态}(\boldsymbol{\sigma}')),$$

其中 $\boldsymbol{\sigma}\boldsymbol{\sigma}'$ 表示拼接。随机化的流式计算和草图算法分别是流式计算和草图算法上的分布，且成功概率至少为$2\ 3$。[§]

–

一个值得关注的草图算法是下面这个用于对 1-范数进行草图化的经典算法，我们在后续章节中将其作为黑盒使用：

定理 2.2 ([Ind06; KNW10])。对于每个 $\epsilon > 0$ 和 $c < \infty$，都存在一个 $O(\log n/\epsilon^2)$- 空间随机化草图算法，用于解决以下问题：输入是一个由集合 $\Sigma = [n] \times \{-O(n^c) \ldots, O(n^c)\}$ 中的更新构成的（按对抗方式排序的）数据流 $\boldsymbol{\sigma}$，目标是估计由 $x_i = \sum_{(i,v)\in\boldsymbol{\sigma}} v$ 定义的向量 $\mathbf{x} \in \mathbb{N}^n$ 的1-范数，误差不超过乘法因子 $1 \pm \epsilon$。

2.3 Hypergraphs

设 $2 \le k, n \in \mathbb{N}$。$k$-超边是 $[n]$ 上的一个 k元组 $\mathsf{e} = (e_1, \ldots, e_k) \in [n]^k$，其中各索引互不相同；$k$-超图（亦称“$k$-均匀超图”）$G$ 是 $[n]$ 上的一个序列 $(\mathsf{e}(1) \ldots, \mathsf{e}(m))$，其中包含（不一定互不相同的）$k$-超边。假设 $k = 2$，当省略 k 时即如此，此时我们省略前缀“超”。给定一个实例 Ψ，它属于一个具有约束 $(\mathsf{b}(\ell), \mathsf{j}(\ell)\ w(\ell))_{\ell\in[m]}$ 的 k元 CSP 最大约束满足问题($\mathcal{F}$)，我们可以定义 Ψ 的约束（超）图 $G(\Psi)$，它是一个 k-超图，其超边为 $(\mathsf{j}(\ell))_{\ell\in[m]}$。请注意，当$|\mathcal{F}| = 1$（例如最大割和最大有向割的情况）且我们仅考虑无权实例时，Ψ 和 $G(\Psi)$ 所包含的数据完全相同。

[§]技术说明：由于我们允许数据流元素重复（特别是 Max-CSP($\mathcal{F}$) 实例中的约束可以重复），为了获得 polylog(n) 空间算法，我们必须预先选定一个数据流长度上界。全文中，我们假设实例最多包含 $O(n^c)$ 个约束，其中 $c < \infty$ 是某个（较大的）固定值。此外，为了在算法的状态中存储约束权重，我们假设这些权重为整数，且绝对值不超过 $O(n^c)$。为简化表述，全文通常省略这些细节。

对于一个包含 m 条边的 k-超图 G，我们将其关联到一个邻接矩阵 $M \in \{0,1\}^{km \times n}$，其第 $(\ell k + j, i)$ 项为 1，当且仅当 $e(\ell)_j = i$（对于 $\ell \in [m], j \in [k], i \in [n]$）。由于它们编码了相同的信息，我们常将邻接矩阵与 k-超图视为可互换的。重要的是，我们常考虑 M 和 $M^\top$ 与 $\mathbb{Z}_q$ 上向量的乘积。给定 $\mathbf{v} \in \mathbb{Z}_q^n$ 和 $\mathbf{s} = M\mathbf{v}$，令 $\mathbf{s}(\ell) = (s_{(k-1)\ell+1}, \ldots, s_{k\ell})$ 表示 $\mathbf{s}$ 中由 k 个坐标组成的第 ℓ 个块；于是 $\mathbf{s}(\ell) = \mathbf{v}|_{\mathbf{e}(\ell)}$。因此，我们可以将 $\mathbf{v}$ 视为“顶点的 $\mathbb{Z}_q$ 标记”，将 $\mathbf{s}$ 视为相应的“超边-顶点关联的 $\mathbb{Z}_q$ 标记”，其中每条超边 $\mathbf{e} = (e_1, \ldots, e_k)$ 确定 k 个唯一关联 $(\mathbf{e}, e_1), \ldots, (\mathbf{e}, e_k)$。反过来，给定 $\mathbf{s} \in \mathbb{Z}_q^m$，若 $\mathbf{v} = M^\top \mathbf{s}$，则对于每个 $i \in [n]$，我们有

$$v_i = \sum_{\ell \in [m], j \in [k]} \mathbb{1}_{\mathbf{e}(\ell)_j = i} \, \mathbf{s}(\ell)_j .$$

我们再次将$\mathbf{s}$ 视为超边-顶点关联上的标签；$\mathbf{v}$ 则表示与每个顶点关联的超边上的$\mathbf{s}$-标签之和。此外，我们有时会考虑邻接矩阵 M 的“折叠”变体，它们会将每个由 k-超边对应的 k 列块“压缩”为更少的列，例如将这些列求和为一列；相应地，$M\mathbf{v}$和 $M^\top\mathbf{s}$也有对应的解释。

对于 $\alpha \in (0,1)$ $n \in \mathbb{N}$，令 $\mathcal{G}_{k,\alpha}(n)$ 表示 k-超图在 $[n]$ 上且含有 αn 条超边的均匀分布。k-超图 G 是一个 k-超匹配，当且仅当任意超边之间没有共享顶点，即若 $v \in e(\ell)$ $e(\ell')$ 则 $\ell = \ell'$；等价地，邻接矩阵 M的每一行至多包含一个 1。我们将含有 αn 条边的 k-超匹配 G 称为 α-部分。令 $\mathcal{M}_{k,\alpha}(n)$ 表示 k-超匹配在 $[n]$上且含有 αn 条超边的均匀分布（其中 $\alpha \in (0,1)$ $n \in \mathbb{N}$）。

2.4 Fourier analysis

设 $q \geq 2 \in \mathbb{N}$，并设 $\omega \stackrel{\text{def}}{=} e^{2\pi i/q}$ 表示一个（固定的本原）q次单位根。这里，我们总结了在 $\mathbb{Z}_q^n$上的傅里叶分析的相关内容；详情请参见例如 [O'D14，§8]。[¶]

¶[O'D14] 采用不同的范数和内积归一化方式，主要是因为它考虑的是期望，而不是对输入求和。

给定函数 $f\colon\ \mathbb{Z}_q^n \to \mathbb{C}$，且$\mathbf{s}\ \in \mathbb{Z}_q^n$，我们定义傅里叶系数

$$\widehat{f}(\mathbf{s}) \stackrel{\text{def}}{=} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \omega^{-\mathbf{s}\cdot\mathbf{x}} f(\mathbf{x})$$

其中，$\cdot$表示在 $\mathbb{Z}_q$上的内积。对于 $p \in (0,\ \infty)$，我们将 f的 p范数定义为

$$\|f\|_p \stackrel{\text{def}}{=} \left(\sum_{\mathbf{x}\in\mathbb{Z}_q^n} |f(\mathbf{x})|^p\right)^{1/p}.$$

我们还将 f的零范数定义为

$$\|f\|_0 \stackrel{\text{def}}{=} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \mathbb{1}_{f(\mathbf{x})\neq 0}$$

（也称其支撑集的大小，以及其“真值表”的汉明重量）。此外，对于$\ell \in \{0\} \cup [n]$，我们将第ℓ 级傅里叶（2）权重定义为

$$\mathsf{W}^{\ell}[f] \stackrel{\text{def}}{=} \sum_{\mathbf{s}\in\mathbb{Z}_q^n:\|\mathbf{s}\|_0=\ell} |\widehat{f}(\mathbf{s})|^2.$$

这些权重与 f的 2-范数密切相关：

命题 2.3（帕塞瓦尔恒等式）。对于任意 q，$n \in \mathbb{N}$ 和 $f\colon\ \mathbb{Z}_q^n \to \mathbb{C}$，有

$$\|f\|_2^2 = q^n \sum_{\ell=0}^{n} \mathsf{W}^{\ell}[f].$$

此外，令 $\mathbb{D} \stackrel{\text{定义为}}{=} \{w \in \mathbb{C}\colon\ |w| \le 1\}$ 表示复平面中的（闭）单位圆盘。以下引理对映射到 $\mathbb{D}$的函数的低阶傅里叶权重进行界定，其推导 [CGS+22]中的超收缩性定理：

引理 2.4 ([CGS+22，引理 2.11])。存在 $\zeta > 0$ 使得以下结论成立。设$q \ge 2$，$n \in \mathbb{N}$并考虑任意函数 $f\colon\ \mathbb{Z}_q^n \to \mathbb{D}$。若 $c \in \mathbb{N}$，$\|f\|_0 \ge q^{n-c}$，则对每个 $\ell \in \{1, \ldots, 4c\}$，都有

$$\frac{q^{2n}}{\|f\|_0^2}\mathsf{W}^{\ell}[f] \le \left(\frac{\zeta c}{\ell}\right)^{\ell}.$$

2.5 Concentration inequalities

我们将使用以下关于子鞅的集中不等式：

引理 2.5 ([KK19，引理 2.5])。设 X_1，...，X_m 是（不一定相互独立的）$\{0,1\}$值随机变量，并且存在某个 $p \in (0,\ 1)$，$\mathbb{E}[X_\ell \mid X_0, \ldots, X_{\ell-1}] \leq p$ 对每个$\ell \in [m]$都成立。设 $\mu = pm$。那么对每个 $\eta > 0$，

$$\Pr\left[\sum_{\ell=1}^{m} X_\ell \geq \mu + \eta\right] \leq e^{-\eta^2/(2(\mu+\eta)))}.$$

2.6 Advantage and total variation distance

设 $\mathcal{Y}$，$\mathcal{N} \in \Delta(\Omega)$，并考虑一个测试函数$\mathsf{Test}\colon \Omega \to \{0,1\}$，它试图通过对从 $\mathcal{Y}$ 中采样的输入比从 $\mathcal{N}$ 中采样的输入更频繁地输出 1（或反之），来区分 $\mathcal{Y}$ 和 $\mathcal{N}$。f 的优势衡量了它在这项区分任务中的成功程度：

$$\mathsf{adv}_{\mathcal{Y},\mathcal{N}}(\mathsf{Test}) \stackrel{\text{def}}{=} |\mathbb{E}[\mathsf{Test}(\mathcal{Y})] - \mathbb{E}[\mathsf{Test}(\mathcal{N})]| \in [0,1].$$

两个分布 $\mathcal{Y}$，$\mathcal{N}$之间的全变差距离，是任意测试 f 在区分 $\mathcal{Y}$ 和 $\mathcal{N}$时所能达到的最大优势。最优的 f 是所谓的“最大似然估计器”，它在输入 $\omega \in \Omega$ 时，输出 $\mathbb{1}_{\mathcal{Y}(\omega)\geq\mathcal{N}(\omega)}$。因此，

$$\|\mathcal{Y} - \mathcal{N}\|_{\text{tv}} \stackrel{\text{def}}{=} \max_{\mathsf{Test}:\Omega\to\{0,1\}} (\mathsf{adv}_{\mathcal{Y},\mathcal{N}}(\mathsf{Test})) = \frac{1}{2}\sum_{\omega\in\Omega} |\mathcal{Y}(\omega) - \mathcal{N}(\omega)|\,.$$

此外，对于两个随机变量 Y和 N，我们用 $\|Y - N\|_{\text{tv}}$作为 $\|\mathcal{P}_Y - \mathcal{P}_N\|_{\text{tv}}$的简写（回想一下，例如，$\mathcal{P}_Y$ 表示 Y的分布）。

总　　变差距离满足两个对我们而言很重要的不等式：

引理 2.6（三角不等式）。设 $\mathcal{Y}$，$\mathcal{N}$，$\mathcal{Z} \in \Delta(\Omega)$。则

$$\|\mathcal{Y} - \mathcal{N}\|_{\text{tv}} \geq \|\mathcal{Y} - \mathcal{Z}\|_{\text{tv}} - \|\mathcal{Z} - \mathcal{N}\|_{\text{tv}}.$$

引理 2.7（数据处理不等式）。设 Y、N 为样本空间Ω上的随机变量，并设 Z 为样本空间 Ω' 上的随机变量，它与 Y 和 N相互独立。若 $g : \Omega \times \Omega' \to \Omega''$ 是任意函数，则

$$\|Y - N\|_{\mathrm{tv}} \geq \|g(Y, Z) - g(N, Z)\|_{\mathrm{tv}}.$$

直观地说，引理 2.7 指出，要区分两个随机变量Y和 N的分布，先进行任何额外的（可能是随机的）变换都没有帮助。

2.7 Lower bound basics

最后，我们考虑几种针对特定类型集合上的分布进行判别的测试。这些概念对于证明流式近似约束满足问题的下界至关重要。

首先，令 Σ 为有限输入空间，并考虑 $\Omega = \Sigma^*$ 的情况。给定一对分布 $\mathcal{Y}$，$\mathcal{N} \in \Delta(\Omega)$，我们可以将确定性流式算法 Alg 视为用于区分 $\mathcal{Y}$ 和 $\mathcal{N}$ 的测试。这一视角使我们能够通过构造不可区分$\mathcal{Y}$ 和 $\mathcal{N}$ 的分布，排除适用于 (β, γ)-最大约束满足问题$(\mathcal{F})$ 的算法（进而排除对最大约束满足问题$(\mathcal{F})$ 的 $(\frac{\beta}{\gamma} + \epsilon)$-近似算法）：

命题 2.8 (极小极大引理 [Yao77], 关于 最大约束满足问题$(\mathcal{F})$ 的非正式表述。考虑一个约束满足问题 最大约束满足问题$(\mathcal{F})$，并令 $\mathcal{S}$ 表示一类随机化算法（例如，具有对抗性输入顺序的 $O(\sqrt{n})$-空间流式算法）。令 $\beta < \gamma \in [0, 1]$，并假设 $\mathcal{Y}$ 和 $\mathcal{N}$ 是定义在 最大约束满足问题$(\mathcal{F})$ 实例上的分布，满足

$$\Pr_{\Psi \sim \mathcal{N}}[\mathit{val}_\Psi \geq \beta] \leq 0.01 \ \mathit{and} \ \Pr_{\Psi \sim \mathcal{Y}}[\mathit{val}_\Psi \leq \gamma] \leq 0.01.$$

那么，如果存在 $\mathit{Alg} \in \mathcal{S}$ 能够求解(β, γ)-最大约束满足问题$(\mathcal{F})$，则存在一个确定性算法，可在 $\mathcal{S}$ 中区分 $\mathcal{Y}$ 和 $\mathcal{N}$，且其优势至少为1_6。

现在考虑乘积集合 $\Omega = \Omega_1 \times \cdots \times \Omega_T$ 的情形。函数集合 $\mathrm{Prot}_t : \{0,1\}^s \times \Omega_t \to \{0,1\}^s$ for $t \in [T]$ 定义了一个空间-s 通信协议 $\mathrm{Prot} : \Omega \to \{0,1\}$，定义方式如下。给定输入 $\boldsymbol{\omega} = (\omega_1, \ldots, \omega_T) \in \Omega$，令 $S \leftarrow 0^s$ 并迭代

对 $t \in [T]$ 应用 $S \leftarrow \mathsf{Prot}_t(S, \omega_t)$；最后输出 S。（我们假设 Prot_T 的陪域是$\{0,1\}$。）Prot 是一种用于区分分布 $\mathcal{Y}, \mathcal{N} \in \Delta(\Omega)$ 的特殊测试。我们也可以将这种协议解释为以下单向通信博弈（或问题）中的策略，参与者为 $\mathsf{Player}_1, \ldots, \mathsf{Player}_T$：

- 我们从 $\mathcal{Y}$（是情形）或 $\mathcal{N}$（否情形）中采样 $\boldsymbol{\omega} = (\omega_1, \ldots, \omega_T)$。玩家$_t$ 收到输入 ω_t。

- 玩家$_1$ 根据自己的输入 ω_1向玩家$_2$发送一条消息。对于 $t \in \{2, \ldots, T-1\}$，玩家$_t$ 根据玩家$_{t-1}$发送的消息以及自己的输入 ω_t，向玩家$_{t+1}$发送一条消息。玩家$_T$根据玩家$_{T-1}$发送的消息以及自己的输入 ω_T，决定输出 1 还是 0。

- 玩家们的共同目标是最大化他们区分**是**情形和**否**情形的优势。

这种博弈可用于模拟流式算法执行期间的信息流动。直观地说，对于长度为 m 的数据流，我们可以将其视为一个 m 人单向通信博弈协议，其中 玩家$_t$ 获得数据流中的第 t 个元素，而每位玩家都会将流式算法的状态传递给下一位玩家。要证明此类协议的下界，只需证明只有常数个 $T = O(1)$ 名玩家的“粗粒度”博弈中的下界，其中每位玩家获得一段包含例如 m/T 个流元素的“数据块”。这相当于放宽流式计算模型的定义，只要求算法状态在数据流中的 T “瓶颈”位置保持简洁。因此，要证明流式下界，我们需要证明在这些瓶颈处，算法状态无法充分捕获其已从数据流中读取的元素的信息。通过这种“归约”，流式问题的下界可以由恰当定义的通信博弈的下界推出。（关于 §3.1 中针对 最大割 的具体说明，见该节。）

现在，我们以一种更方便、更一般的表述，精确定义这一通信到流式（归约）归约：每位参与者的输入不一定是一段约束；相反，每位参与者都会根据某些预先定义的“归约函数”，从自己的输入中构造约束。假设 Σ是一个有限输入空间，而 $\Omega = \Omega_1 \times \cdots \times \Omega_T$

仍然是一个乘积空间。给定一个分布 $\mathcal{D} \in \Delta(\Omega)$ 和归约函数 $\mathrm{R}_t : \Omega_t \to \Sigma^*$ for $t \in [T]$，定义 $(R_1, \ldots, R_T) \circ \mathcal{D}$ 为如下分布：从 Σ^* 中采样 $(\omega_1, \ldots, \omega_T) \sim \mathcal{D}$，并输出拼接结果 $\mathrm{R}_1(\omega_1) \cdots \mathrm{R}_T(\omega_T)$。

引理 2.9 (通信到流式归约)。 设 $\Omega = \Omega_1 \times \cdots \times \Omega_t$ 和 Σ 为有限集。设 $\mathcal{Y}, \mathcal{N} \in \Delta(\Omega)$ 和 $R_t : \Omega_t \to \Sigma^*$ 对于 $t \in [T]$。若存在一个确定性空间-s 流式算法 Alg，用于区分 $(R_1, \ldots, R_T) \circ \mathcal{Y}$ 与 $(R_1, \ldots, R_T) \circ \mathcal{N}$，其优势为 δ，则存在一个空间-s 通信协议 $Prot$，用于区分 $\mathcal{Y}$ 与 $\mathcal{N}$，其优势为 δ。

证明。设 Alg 由 (NextState, Output) 给出。考虑协议 Prot，其中玩家$_1$在输入 ω_1 上，设置 $S \leftarrow \mathrm{NextState}(\mathrm{R}_1(\omega_1)\ 0^s)$，并将其发送给玩家$_2$。现在，对于 $t \in \{2, \ldots, T-1\}$，玩家$_t$ 从玩家$_{t-1}$接收 S，设置 $S \leftarrow \mathrm{NextState}(\mathrm{R}_t(\omega_t)\ S)$，并将其发送给玩家$_{t+1}$。最后，玩家$_T$输出 $\mathrm{Output}(\mathrm{NextState}(\mathrm{R}_T(\omega_T)\ S))$。根据定义，当玩家接收到输入 $(\omega_1, \ldots, \omega_T)$ 时，他们运行 Alg 处理数据流 $\boldsymbol{\sigma} = \mathrm{R}_1(\omega_1) \cdots \mathrm{R}_T(\omega_T)$。如果玩家的输入来自 $\mathcal{Y}$，那么 $\boldsymbol{\sigma}$ 的分布为 $(\mathrm{R1}, \ldots, \mathrm{R}_T) \circ \mathcal{Y}$，对于$\mathcal{N}$也同理。

□

在我们的设定中，归约会生成 CSP 实例，我们通常认为每个归约函数都会为每位参与者输出一个“子实例”，这些子实例的并集就是输出实例 Ψ。

我们考虑的优势的最后一种特殊情形，是区分 $\mathcal{D} \in \Delta(\mathbb{Z}_q^n)$ 与均匀分布 $\mathcal{U}_{\mathbb{Z}_q^n}$。回想一下，我们将 $\mathcal{D} \in \Delta(\mathbb{Z}_q^n)$ 视为函数 $\mathbb{Z}_q^n \to [0,1]$，$\widehat{\ }$，于是可以考虑 $\mathcal{D}(\mathbf{s})$ 对 $\mathbf{s} \in \mathbb{Z}_q^n$ 的傅里叶系数。下面这个简单但至关重要的引理，将 $\mathcal{D}$ 与均匀分布的距离和这些系数联系起来：

引理 2.10. 设 $\mathcal{D} \in \Delta(\mathbb{Z}_q^n)$，并设 $\mathcal{U} = \mathcal{U}_{\mathbb{Z}_q^n}$。则

$$\|\mathcal{D} - \mathcal{U}\|_{\mathrm{tv}}^2 \le q^{2n} \sum_{\mathbf{s} \neq \mathbf{0} \in \mathbb{Z}_q^n} |\widehat{\mathcal{D}}(\mathbf{s})|^2.$$

$\widehat{\ }$ $\widehat{\ }$证明。我们有 $\mathcal{D}(\mathbf{0}) = \sum_{\mathbf{z} \in \mathbb{Z}_q^{\alpha n}} \mathcal{D}(\mathbf{z}) = 1$。类似地，$\mathcal{U}(\mathbf{0}) = 1$；而对于$\mathbf{s} \neq \mathbf{0} \in \mathbb{Z}_q^{\alpha n}$，我们有 $\widehat{\mathcal{U}}(\mathbf{s}) = \frac{1}{q^{\alpha n}} \sum_{\mathbf{z} \in \mathbb{Z}_2^{\alpha n}} (-1)^{\mathbf{s} \cdot \mathbf{z}} = 0$，由对称性可得。此外，根据定义，$\|\mathcal{D} - \mathcal{U}\|_{\mathrm{tv}} = \frac{1}{2}\|\mathcal{D} - \mathcal{U}\|_1$，其中 $\mathcal{D} - \mathcal{U} : \mathbb{Z}_q^n \to [-1, 1]$ 是 $\mathcal{D}$ 和 $\mathcal{U}$ 的概率质量函数之差。

因此，利用柯西-施瓦茨不等式和帕塞瓦尔恒等式（命题 2.3），我们有

$$\|\mathcal{D}-\mathcal{U}\|_{\mathrm{tv}}^2 \le q^n \|\mathcal{D}-\mathcal{U}\|_2^2 = q^{2n} \sum_{\mathbf{s}\in\mathbb{Z}_q^n} |\widehat{\mathcal{D}}(\mathbf{s}) - \widehat{\mathcal{U}}(\mathbf{s})|^2 = q^{2n} \sum_{\mathbf{s}\neq\mathbf{0}\in\mathbb{Z}_q^n} |\widehat{\mathcal{D}}(\mathbf{s})|^2,$$

按需要。 □

引理 2.10 是所谓“XOR 引理”的一个例子（参见 [Gol11，§1]）。在 $q = 2$ 情形下，对于每个 $\mathbf{s} \in \mathbb{Z}_q^n$，$\mathcal{D}(\mathbf{s})$ 是线性测试的优势；该测试针对 $\mathcal{D}$，给定样本 $\mathbf{z} \sim \mathcal{D}$ 后，输出 $\sum_{i\in[n]:s_i=1} z_i$。该引理大致表明，如果这些测试都无法取得良好效果，那么 $\mathcal{D}$ 实际上接近均匀分布。

总之，命题 2.8 和 引理 2.9 和 2.10 为证明 CSP 流式不可近似性结果提供了一个“路线图”。具体而言，我们设计一个具有以下两个性质的单向通信博弈：

1. 玩家可以使用归约函数（依照 引理 2.9）根据各自的输入生成 CSP 实例，并使得在 **是** 和 **否** 两种情形下，实例的值之间存在很大差距（以高概率成立）。

2. 该博弈本身的困难性可以通过引理 2.10 以及额外的傅里叶分析和组合学来证明。

在约束满足问题的语境中，Kapralov、Khanna 和 Sudan 首先将这一方法用于 [KKS15] 处理最大割。我们将在下一章讨论这一证明。

I

已有结果

3

最大割具有近似抗性

问题定义如下：给定一个含有 n 个节点的图G的边数据流，估计 G中的最大割的值。问题：是否存在一种使用$o(n)$ 空间、近似因子严格优于 1/2 的算法?

[IMNO11，问题 10],归功于 Robert Krauthgamer

Max-Cut was the first CSP其流式近似性得到了精确刻画。具体而言，Kapralov、Khanna 和 Sudan [KKS15] 证明了以下定理：

定理 3.1 ([KKS15])。对于任意常数 $\epsilon > 0$，任何以 $(\frac{1}{2} + \epsilon)$-近似 最大割的流式算法都需要 $\Omega(\sqrt{n})$ 空间。

本章旨在证明定理 3.1。我们还指出，在经典情形下，Goemans 和 Williamson [GW95]给出了一种基于半定规划舍入的算法，该算法对最大割的近似比为 α_{GW}，其中 $\alpha_{\mathrm{GW}} = \min_{\theta \in [0,\mathrm{Prot}]} \frac{2\theta}{1 - \mathrm{Prot}(\cos(\theta))} \approx 0.87856$;*

*Khot、Kindler、Mossel 和 O'Donnell [KKMO07] 证明了（$\alpha_{\mathrm{GW}} + \epsilon$）-近似是 UG 困难的。无需唯一博弈猜想（UGC），Trevisan 等人 [TSSW00] 证明了（$\frac{16}{17} + \epsilon$）-近似是 **NP**-困难的，但 $\frac{16}{17} \approx 0.94118$。

因此，定理 3.1 表明，最大割 在流式设置下的可近似性相较于经典情形要低得多。

现在，我们先直观说明一下，为什么使用小空间流式算法对最大割进行近似应该是困难的。考虑一个在输入实例 Ψ 上求解最大割的流式算法。假设我们在输入流进行到一半时暂停该算法，此时，该算法已经相当有把握地认为 val_Ψ 很大，并且对一个具有较高值的赋值有一个“猜测” $\mathbf{x} \in \mathbb{Z}_2^n$。那么，在数据流的后半段，该算法应当能够确认它所看到的约束也与 $\mathbf{x}$（大部分）一致。

为了证明最大割的流式近似抗性，我们在第 3.1 节首先定义一个将这一困难形式化的单向通信问题，并将其称为布尔划分检测（BPD），[†] 同时概述 BPD 的困难性如何通过中间问题“序贯布尔划分检测问题（sBPD）”蕴含最大割的困难性。接着，在第 3.2 节中，我们介绍 Gavinsky 等人 [GKK+08] 最初提出的、用于证明 BPD 困难性的傅里叶分析证明；在第 3.3 节中，我们展示 sBPD 如何通过 Kapralov、Khanna 和 Sudan [KKS15] 的混合论证归约到 BPD。最后，在第 3.4 节中，我们对最大割下界的若干重要特征作出评论，而这些特征对于本论文所考虑的其他约束满足问题仍将具有重要意义。

3.1 Boolean partition detection problems

设 $M \in \{0,1\}^{2\alpha n \times n}$ 是一个图的邻接矩阵，该图有 n 个顶点和 αn 条边。回想一下，在 M 中，每条边对应一个 $2 \times n$ 块。我们将 M 的一个折叠变体定义为：用每个 $2 \times n$ 边块各列之和替换该块，并将其记为 $M^{\mathsf{fold}} \in \{0,1\}^{\alpha n \times n}$；因此，$M^{\mathsf{fold}}$ 的每一列对应一条边，其中的 1 表示与该边相接的两个顶点。于是，BPD 问题定义如下。

定义 3.2 (BPD)。设 $\alpha \in (0,\ 1)$ 且 $n \in \mathbb{N}$。那么，$\mathit{BPD}_\alpha(n)$ 是以下由 *Alice* 和 *Bob* 参与的双人单向通信问题：

- *Alice* 收到一个随机向量 $\mathbf{x}^* \sim \mathcal{U}_{\mathbb{Z}_2^n}$。

[†] 文献中通常将其称为布尔隐藏匹配问题（例如参见 [KKS15]）。不过，在本文中，由于我们需要兼顾各种通信问题，因此选择采用一种更为统一的命名方案。

- *Bob* 收到一个从 $\mathcal{M}_\alpha(n)$ 中采样得到的邻接矩阵 $M \in \{0,1\}^{2\alpha n \times n}$，以及一个向量 $\mathbf{z} \in \mathbb{Z}_2^{\alpha n}$，它为 M 的每条边赋予标签，定义如下：– 是 情况：$\mathbf{z} = (M_{\text{折叠}})\mathbf{x}^*$。– 否 情况：$\mathbf{z} \sim \mathcal{U}_{\mathbb{Z}_2^{\alpha n}}$。

- *Alice* 可以向 *Bob* 发送一条消息，随后 *Bob* 必须判断他们处于是情形还是否情形。

我们可以将 Alice 的向量 $\mathbf{x}^*$ 视为 M 的顶点的一种划分。在**是** 情形下，Bob 的向量 $\mathbf{z}$ 可以解释如下：如果$\mathbf{e}(\ell) = (u, v)$ 是 M 的第 ℓ 条边，那么 $z_\ell = x^*_u + x^*_v$。因此，$\mathbf{z}$ 精确地编码了 M 中哪些边跨越了划分$\mathbf{x}^*$。另一方面，在**否** 情形下，$\mathbf{z}$ 服从均匀分布。因此，Bob 的目标是根据 Alice 的消息，判断自己的输入$\mathbf{z}$ 是否与划分$\mathbf{x}^*$ 一致。

在 §3.2 下文中，我们将证明，这项任务需要 Alice向 Bob进行大量通信：

定理 3.3 ([GKK+08])。对于任意 $\alpha, \delta \in (0,1)$，存在 $\tau > 0$和 $n_0 \in \mathbb{N}$，使得对于所有 $n \geq n_0$，任何针对 $BPD_\alpha(n)$ 且优势至少为 δ 的协议，都需要 $\tau\sqrt{n}$通信。 –

虽然定理 3.3 揭示了在流式计算设置下计算最大割的根本障碍，但仅凭它还不足以证明不可近似性。为此，我们希望 Alice 和 Bob 通过流式计算到通信的归约（见引理 2.9）构造最大割实例，使是与否情形之间存在较大的值差距。事实上，要排除 $\approx \frac{1}{2}$-近似，是实例的值应为 ≈ 1，而否实例的值应为 $\approx \frac{1}{2}$。起初，我们可能希望通过从 BPD 到最大割的直接归约来构造这样的实例。在 BPD 的是情形中，假设对每条跨越该割的边（即满足 $z_\ell = 1$ 的边），Bob 都创建一个对应的最大割约束；令人鼓舞的是，由此得到的实例的值为 1！但遗憾的是，否情形也一样，因为每个 $\mathbf{z}$ 都与某个 M 的划分 $\mathbf{x}'$ 相一致。例如，对于每个 $\mathbf{e}(\ell) = (u, v)$，我们都可以设定 $x'_u = 0$ 和 $x'_v = z_\ell$（并任意赋值其余的 x值）；特别是，由于 M 是一个匹配，这些赋值彼此不会冲突。‡

‡换句话说，Bob 创建的最大割实例所对应的图始终是一个匹配，而匹配总是二部图；因此，Bob 的实例的值始终为 1。

简言之，问题在于 BPD 中的底层图过于稀疏，无法用于构造低值的最大割实例。为了解决这一问题，我们引入 BPD 的一种顺序变体，它能够产生更稠密的图：

定义 3.4 (sBPD)。 设 $\alpha \in (0, 1)$ 且 $T, n \in \mathbb{N}$。那么 $\mathit{sBPD}_{\alpha,T}(n)$ 是如下$(T+1)$人单向通信问题，参与者为 *Alice* 和 Bob_1、……、Bob_T：

- *Alice* 收到一个随机向量 $\mathbf{x}^* \sim \mathcal{U}_{\mathbb{Z}_2^n}$。
- 每个 Bob_t 都会收到一个从 $\mathcal{M}_\alpha(n)$中抽样得到的邻接矩阵 $M_t \in \{0,1\}^{2\alpha n \times n}$，以及一个向量 $\mathbf{z}(t) \in \mathbb{Z}_2^{\alpha n}$，按如下方式为 M_t 的每条边赋标签：

  – 是 情形：$\mathbf{z}(t) = (M_t^{\mathit{fold}})\mathbf{x}^*$。–

  否 情形：$\mathbf{z}(t) \sim \mathcal{U}_{\mathbb{Z}_2^{\alpha n}}$。
- *Alice* 可以向 Bob_1发送一条消息；每个 Bob_t 可以向 Bob_{t+1}发送一条消息；最后，Bob_T 必须判断他们属于是情形还是否 情形。

sBPD 是一种“折中方案”，使我们既可以从 BPD 进行归约，也可以归约到最大割。事实上，我们有：

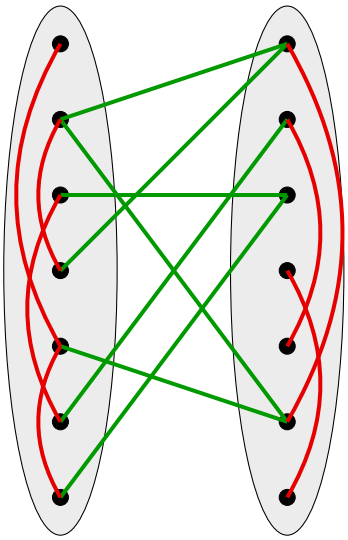
引理 3.5。 设 $\alpha, \delta \in (0, 1)$ 以及 $T, n, s \in \mathbb{N}$。假设存在一个针对 $\mathit{sBPD}_{\alpha,T}(n)$的协议，能够达到优势 δ，并使用 s 通信量。那么存在一个针对 $\mathit{BPD}_\alpha(n)$ 的协议，能够达到至少 $\frac{\delta}{T}$ 的优势，并使用 s 通信量。

我们在下文§3.3 中证明引理 3.5，采用Kapralov、Khanna 和 Sudan 的 [KKS15]混合论证。我们还有：

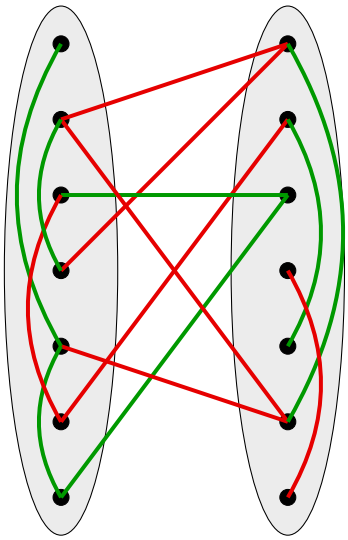
构造 3.6 （从sBPD 到最大割的 C2S 归约）。 *Alice* 的归约函数（记作 R_0,）不输出任何约束。对于每个 $t \in [T]$，*Bob* 的归约函数 R_t 按如下方式输出一个实例 Ψ_t：对于 M_t 中的每个 $\mathbf{e}(t, \ell) = (u, v)$，若 $z(t)_\ell = 1$，则 *Bob* 将 $\mathbf{e}(t, \ell)$ 加入 Ψ_t。

用于最大割 的困难实例由构造 3.6 生成，并以图示形式呈现在图 3.1中。

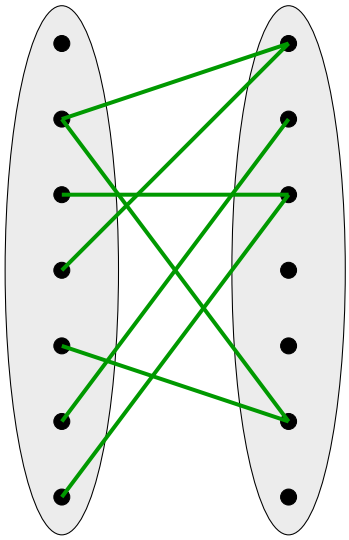
引理 3.7。 对于所有 $\alpha \in (0, 1)$ 以及 $\epsilon \in (0, \frac{1}{2})$，存在 $T, n_0 \in \mathbb{N}$，使得对于每个 $n \geq n_0$，以下结论成立。令 $\mathcal{Y}$ 和 $\mathcal{N}$ 分别表示是分布和否分布，用于



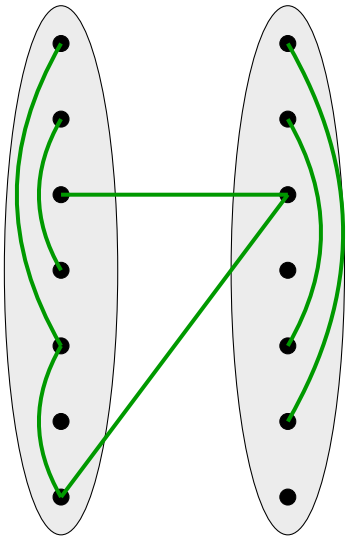
(a) 是情形来自 sBPD 的样本。



(b) 否情形来自 sBPD 的样本。



(c) 是情形的最大割实例。



(d) 否情形的最大割实例。

图 3.1：最大割的困难实例示例。图 3.1a 和图 3.1b 分别展示了来自 sBPD 的是分布和否分布的样本。回顾一下，在 sBPD 中，Alice 收到一个隐藏划分 $\mathbf{x}^* \in \mathbb{Z}_2^n$，而每个 Bob$_t$ 收到一个匹配 M_t，以及一个向量 $\mathbf{z}(t)$，用于标记 M_t 的边。在是情形中，$\mathbf{z}(t)$ 标记 M_t 中跨越划分 $\mathbf{x}^*$ 的边；而在否情形中，$\mathbf{z}(t)$ 是均匀随机的。图 3.1a 和图 3.1b 中的图表示匹配 $M_1, \ldots, M_t$ 的并集；$\mathbf{x}^*$ 将顶点划分为“左”（0）和“右”（1）；边的 z 值则为“绿色”（1）或“红色”（0）。在我们从 sBPD 到最大割的归约（构造 3.6）中，Alice 不添加任何边，而每个 Bob$_t$ 添加所有 z 值为“绿色”（1）的边。在是情形中，所得图是二部图（图 3.1c），因此最大割值为 1；而在否情形中，该图是随机的（图 3.1d），并且以高概率其值为 $\approx \frac{1}{2}$（当 T 足够大时）。

$sBPD_{\alpha,\ T}$（n），并令（R_0，……，R_T）为来自构造 3.6的归约函数。则

$$\Pr_{\Psi\sim(R_0,\ldots,R_T)\circ\mathcal{Y}}[val_\Psi = 1] = 1 \ and \ \Pr_{\Psi\sim(R_0,\ldots,R_T)\circ\mathcal{N}}\left[val_\Psi \geq \frac{1}{2}+\epsilon\right] \leq \exp(-n).$$

注意，引理 3.7 可能迫使我们令 T 非常大；但它是常数，此时引理 3.5 给出BPD的一个虽小但为常数的优势。幸运的是，定理 3.3 排除了所有针对BPD的常数优势。

作为本节的总结，我们给出定理 3.1和引理 3.7的证明。

定理 *3.1* 的证明。考虑任意 $\epsilon > 0$，令 $\tau > 0$ 稍后确定，并令Alg 为一个随机化的、空间为$s(n)$的流式算法，它对$\frac{1}{2}+\epsilon$-近似最大割。根据引理 3.7，我们可以选取足够大的 T，$n_0 \in \mathbb{N}$ 使得对任意固定的 $n \geq n_0$，都有

$$\Pr_{\Psi\sim(\mathsf{R}_0,\ldots,\mathsf{R}_T)\circ\mathcal{Y}}[\mathsf{val}_\Psi = 1] = 1 \text{ and } \Pr_{\Psi\sim(\mathsf{R}_0,\ldots,\mathsf{R}_T)\circ\mathcal{N}}\left[\mathsf{val}_\Psi \geq \frac{1}{2}+\frac{\epsilon}{2}\right] \leq \exp(-n)$$

其中，$\mathcal{Y}$、$\mathcal{N}$分别是 $\mathsf{sBPD}_{\alpha,T}(n)$ 的是分布和否分布，而 $(\mathsf{R}0,\ldots,\mathsf{R}_T)$ 与构造 3.6 中的相同。由于 Alg 求解了 $(1, 1-\epsilon/2)$-最大割问题，根据命题 2.8，存在一个确定性空间-$s(n)$流式算法，能够区分 $(\mathsf{R}0,\ldots,\mathsf{R}_T)\circ\mathcal{Y}$ 和 $(\mathsf{R}0,\ldots,\mathsf{R}_T)\circ\mathcal{N}$，且优势至少为 1 6。根据引理 2.9，存在一个针对 $\mathsf{sBPD}_{\alpha,T}(n)$ 的确定性空间-$s(n)$ 通信协议，其优势至少为 1 6。根据引理 3.5，存在一个针对 $\mathsf{BPD}_\alpha(n)$ 的确定性空间-$s(n)$ 通信协议，其优势至少为 $\frac{-1}{6T}$。最后，根据定理 3.3，存在某个 $\tau > 0$ 和 $n_0' \in \mathbb{N}$，使得在进一步假设 $n \geq n_0'$的情况下，我们可以得出 $s(n) \geq \tau\sqrt{n}$，如所需。

□

引理 *3.7* 的证明略述。设 $\Psi = \Psi_1 \cup \cdots \cup \Psi_T$为归约所构造的实例。在 **是** 情况下，无论 T 如何，我们总有 $\mathsf{val}_\Psi(\mathbf{x}^*) = 1$，因为 Ψ 中的每个约束 $(u,\ v)$ 都是按照 $x_u^* + x_v^* = 1$来选取的。

对于 **否** 的情况，只需证明对于每个固定的赋值 $\mathbf{x} \in \mathbb{Z}_2^n$，

$$\Pr\left[\mathsf{val}_\Psi(\mathbf{x}) \geq \frac{1}{2}+\epsilon\right] \leq \exp(-\epsilon^2\alpha T n), \tag{3.8}$$

因此，我们可以对 $\mathbf{x}$ 取并集界，并令 T 足够大。在“更理想”的模型中，Ψ 具有 $\alpha T n$ 个均匀随机选取的约束，方程 (3.8) 将可由此推出

这可直接由切尔诺夫界推出，因为$\mathbf{x}$ 将以$_1$ $_2$的概率独立地满足每个 αTn 约束。遗憾的是，这里存在两个问题：-

1. 由于$\mathbf{z}(t)$是均匀随机的，Bob_t 仅以概率$_1$ $_2$ （相互独立地）将 M_t 中的每条边添加为 Ψ_t 中的一个约束。因此，每个子实例 Ψ_t 中的约束数量服从二项分布。特别地，中的约束数量不是常数。

2. 每个 M_t 都是一个随机匹配，因此其中的边并不独立。因此， Ψ的约束并不独立，尽管如果$t \neq t'$， Ψ_t 和 $\Psi_{t'}$ 的约束是相互独立的。

问题（1）可以通过将每个 Ψ_t 中的约束数量视为随机变量并进行条件化来解决。具体而言，我们对每个 $t \in [T]$ 定义 β_t 定义为$=$ $^{m(\Psi_t)}$ $_n$ ，并定义β 定义为$=m(\ \Psi\ _{Tn}) = \frac{1}{T}\sum_{t=1}^{T}\beta_t$ $\mathbb{E}[\beta_1] = \cdots = \mathbb{E}[\beta_T] = \mathbb{E}[\beta] = \frac{\alpha}{2}$，然后对固定值 β_1、.....、β_T进行条件化。这样，我们就可以将每个 Ψ_t的约束视为从 $\mathcal{M}_{\beta_t}(n)$中抽取的随机匹配的边。

现在，假设我们定义随机变量 $\{X_{t,\ell}\}_{t\in[T],\ \ell\in[\beta_t n]}$，它们各自是指示变量，表示 $\mathbf{x}$ 满足 Ψ_t 的第 ℓ 个约束这一事件。我们有 $\mathrm{val}_\Psi(\mathbf{x}) = \frac{1}{\beta Tn}\sum_{t=1}^{T}\sum_{\ell=1}^{\beta_t n} X_{t,\ell}$。由于问题(2)，我们不能对 $\mathrm{val}_\Psi(\mathbf{x})$ 使用切尔诺夫界，但可以使用引理 2.5。对于 $t \neq t'$, $X_{t,\ell}$ 和 $X_{t',\ell'}$ 将相互独立；尽管 $X_{t,\ell}$ 与$X_{t,1}, \ldots, X_{t,\ell-1}$不独立，但我们有 $\mathbb{E}[X_{t,\ell} \mid X_{t,1}, \ldots, X_{t,\ell-1}] \leq \frac{1}{2}$。实际上， Ψ_t 中第 ℓ 个约束是从一个集合中均匀抽样得到的，该集合包含所有与前 $\ell - 1$ 个约束不共享变量的约束，而其中至多一半能被 $\mathbf{x}$ 满足。

（还有一个小问题：引理 引理 2.5 给出的概率界在 βTn中会呈指数级小，而不是 αTn。但根据切尔诺夫界，不失一般性，我们可以假设，例如，$\beta \geq \frac{\alpha}{4}$。这会额外产生一个并集界项，该项在$\alpha n$中呈指数级小。）

□

3.2 BPD is hard: Proving Theorem 3.3

本节的目标是证明定理 3.3，该定理由 Gavinsky、Kempe、Kerenidis、Raz 和 de Wolf [GKK+08]提出，指出BPD 需要大量通信。

令 $\mathcal{U}$ 定义$=$ $\mathcal{U}_{\mathbb{Z}_2^{\alpha n}}$。首先，假设 Alice 使用确定性协议向 Bob 发送某条固定消息 $a \in \{0,1\}^s$ ，并令 $A \subseteq \mathbb{Z}_2^n$ 为与该消息相一致的$\mathbf{x}^*$的集合

消息。对于每个匹配 $M \in \{0,1\}^{2\alpha n \times n}$，我们考虑在**是** 情况下 Bob 的第二个输入$\mathbf{z} \in \mathbb{Z}_2^{\alpha n}$的条件分布：

$$\mathcal{Z}_{A,M}(\mathbf{z}) \stackrel{\text{def}}{=} \Pr_{\mathbf{x}^* \sim \mathcal{U}_A}[\mathbf{z} = (M^{\mathsf{fold}})\mathbf{x}^*].$$

我们通过证明定理 3.3来说明：如果 A 足够大（当通信 s 足够小时，以高概率会是如此），那么对 M而言，以高概率，分布$\mathcal{Z}_{A,M}$ 在统计上接近 $\mathcal{U}$，因此 Bob 无法区分**是**和**否**两种情况。为此，我们关键地依赖以下"归约"：

引理 3.9（傅里叶分析归约）。设 $A \subseteq \mathbb{Z}_2^n$ 和 $\mathbb{1}_A : \mathbb{Z}_2^n \to \{0,1\}$ 是 A的指示变量，并设 $\alpha \in (0,1)$。那么

$$\mathop{\mathbb{E}}_{M \sim \mathcal{M}_\alpha(n)}[\|\mathcal{Z}_{A,M} - \mathcal{U}\|_{\text{tv}}^2] \leq \frac{2^{2n}}{|A|^2} \sum_{\ell \geq 2}^{2\alpha n} h_\alpha(\ell, n) \mathsf{W}^\ell[\mathbb{1}_A]$$

其中，对于 $\ell \in [n]$,

$$h_\alpha(\ell, n) \stackrel{\text{def}}{=} \max_{\mathbf{v} \in \mathbb{Z}_2^n, \|\mathbf{v}\|_0 = \ell} \left(\Pr_{M \sim \mathcal{M}_\alpha(n)} \left[\exists \mathbf{s} \neq \mathbf{0} \in \mathbb{Z}_2^{\alpha n} \ s.t. \ (M^{\mathsf{fold}})^\top \mathbf{s} = \mathbf{v} \right] \right).$$

为理解 $h_\alpha(\ell, n)$的定义，我们可以将$\mathbf{s}$ 视为用 1"标记"匹配 M 中的某些边；那么向量 $(M^{\mathsf{fold}})^\top \mathbf{s}$ 便标记了哪些顶点与被标记的边相接。

要对引理 3.9中的总和进行界定，我们在较小和较大的两种情况下分别采用两个不等式。在较小的情况下，我们应用引理 2.4；在较大的情况下，我们应用以下界：

引理 3.10 (h 的组合界)。 设 $h_\alpha(\ell, n)$ 定义如引理 *3.9*所示。对于每个 $\alpha \in (0,1)$中的 n, $\ell \in \mathbb{N}$ 以及任意偶数 $\ell \leq n/2$，都有

$$h_\alpha(\ell, n) = \frac{\binom{\alpha n}{k/2}}{\binom{n}{\ell}} \leq \left(\frac{2\alpha e \ell}{n} \right)^{\ell/2}.$$

对于奇数 ℓ, $h_\alpha(\ell, n) = 0$。

在证明 引理 3.9 和 3.10之前，我们先说明它们如何足以证明 定理 3.3。

证明 *定理 3.3*。 假设 Alice 和 Bob 使用一个用于 BPD_α 的单向通信协议 Prot，该协议至多使用 $s = \tau\sqrt{n}$ 通信，并取得优势 δ，其中τ 是稍后确定的常数。从 Bob 的角度来看，Alice 发送的消息将所有可能的 $\mathbf{x}^*$ 划分为若干集合 $\{A_i \subseteq \mathbb{Z}_2^n\}_{i\in[2^s]}$。在给定集合 $A \subseteq \mathbb{Z}_n^2$ 的条件下，对于随机 $M \sim \mathcal{M}_\alpha(n)$，Prot 正在区分分布 $\mathcal{Z}_{A,M}$ 和 $\mathcal{U}$，因此其取得的优势至多为 $\delta_A \overset{\text{定义为}}{=} \mathbb{E}_{M\sim\mathcal{M}_\alpha(n)}[\|\mathcal{Z}_{A,M} - \mathcal{U}\|_{\mathrm{tv}}]$。令 $\mathcal{A}$ 表示以概率 $|A_i|/2^n$ 对每个 A_i 进行采样的分布，我们有

$$\delta \le \mathop{\mathbb{E}}_{A\sim\mathcal{A}}[\delta_A]. \tag{3.11}$$

我们的目标是，在 式 (3.11) 中选取足够小的 τ，从而得到矛盾。我们令$\tau = 2\tau'$，其中 $\tau' > 0$将在稍后确定，并令 $s' = \tau'\sqrt{n}$。

一个“典型的” $A \sim \mathcal{A}$很大，因此要与式 (3.11)矛盾，只需证明δ_A 在 A足够大时很小。事实上，由于 $s' < s - \log(2/\delta)$（当 n足够大时），我们有 $\Pr_{A\sim\mathcal{A}}[|A| \le 2^{n-s'}] \le \frac{\delta}{2}$，因此只需证明：若 $|A| \ge 2^{n-s'}$，则 $\delta_A \le \frac{\delta}{2}$。

设 $A \subseteq \mathbb{Z}_2^n$ 且 $|A| \ge 2^{n-s'}$。根据詹森不等式，

$$\delta_A \le \sqrt{\mathop{\mathbb{E}}_{M\sim\mathcal{M}_\alpha(n)}[\|\mathcal{Z}_{A,M} - \mathcal{U}\|_{\mathrm{tv}}^2]}. \tag{3.12}$$

现在我们应用引理 3.9:

$$\mathop{\mathbb{E}}_{M\sim\mathcal{M}_\alpha(n)}[\|\mathcal{Z}_{A,M} - \mathcal{U}\|_{\mathrm{tv}}^2] \le \frac{2^{2n}}{|A|^2}\sum_{\ell=2}^{2\alpha n} h_\alpha(\ell,n)\mathsf{W}^\ell[\mathbb{1}_A].$$

我们在 $\ell = 4s'$ 处分割求和，第一项使用 引理 2.4，第二项使用 命题 2.3：

$$\begin{aligned}
&= \frac{2^{2n}}{|A|^2}\sum_{\ell=2}^{4s'} h_\alpha(\ell,n)\mathsf{W}^\ell[\mathbb{1}_A] + \frac{2^{2n}}{|A|^2}\sum_{\ell=4s'}^{2\alpha n} h_\alpha(\ell,n)\mathsf{W}^\ell[\mathbb{1}_A] \\
&\le \sum_{\ell=2}^{4s'} h_\alpha(\ell,n)\left(\frac{\zeta s'}{\ell}\right)^\ell + \frac{2^{2n}}{|A|^2}\max_{4s'\le\ell\le 2\alpha n} h_\alpha(\ell,n).
\end{aligned} \tag{3.13}$$

应用 引理 3.10 和不等式 $|A| \geq 2^{n-s'}$:

$$\leq \sum_{\text{even } \ell=2}^{4s'} \left(\frac{2\alpha e(\zeta s')^2}{\ell n}\right)^{\ell/2} + \left(\frac{16\alpha e s'}{n}\right)^{2s'}.$$

最后，我们利用不等式 $\binom{s'}{n} \leq \left(\frac{(s')}{n}\right)^2 = (\tau')^2$, $\ell \geq 2$, $2s' \geq 1$ ，并用几何级数给出上界:

$$\begin{aligned}
&\leq \sum_{\text{even } \ell=2}^{4s'} \left(\tau'\zeta\sqrt{\alpha e}\right)^{\ell} + 16\alpha e(\tau')^2 \\
&\leq \sum_{\text{even } \ell=2}^{\infty} \left(\tau'\zeta\sqrt{\alpha e}\right)^{\ell} + 16\alpha e(\tau')^2 \\
&= \frac{\alpha e(\tau'\zeta)^2}{1-\alpha e(\tau'\zeta)^2} + 16\alpha e(\tau')^2.
\end{aligned}$$

不失一般性地假设 $\alpha e(\tau'\zeta)^2 \leq \frac{1}{2}$，方程 (3.12) 于是给出 $\delta_A \leq \overline{\tau'\sqrt{4\zeta}}^2 + 8$，从而当 $\delta_A \leq \frac{\delta}{2}$足够小时，取 $\tau' = \Theta(\delta$即可得到所需结论。 □

注释 3.14。 在方程 (3.13)中，“低阶ℓ 项”在定性上最为重要；它们体现了 n 的幂之间的“平衡”，介于低阶傅里叶权重界（引理 *2.4*）与随机图分析（引理 *3.10*）之间。特别地，对于$\ell \in \{2, \ldots, 4s'\}$，我们得到形如 $h_\alpha(\ell, n)\binom{\zeta s'}{\ell}^{\ell}$的项，它们由 $\left(O\left(\frac{(s')}{\ell n}^2\right)\right)^{\ell/2}$ 根据引理 *3.10*给出上界。即使例如 $\ell = 2$，只要 $s = \omega(\sqrt{n})$，该项仍为超常数。

现在我们证明引理 3.9和3.10。

引理 *3.9* 的证明。 令 $M \in \{0,1\}^{2\alpha n \times n}$为一个固定的匹配。对于固定的 $\mathbf{s} \neq \mathbf{0} \in \{0,1\}^{\alpha n}$，我们有

$$\begin{aligned}
\widehat{\mathcal{Z}_{A,M}}(\mathbf{s}) &= \frac{1}{2^{\alpha n}} \sum_{\mathbf{z} \in \mathbb{Z}_2^{\alpha n}} (-1)^{-\mathbf{s}\cdot\mathbf{z}}\, \mathcal{Z}_{A,M}(\mathbf{z}) && \text{(definition of } \widehat{\mathcal{Z}_{A,M}}) \\
&= \frac{1}{2^{\alpha n}} \sum_{\mathbf{z} \in \mathbb{Z}_2^{\alpha n}} (-1)^{\mathbf{s}\cdot\mathbf{z}} \left(\mathop{\mathbb{E}}_{\mathbf{x}^* \sim \mathcal{U}_A} \left[\mathbb{1}_{\mathbf{z}=(M^{\mathsf{fold}})\mathbf{x}^*}\right]\right) && \text{(definition of } \mathcal{Z}_{A,M})
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2^{\alpha n}} \mathop{\mathbb{E}}_{\mathbf{x}^* \sim \mathcal{U}_A} \left[(-1)^{-\mathbf{s} \cdot ((M^{\mathsf{fold}})\mathbf{x}^*)} \right] && \text{(linearity of expectation)} \\
&= \frac{1}{2^{\alpha n}} \mathop{\mathbb{E}}_{\mathbf{x}^* \sim \mathcal{U}_A} \left[(-1)^{-((M^{\mathsf{fold}})^\top \mathbf{s}) \cdot \mathbf{x}^*} \right] && \text{(adjointness)} \\
&= \frac{2^n}{2^{\alpha n}|A|} \widehat{\mathbb{1}_A}((M^{\mathsf{fold}})^\top \mathbf{s}). && \text{(definition of } \widehat{\mathbb{1}_A}\text{)}
\end{aligned}
$$

结合 引理 2.10，可得

$$
\|\mathcal{Z}_{A,M} - \mathcal{U}\|_{\mathrm{tv}}^2 \le \frac{2^{2n}}{|A|^2} \sum_{\mathbf{s} \neq \mathbf{0} \in \mathbb{Z}_2^{\alpha n}} \widehat{\mathbb{1}_A}((M^{\mathsf{fold}})^\top \mathbf{s}).
$$

最后，我们注意到 $(M^{\mathsf{fold}})^\top$ 是一个单射，因为每一行至多有一个 $\mathbf{1}$（因为 M 是一个匹配）。因此，对 M取期望可得

$$
\mathop{\mathbb{E}}_{M}[\|\mathcal{Z}_{A,M} - \mathcal{U}\|_{\mathrm{tv}}^2] \le \frac{2^{2n}}{|A|^2} \sum_{\mathbf{v} \neq \mathbf{0} \in \mathbb{Z}_2^n} \widehat{\mathbb{1}_A}(\mathbf{v}) \left(\Pr_M[\exists \mathbf{s} \neq \mathbf{0} \in \mathbb{Z}_2^{\alpha n} \text{ s.t. } (M^{\mathsf{fold}})^\top \mathbf{s} = \mathbf{v}] \right),
$$

从而证明了该引理。 □

引理 *3.10*的证明。 设$\mathbf{z} \in \mathbb{Z}_2^n$ 和 M 是一个 α-部分匹配，它定义在 $[n]$上。向量$\mathbf{s} \neq \mathbf{0} \in \mathbb{Z}_2^n$ 满足 $(M^{\mathsf{fold}})^\top \mathbf{s} = \mathbf{v}$ 标记了 M 的边，使得 $\mathbf{v}$ 标记了与被标记边关联的顶点。因此，当且仅当 $\mathbf{v}$ 中的每对顶点都由 M中的一条边相连时，这样的向量才存在。

对顶点进行均匀重标记后，固定匹配 M 会变成均匀匹配。因此，不妨固定 M，使边为 $\{(1, 2), (3, 4) \ldots, (2\alpha n - 1, 2\alpha n)\}$，并令 $\mathbf{v}$ 在 $\mathbb{Z}_2^n$ 中所有汉明重量为 ℓ 的向量中均匀分布。仅当$\mathbf{v}$ 完全支撑在 $[2\alpha n]$ 上，且每当$\mathbf{v}$ 支撑在 $2i - 1$ 上时，它也支撑在 $2i$ 上，反之亦然，$\mathbf{s}$ 才存在。$\mathbf{v}$总共有 $\binom{n}{\ell}$ 种可能，但在 $2\alpha n - 1$ 内，为$\mathbf{v}$在奇数顶点上选择支撑集只有 $\binom{\alpha n}{\ell/2}$ 种方式。因此，

$$
h_\alpha(\ell, n) = \frac{\binom{\alpha n}{\ell/2}}{\binom{n}{\ell}},
$$

正如所需。[§]

最后，利用不等式 $\binom{a}{b}^b \le \binom{a}{b} \le \binom{ea}{b}^b$，我们有

$$\frac{\binom{\alpha n}{\ell/2}}{\binom{n}{\ell}} \le \frac{\left(\frac{e\alpha n}{\ell/2}\right)^{\ell/2}}{\left(\frac{n}{\ell}\right)^{\ell}} = (2\alpha e)^{\ell/2}\left(\frac{\ell}{n}\right)^{\ell/2},$$

正如所需。 □

3.3 The hybrid argument: Proving Lemma 3.5

为了将 $\mathsf{sBPD}_{\alpha,\ \tau}(n)$ 归约为 $\mathsf{BPD}_{\alpha}(n)$（并证明引理 3.5），我们采用一种标准的混合论证，该方法由 Kapralov、Khanna 和 Sudan [KKS15] 在此背景下提出。直观而言，在 $\mathsf{sBPD}_{\alpha,\ \tau}(n)$ 中，每个 Bob_t 都必须解决自己的 $\mathsf{BPD}_{\alpha}(n)$ 实例（尽管他会得到 Bob_1、……、Bob_{t-1} 的“帮助”）。因此，在我们的证明中，我们使用三角不等式来说明，这些 Bob_t 中必有一人“做得还不错”，能够解决自己的 $\mathsf{BPD}_{\alpha}(n)$ 实例；然后，我们通过模拟 Bob_1、……、Bob_{t-1} 的“帮助”，将其转化为一个适用于 $\mathsf{BPD}_{\alpha}(n)$ 的通用算法。

引理 3.5 的证明。 设 Prot 是一个针对 $\mathsf{sBPD}_{\alpha,\ \tau}(n)$ 的空间-s 协议，由消息函数 Prot_0、……、Prot_t 给出，其中 Alice 的消息由函数 Prot_0, 确定，该函数以 $\mathbf{x}^* \in \mathbb{Z}_2^n$ 为输入；Bob_t 的消息则由函数 Prot_t 确定，该函数以 $(m_{t-1}、\ M_t、\ \mathbf{z}(t)) \in \{0,1\}^s \times \{0,1\}^{\alpha n \times n} \times \mathbb{Z}_2^{\alpha n}$ 为输入。

现在，我们考虑“耦合”实验：先对 Alice 的输入进行采样，然后考察在**是**和**否**两种情况下 Bob 的行为。令 $S_0^{\mathbf{Y}} = S_0^{\mathbf{N}}$定义为$= \mathsf{Prot}_0(\mathcal{U}_{\mathbb{Z}_2^n})$ 表示 Alice 的输出（作为一个随机变量）。于是，对于 $t \in [T]$，定义

$$S_t^{\mathbf{Y}} \stackrel{\text{def}}{=} \mathsf{Prot}_t(S_{t-1}^{\mathbf{Y}}, M_t, (M^{\mathsf{fold}})^\top \mathbf{x}^*) \text{ and } S_t^{\mathbf{N}} \stackrel{\text{def}}{=} \mathsf{Prot}_t(S_{t-1}^{\mathbf{N}}, M_t, \mathcal{U}_{\mathbb{Z}_2^{\alpha n}}) \in \Delta(\{0,1\}^s)$$

[§]Gavinsky等人 [GKK+08] 的原始证明采用了不同的论证，得出了相同的答案。考虑一个固定的向量 $\mathbf{v}$，不失一般性，$1^\ell 0^{n-\ell}$，以及一个随机匹配 M。当且仅当 M 是 $[\ell]$ 上的一个完美匹配与 $[n] \setminus [\ell]$上的一个（$\alpha - \frac{\ell}{2n}$）-部分匹配的不相交并时，$_n$ 才存在。令$m_{\alpha,n}$ 表示 n 个顶点上α-部分匹配的数量。那么可以证明

$$m_{\alpha,n} = \frac{n!}{2^{\alpha n}(\alpha n)!(n-2\alpha n)!} \quad \text{and therefore} \quad \frac{m_{1,\ell} \cdot m_{\alpha - \frac{\ell}{2n}, n-\ell}}{m_{\alpha,n}} = \frac{\binom{\alpha n}{\ell/2}}{\binom{n}{\ell}}.$$

分别作为 Bob 在**是**和**否**情形下输出的消息。由于 Prot 能以 δ的优势区分**是**和**否**分布，因此我们有

$$\|S_T^{\mathbf{Y}} - S_T^{\mathbf{N}}\|_{\mathrm{tv}} \geq \delta.$$

根据三角不等式（引理 2.6），存在 $t \in [T]$ 使得

$$\|S_t^{\mathbf{Y}} - S_t^{\mathbf{N}}\|_{\mathrm{tv}} - \|S_{t-1}^{\mathbf{Y}} - S_{t-1}^{\mathbf{N}}\|_{\mathrm{tv}} \geq \frac{\delta}{T}. \tag{3.15}$$

现在，令 $\widetilde{S} \overset{\text{定义}}{=} \mathsf{Prot}_t(S_{t-1}^{\mathbf{Y}}, M_t, \mathcal{U}_{\mathbb{Z}_2^{an}})$，即 $\widetilde{S}$是 Bob_t在以下混合 实验中的输出消息：Bob_1，……，Bob_{t-1} 接收 **是** 输入，而 Bob_t 接收一个**否** 输入。根据三角不等式，

$$\|S_t^{\mathbf{Y}} - \widetilde{S}\|_{\mathrm{tv}} \geq \|S_t^{\mathbf{Y}} - S_t^{\mathbf{N}}\|_{\mathrm{tv}} - \|S_t^{\mathbf{N}} - \widetilde{S}\|_{\mathrm{tv}}. \tag{3.16}$$

注意，$S_t^{\mathbf{N}} = \mathsf{Prot}_t(S_{t-1}^{\mathbf{N}}, M_t, \mathcal{U}_{\mathbb{Z}_2^{an}})$和 $S = \mathsf{Prot}_t(S_{t-1}^{\mathbf{Y}}, M_t, \mathcal{U}_{\mathbb{Z}_2^{an}})$。（也就是说，在这两个实验中，$\mathsf{Bob}_t$ 接收一个从否分布中采样的输入，而 Bob1，……，Bob_{t-1}分别接收来自否分布和是分布的输入。）在这两种情况下，Bob_t的否输入（$M_t, \mathcal{U}_{\mathbb{Z}_2^{an}}$）都与 $S_{t-1}^{\mathbf{N}}$ 和 $S_{t-1}^{\mathbf{Y}}$独立。因此，根据数据处理不等式（引理 2.7），我们有：

$$\|S_t^{\mathbf{N}} - \widetilde{S}\|_{\mathrm{tv}} \leq \|S_{t-1}^{\mathbf{Y}} - S_{t-1}^{\mathbf{N}}\|_{\mathrm{tv}}. \tag{3.17}$$

将式 (3.15) 至 (3.17) 合并可得

$$\|S_t^{\mathbf{Y}} - \widetilde{S}\|_{\mathrm{tv}} \geq \frac{\delta}{T}.$$

但是 $\widetilde{S} = \mathsf{Prot}_t(S_{t-1}^{\mathbf{Y}}, M_t, \mathcal{U}_{\mathbb{Z}_2^{an}})$ 和 $S_t^{\mathbf{Y}} = \mathsf{Prot}_t(S_{t-1}^{\mathbf{Y}}, M_t, (M_t^{\mathsf{fold}})\mathbf{x}^*)$。（也就是说，在这两个实验中，$\mathsf{Bob}_1$、……、$\mathsf{Bob}_{t-1}$ 接收从是分布中采样的输入，而 Bob_t 分别接收来自否分布和是分布的输入。）这给出了一个实现优势 $\frac{\delta}{T}$ 的 BPD 算法：Alice 可以为 Bob_1、……、Bob_{t-1}模拟是输入，然后将 Bob_{t-1}的消息发送给 Bob，后者可以以优势区分 $S_t^{\mathbf{Y}}$ 和 S

$\sim \|S_t^{\mathbf{Y}} - S\|_{\mathrm{tv}}$.

¶ □

3.4 Discussion

我们在本章最后讨论定理 3.1证明的一些关键特征，这些特征将在本文余下部分中发挥作用。

3.4.1 Strengths of the model

我们证明了定理 3.1 通过从 sBPD 到 最大割的归约得出。该下界针对“流式算法”成立，但我们究竟需要这些算法具备哪些性质？我们不对其一致性或时间复杂度作任何假设。我们确实假设$O(\sqrt{n})$ 空间，但实际上只有在每位参与者将算法状态传递给下一位参与者时，才会用到这一假设。此外，这些实例的次数为常数度，也就是说，每个变量至多出现在 $O(1)$ 个约束中。事实上，Ψ 是 $T = O(1)$ 个子实例的并集，$\Psi_1 \cup \cdots \cup \Psi_T$而每个 Ψ_t 都对应一个匹配，因此每个变量的次数至多为 T。因此，这些下界实际上在一个更强的模型中也成立：在该模型中，流式算法可以将输入实例分成 $O(1)$ 个“等间隔的数据块”进行处理，并且保证实例具有常数度。

3.4.2 Weaknesses of the model: Input ordering

然而，下界及迄今用于证明这些下界的技术也存在若干不足。首先，我们关注对抗性排序的输入流这一假设。归约（构造 3.6）生成的实例并非随机排序。事实上，回想一下，在构造 3.6中，Alice不添加任何约束，而每个Bob$_t$ 都会添加一个子实例 Ψ_t，该子实例对应一个随机匹配。因此，实例 $\Psi = \Psi_1 \cup \cdots \cup \Psi_t$具有这样的性质：在对应于 αn 的每个约束块中 Ψ_t，变量都不会重复；如果我们随机重排这些约束，这种情况就不太可能发生。幸运的是，Kapralov、Khanna 和 Sudan [KKS15]通过考虑一种基于 Erd˝os-R´enyi 图（即 $\mathcal{G}_\alpha(n)$）的 BPD 变体，而非随机匹配，解决了这一问题

¶具体而言，Bob 应根据 Bob$_t$ 的输出消息在 $S_{\mathbf{Y}t}$ 或 $\widetilde{S}$ 中出现的概率哪个更高，分别输出 **是** 或 **否** 。

（即 $\mathcal{M}_\alpha(n)$）。[‖] 这一改动使困难性的证明略微复杂；具体来说，在傅里叶分析归约（即引理 3.9）中，$(M^{\mathsf{fold}})^\top$ 不再是单射，因此 $h_\alpha(\ell, n)$ 必须重新定义为

$$\max_{\mathbf{v}\in\mathbb{Z}_2^n, \|\mathbf{v}\|_0=\ell} \left(\mathop{\mathbb{E}}_{M\sim\mathcal{G}_\alpha(n)} \left[\left| \left\{ \mathbf{s} \in \mathbb{Z}_2^{\alpha n} : \mathbf{s} \neq \mathbf{0}, (M^{\mathsf{fold}})^\top \mathbf{s} = \mathbf{v} \right\} \right| \right] \right).$$

相应地，关于 $h_\alpha(\ell,\ n)$ 的界（参见 引理 3.10）会变得稍微复杂一些，但最终证明仍然成立。

3.4.3 Weaknesses of the model: Space bound

此外，还存在一个问题：如何将最大割困难性的空间界扩展到$o(\sqrt{n})$之外。如上文注释 3.14所述，[GKK+08] 对 BPD 困难性的证明（定理 3.3）仅适用于 $\sqrt{n}$-空间协议。但 $\sqrt{n}$ 依赖性并非只是这一证明的产物。事实上，定理 3.3在以下意义下是紧的：对于任意 α, $\delta \in (0, 1)$，存在一个针对 $\mathrm{BPD}_\alpha(n)$ 的协议，能以 $O(\sqrt{n})$通信量达到优势 δ。事实上，Alice 只需从集合 $S \subseteq [n]$ 中均匀抽取大小为 $\widetilde{n}$ 的子集（具体大小稍后确定），并将x_s 发送给 Bob（对每个 $s \in S$）。令 $\widetilde{m}$ 表示 Bob 的匹配中，两个端点都属于 S的边数。在是情形下，Bob 的输入 z 总是会在这些边上与他从 Alice 收到的信息相符；而在否情形下，它们全部相符的概率仅为 $2^{-\widetilde{m}}$。此外，根据期望的线性性，$\mathbb{E}[\widetilde{m}] \approx \frac{\alpha\widetilde{n}^2}{n}$，因此（利用集中界，以高概率）$\widetilde{m}$ 可以随着 $\widetilde{n} = O(\sqrt{n})$的任意增大而成为任意大的常数。（$\widetilde{n} = O(\sqrt{n})$是为期望在诱导子图中看到边而应抽取的顶点数，[GKK+08]称这一事实为“生日悖论”的一个例子。）因此，Bob 可以区分是与否情形。由于该协议也适用于 sBPD，这意味着，无法通过从 sBPD 问题进行归约来得到更好的最大割空间下界。

为了解决这一问题，Kapralov、Khanna、Sudan 和 Velingker [KKSV17] 提出了一种隐式变体sBPD，我们将其记为siBPD。在siBPD 问题中，与

[‖]注意，从 $\mathcal{G}_\alpha(n$ 中采样的图都是简单图，因此这些实例仍然具有这样的性质：每个“块”中都没有重复的 约束。不过，由于只有 $O(1)$ 个块，在随机重新排列约束后，这一性质仍很可能成立；参见 [KKS15, 引理 4。7]。

sBPD不同，没有任何一方会将隐藏划分作为输入（也就是说，不存在Alice）。基于[KKSV17], Kapralov 和 Krachun [KK19]证明了以下结论：

定理 3.18 ([KK19])。对于 $\alpha, \delta \in (0,1)$ 和 $T \in \mathbb{N}$，存在一个 $n_0 \in \mathbb{N}$，使得对于所有 $n \geq n_0$，任何在 $siBPD_{\alpha,T}(n)$ 中达到至少 δ 优势的协议，都需要$\Omega(n)$ 通信。

[KK19] 证明 定理 3.18 及其在 [CGS+22] 中的推广在技术上都非常复杂；简要说明请参见 §5.2末尾的讨论。

回想一下，在 构造 3.6中，Alice没有贡献任何约束，因此 构造 3.6 完全可以看作是从 siBPD 而非 sBPD 归约到 最大割。因此，定理 3.18 立即将 最大割的困难性推广到了线性空间情形。也就是说，任何一个 $(\frac{1}{2}+\epsilon)$-近似算法最大割 都需要 $\Omega(n)$ 空间。

备注 3.19. 这个$\Omega(n)$ 界在对数因子范围内是最优的。事实上，对于每个$\epsilon > 0$，我们都可以选取一个足够大的常数 C，并且给定一个输入实例 Ψ，我们可以采样 $Cn\tilde{}$个约束，得到一个 Ψ的子实例 $\tilde{\Psi}$，输出 $val_{\tilde{\Psi}}$即可为 val_{Ψ} 提供$(1-\epsilon)$-近似$\tilde{}$，只要 C足够大！这种“稀疏化”算法只需 $O(n)$ 空间$\tilde{}$，而且同样的技术可以在 $O(n)$ 空间内，为每个约束满足问题实现任意高精度的近似。

3.4.4 Weaknesses of the proof: Choosing the hybrid

最后$\tilde{}$，我们指出从 BPD 到 sBPD 的归约（引理 3.5，见 §3.3）中，混合变量 S 的选择有一处微妙之处。回想一下，我们应用数据处理$\tilde{}$不等式（引理 2.7）来论证 Bob_t 无法帮助区分 S 与否情形S_t^{N}（见方程 (3.17)）。但使用这一不等式的前提是，在是与否情形下，Bob_t的否输入都与 $\text{Bob}1, \ldots, \text{Bob}_{t-1}$ 的输入相互独立。因此，我们$\tilde{}$不能例如通过混合 $\text{Bob}1, \ldots, \text{Bob}_{t-1}$ 的否输入和 Bob_t的是输入来定义 S。针对一般约束满足问题的后续流式混合论证中也存在同样的问题 [CGSV21a; CGSV21b]。特别是，在 BPD 和 sBPD 的相应推广中，Bob_t 必须具有均匀分布的输入（通常是在否情形下）。

4

最大有向割是轻度可近似的

[最大割] 引出了这样一个问题：小空间流式算法能否对某些 约束满足问题实现非平凡近似（即超过随机赋值阈值），还是说在流式计算模型中，每个约束满足问题都具有近似抗性。

Guruswami 等人 [GVV17]

Unlike Max-Cut, Max-DiCut is approximable在流式设置中。事实上，Guruswami、Velingker 和 Velusamy [GVV17] 证明了最大有向割可以被（$\frac{2}{5} - \epsilon$）近似，所需空间为 $O(\log n)$ 的线性草图算法可以实现这一点；但对于任意 $\frac{1}{2} + \epsilon$，都无法用 $\sqrt{n}$空间的流式算法将其近似到（$\epsilon > 0$）。随后，Chou、Golovnev 和 Velusamy [CGV20]给出了更精确的刻画：

定理 4.1 （[CGV20]）。对于每个常数 $\epsilon > 0$:

i. 存在一种 $O(\log n)$ 空间的线性草图算法，可以将最大有向割（甚至 *Max-2AND*）近似到 （$\frac{4}{9} - \epsilon$）。

ii. 任何以$(\frac{4}{9} + \epsilon)$近似最大有向割的流式算法都需要$\Omega(\sqrt{n})$ 空间。

我们指出，在经典情形下，已有多项工作 [GW95；FG95；Zwi00；MM01；LLZ02] 提出了算法，使Max-2AND和/或最大有向割的近似比不断提升。最近，Lewin、Livnat 和 Zwick [LLZ02]提出并分析了一种针对Max-2AND 的算法，其近似比为 $\alpha_{\mathrm{LLZ}} \geq 0.87401$。*因此，尽管Max-2AND 在流式设置下具有非平凡的可近似性，但其流式可近似性仍远不及经典情形下的可近似性。

本章旨在证明 定理 4.1。我们分别证明其两个部分——在 第 i 项（算法结果）中，见 §4.1；在 第 ii 项（困难性结果）中，见 §4.2。在这两种情况下，我们都会重点说明某些关于 CSP 实例的信息所发挥的关键作用，我们将其称为 模板分布。稍后，这些信息将成为 [CGSV21a；CGSV21b] 中的二分定理的基础（见下文 §5.1）。最后，我们将在 §4.3中进一步讨论并作结。

4.1 Bias-based algorithms for Max-2AND

针对 $\frac{4}{9} - \epsilon$ 的最优近似草图算法Max-2AND 由 [CGV20] 提出（即 定理 4.1 的第 i 项），其核心是测量输入实例中称为 偏差 的量 Ψ。Guruswami、Velingker 和 Velusamy [GVV17] 首先引入了这一量（并用它实现了较弱的 $\frac{2}{5}$ 近似因子）。本节将介绍我们后续合作研究 [BHP+22] 中经过进一步简化后得到的、更简洁的分析。下文 §7.6 将介绍这项后续研究中的分析，它把我们对 Max-2AND 的论证推广到 最大布尔约束满足问题(f)，适用于每个“阈值函数” f。

4.1.1 Setup: Bias-based algorithms

在本节中，我们始终假设 Ψ 具有约束 $(\mathbf{b}(\ell), \mathbf{j}(\ell)\ w(\ell))_{\ell \in [m]}$。对于每个变量 $i \in [n]$，我们令

$$\mathsf{bias}_{\Psi}(i) \stackrel{\text{def}}{=} \sum_{\ell \in [m], t \in [2]:\ j(\ell)_t = i} (-1)^{b(\ell)_t} w_\ell, \tag{4.2}$$

*Austrin [Aus10] 证明了 $(\alpha_{\mathrm{Aus}} + \epsilon)$-近似 Max-2AND 是 UG 困难的，其中 $\alpha_{\mathrm{Aus}} \approx 0.87435$。在不采用唯一博弈猜想的情况下，Trevisan 等人 [TSSW00] 证明了$(\frac{12}{13} + \epsilon)$-近似是 NP-困难的。

然后我们定义

$$\mathsf{bias}_\Psi \stackrel{\text{def}}{=} \frac{1}{2W}\sum_{i\in[n]} |\mathsf{bias}_\Psi(i)|. \tag{4.3}$$

（注意，$\mathsf{bias}_\Psi(i) \in [-W_\Psi, W_\Psi]$，其中 W_Ψ 是 Ψ中的总权重，而 $\mathsf{bias}_\Psi \in [0,1]$。）

对于每个变量 i，$|\mathsf{bias}_\Psi(i)|$ 衡量的是 i的否定出现与非否定出现之间的不平衡，因此与“i 有多容易赋值”相关。例如，如果 $\mathsf{bias}_\Psi(i) \gg 0$，那么 x_i 很少被否定（也就是说，b 值通常为 0），所以我们应该将 $x_i = 1$赋为相应的值。因此，我们预期 bias_Ψ 与 val_Ψ之间存在某种正相关关系。确实，我们有：

Le引理 4.4 ([GVV17，定理 11])。设 Ψ 是一个 *Max-2AND* 实例。该 n

$$\mathit{val}_\Psi \geq \frac{2}{9}(1+\mathit{bias}_\Psi).$$

引理 4.5 ([CGV20，引理 3。3])。设 Ψ 是一个 *Max-2AND* 实例。那么

$$\mathit{val}_\Psi \leq \frac{1}{2}(1+\mathit{bias}_\Psi).$$

引理 4.4 和 4.5 合起来意味着，输出 $\frac{2}{9}(1+\mathsf{bias}_\Psi)$ 可为 val_Ψ提供 $\frac{4}{9}$-近似。要在 $O(\log n)$-空间的流式计算设置下实现 measure bias_Ψ，我们注意到 bias_Ψ 是向量 $\mathsf{bias}(\Psi)$ $\mathsf{def}=(\mathsf{bias}_1(\Psi)\ldots,\mathsf{bias}_n(\Psi))$ 的 ℓ_1-范数。因此，我们可以使用针对 $\mathsf{bias}(\Psi)$ 的 ℓ_1-草图化（定理 2.2）来计算它：对于每个新约束 $(\mathsf{b}(\ell),\mathsf{j}(\ell))$ 及其权重 w_ℓ，我们只需对每个 $t\in[2]$，将 $(-1)^{b(\ell)_t} w_\ell$ 加到 $\mathsf{bias}(\Psi)_{j(\ell)_t}$ 上。

4.1.2 Analysis: template distributions

为了证明 引理 4.4 和 4.5，我们定义几个有用的概念。对于一个分布 $\mathcal{D}\in\Delta(\mathbb{Z}_2^2)$，令 $\mathcal{D}\langle 0\rangle = \mathcal{D}(0,0)$ $\mathcal{D}\langle 1\rangle = \mathcal{D}(1,0)+\mathcal{D}(0,1)$，以及 $\mathcal{D}\langle 2\rangle = \mathcal{D}(1,1)$，也就是说，$\mathcal{D}\langle t\rangle$ 是汉明重量 t对应的概率质量。

给定 Max-2AND 实例 Ψ 的一个赋值$\mathbf{x}\in\mathbb{Z}_2^n$，其约束为 $((\mathbf{b}(\ell),\mathbf{j}(\ell)\ w(\ell))^{\ell\in[m]}$，我们将模板分布 $\mathcal{D}_\Psi^{\mathbf{x}}\in\Delta(\mathbb{Z}_2^2)$定义如下：我们以概率 $^{w_{(\ell)}}/_{W_\Psi}$采样 ℓ，并输出 $\mathbf{b}(\ell)+\mathbf{x}|_{\mathbf{j}(\ell)}$。因此，$\mathcal{D}_\Psi^{\mathbf{x}}\langle t\rangle$是这样的约束所占的权重比例：在赋值$\mathbf{x}$下，$t$ 个变量等于 1。

例 4.6。 设 Ψ 由 $n = 2$ 个变量和 $m = 3$ 个约束组成((0,0),(1, 2)),((0,1),(1,2))，以及((1,1),(1, 2))，其权重分别为2、1和3。（用布尔记法，这些约束可写为 $x_1 \wedge x_2$、$x_1 \wedge \bar{x_2}$、$\bar{x_1} \wedge \bar{x_2}$。）设$\mathbf{x} = (1,1)$。则$\mathcal{D}^{\mathbf{x}}_{\Psi}\langle 2\rangle = \frac{1}{3}$、$\mathcal{D}^{\mathbf{x}}_{\Psi}\langle 1\rangle = \frac{1}{6}$和 $\mathcal{D}^{\mathbf{x}}_{\Psi}\langle 0\rangle = \frac{1}{2}$。

分布 $\mathcal{D}^{\mathbf{x}}_{\Psi}$ 简洁地描述了赋值$\mathbf{x}$的若干重要性质，并帮助我们在可测量的量（偏差）与希望测量的量（值）之间建立联系。例如，我们定义

$$\mu_S(\mathcal{D}) \stackrel{\text{def}}{=} \mathcal{D}\langle 2\rangle - \mathcal{D}\langle 0\rangle. \tag{4.7}$$

大致而言，$\mu_S(\mathcal{D}^{\mathbf{x}}_{\Psi})$ 衡量$\mathbf{x}$ 在偏差$_{\Psi}(i)$较大时，将 i 赋为 sign(bias$_{\Psi}(i)$) 的效果：

事实 4.8。 对于所有$\mathbf{x} \in \mathbb{Z}_q^n$, $\mu_S(\mathcal{D}^{\mathbf{x}}_{\Psi}) = \frac{1}{2W}\sum_{i=1}^{n}(-1)^{x_i}$偏差$_{\Psi}(i)$。特别地，$\mu_S(\mathcal{D}^{\mathbf{x}}_{\Psi}) \leq$ 偏差$_{\Psi}$，并且，$\mu_S(\mathcal{D}^{\mathbf{x}}_{\Psi}) =$ 偏差$_{\Psi}$ 当且仅当对每个 $i \in [n]$，偏差$_{\Psi}(i) > 0 \Longrightarrow x_i = 1$ 且偏差$_{\Psi}(i) < 0 \Longrightarrow x_i = 0$。

事实 4.8 是 命题 7.42的 第 ii 和 iii 项的特殊情形。

现在，我们将分布 $\mathcal{D} \in \Delta(\mathbb{Z}_2^2)$ 与一个关于 2 个变量的 Max-2AND 规范实例 $\Psi^{\mathcal{D}}$ 关联起来；对于每个 $\mathbf{b} \in \mathbb{Z}_2^2$，该实例在约束 ((1，2)，b) 上赋予权重 $\mathcal{D}(\mathbf{b})$。因此，我们可以定义如下量：

$$\gamma(\mathcal{D}) \stackrel{\text{def}}{=} \mathsf{val}_{\Psi^{\mathcal{D}}}(\mathbf{0}) = \mathcal{D}\langle 2\rangle. \tag{4.9}$$

$\gamma(\mathcal{D}^{\mathbf{x}}_{\Psi})$ 衡量 $\mathbf{x}$ 的值：

事实 4.10。对于所有 $\mathbf{x} \in \mathbb{Z}_2^n$，$\gamma(\mathcal{D}^{\mathbf{x}}_{\Psi}) = \mathit{val}_{\Psi}(\mathbf{x})$。

Fa事实 4.10 是下文第 i 项（属于命题 7.42 ）的特殊情形。现在我们有　　：

引理 *4.4* 的证明。设 $\mathbf{x}^* \in \mathbb{Z}_2^n$ 是 Ψ 的最优赋值。

$$\begin{aligned}
\mathsf{val}_{\Psi} &= \mathsf{val}_{\Psi}(\mathbf{x}^*) && \text{(optimality of } \mathbf{x}^*) \\
&= \gamma(\mathcal{D}^{\mathbf{x}^*}_{\Psi}) && \text{(Fact 4.10)} \\
&= \mathcal{D}^{\mathbf{x}^*}_{\Psi}\langle 2\rangle && \text{(definition of } \gamma) \\
&= \frac{1}{2}\left(\mathcal{D}^{\mathbf{x}^*}_{\Psi}\langle 0\rangle + \mathcal{D}^{\mathbf{x}^*}_{\Psi}\langle 1\rangle + \mathcal{D}^{\mathbf{x}^*}_{\Psi}\langle 2\rangle\right) + \frac{1}{2}\left(\mathcal{D}^{\mathbf{x}^*}_{\Psi}\langle 2\rangle - \mathcal{D}^{\mathbf{x}^*}_{\Psi}\langle 0\rangle\right)
\end{aligned}$$

$$\leq \frac{1}{2}(1+\mu_{\mathsf{S}}(\mathcal{D}_{\Psi}^{\mathbf{x}^*})) \qquad (\mu_{\mathsf{S}} \text{ 的定义})$$
$$\leq \frac{1}{2}(1+\mathsf{bias}_{\Psi}). \qquad (\text{Fact 4.8})$$

□

另一方面，为了证明 引理 4.5，对于 $\mathcal{D} \in \Delta(\mathbb{Z}_2^2)$ 和 $p \in [0,1]$，我们定义以下量

$$\lambda(\mathcal{D}, p) \stackrel{\text{def}}{=} \mathop{\mathbb{E}}_{\mathbf{b}\sim\mathcal{B}_p^2}[\mathsf{val}_{\Psi^{\mathcal{D}}}(\mathbf{b})] = q^2\mathcal{D}\langle 0\rangle + pq\mathcal{D}\langle 1\rangle + p^2\mathcal{D}\langle 2\rangle \tag{4.11}$$

其中 $q = 1-p$。特别地，$\lambda(\mathcal{D},1) = \gamma(\mathcal{D})$。我们也可以定义 $\beta(\mathcal{D}) \text{ 定义为 } = \max_{p\in[0,1]} \lambda(\mathcal{D}, p)$，此时 $\beta(\mathcal{D}) \geq \gamma(\mathcal{D})$。

事实 4.12。对于所有 $\mathbf{x} \in \mathbb{Z}_2^n$ 和 $p \in [0,1]$，$\lambda(\mathcal{D}_{\Psi}^{\mathbf{x}}, p) = \mathbb{E}_{\mathbf{a}\sim\mathcal{B}_p^n}[val_{\Psi}(\mathbf{a}+\mathbf{x})]$。特别地，$\beta(\mathcal{D}_{\Psi}^{\mathbf{x}}) \leq val_{\Psi}$。

事实 4.12 是下文 命题 7.42 的 第 i 项 的特殊情形。我们有：

引理 *4.4* 的证明 。令 $\tilde{\mathbf{x}} \in \mathbb{Z}_2^n$ 为“多数赋值”，即 $\widetilde{x}_i = \mathbb{1}_{\text{偏差}_{\Psi}(i)\geq 0}$。我们有

$$\begin{aligned}
\mathsf{val}_{\Psi} &\geq \lambda\left(\mathcal{D}_{\Psi}^{\tilde{\mathbf{x}}}, \frac{2}{3}\right) && (\text{Fact 4.12})\\
&= \frac{4}{9}\mathcal{D}_{\Psi}^{\tilde{\mathbf{x}}}\langle 2\rangle + \frac{2}{9}\mathcal{D}_{\Psi}^{\tilde{\mathbf{x}}}\langle 1\rangle + \frac{1}{9}\mathcal{D}_{\Psi}^{\tilde{\mathbf{x}}}\langle 0\rangle && (\text{definition of } \lambda)\\
&= \frac{2}{9}\left(\mathcal{D}_{\Psi}^{\tilde{\mathbf{x}}}\langle 0\rangle + \mathcal{D}_{\Psi}^{\tilde{\mathbf{x}}}\langle 1\rangle + \mathcal{D}_{\Psi}^{\tilde{\mathbf{x}}}\langle 2\rangle\right) + \frac{2}{9}\left(\mathcal{D}_{\Psi}^{\tilde{\mathbf{x}}}\langle 2\rangle - \mathcal{D}_{\Psi}^{\tilde{\mathbf{x}}}\langle 0\rangle\right) + \frac{1}{9}\mathcal{D}_{\Psi}^{\tilde{\mathbf{x}}}\langle 0\rangle && (\text{definition 的 } \mu_{\mathsf{S}})\\
&\geq \frac{2}{9}(1+\mu_{\mathsf{S}}(\mathcal{D}_{\Psi}^{\mathbf{x}}))\\
&= \frac{2}{9}(1+\mathsf{bias}_{\Psi}) && (\text{Fact 4.8 and definition 的 } \tilde{\mathbf{x}})
\end{aligned}$$

□

引理 4.4 的证明引理 4.4 包含不等式

$$\lambda\left(\mathcal{D}_{\Psi}^{\tilde{\mathbf{x}}}, \frac{2}{3}\right) \geq \frac{2}{9}(1+\mathsf{bias}_{\Psi}).$$

结合引理 4.5，可得

$$\lambda\left(\mathcal{D}_{\Psi}^{\tilde{\mathbf{x}}}, \frac{2}{3}\right) \geq \frac{4}{9}\mathsf{val}_{\Psi}.$$

这为另一个问题提供了一种简单的流式算法，即在时间和空间均为线性复杂度的情况下，输出一个期望值至少为$_{4\ 9}\mathsf{val}_{\Psi}$的赋值：-我们只需计算多数赋值 $\tilde{\mathbf{x}}$，然后以$_{1\ 3}$的概率独立地翻转每一位。

备注 *4.13*。 *[CGV20]* 中引理 *4.4* 的原始证明比这里给出的证明复杂得多（参见该论文中引理 *3.3* 的证明），因为它考虑了使二次函数 $\lambda(\mathcal{D}_{\Psi}^{\tilde{\mathbf{x}}}, p)$ 取最大值的值 $p \in [0,1]$（在 $\mathit{bias}_{\Psi} \in [0, \frac{1}{3}]$ 的情形下，该值为 $\frac{1}{2} + \mathit{bias}_{2\ 1-2}{}^{\Psi}(\mathit{bias}_{\Psi})$）。认识到这属于“杀鸡用~~牛刀~~”，并且设置 $p = \frac{2}{3}$ 足以得到 $(\frac{4}{9} - \epsilon)$-近似，是我们与 *[BHP+22]* 合作的成果。当我们考虑 k *AND*（针对 k-> 2）时，这个问题会更加突出，因为 λ 的次数将为 k，因此它在 $[0,1]$ 上的最大化点没有简单的表达式；见下文 *§7.3.1* 的讨论。

4.2 Proving hardness for Max-DiCut

在本节中，我们证明第 ii 项的定理 4.1，这是一个关于最大有向割在流式设置下的近似困难性结果。首先，我们对这一构造给出一些直观解释。

4.2.1 Intuition: What's wrong with sBPD?

我们最初可能会希望通过构造 3.6 直接从 sBPD 进行归约（即我们用于最大割的归约），方法是将每个最大割约束 (u, v) 转换为一对最大有向割约束 $\{(u, v)$ 和 $(v, u)\}$。在这种情况下，我们能否希望证明一个类似于引理 3.7 的结论，并得到一个 4/9 的间隙？在否情形下，$\mathsf{z}(t)$ 是随机的，因此对于一个固定的赋值 $\mathbf{x}$，$\in \mathbb{Z}_2^n$, $\mathbb{E}[\mathsf{val}_{\Psi}(\mathbf{x})] = \frac{1}{4}$。但在是情形下，如果 $\mathbf{x}^* \in \mathbb{Z}_2^n$ 是 Alice 的输入，当 $z(t)_{\ell}$-= 1 对于 $\mathsf{e}(\ell)$ $= (u, v)$ 时，那么 (x_u^*, x_v^*) 要么是 (0, 1)，要么是 (1, 0)，因此约束 (u, v) 和 (v, u) 中恰好有一个会得到满足！因此，我们有 $\mathsf{val}_{\Psi}(\mathbf{x}^*)$ $= \frac{1}{2}$。由此可见，构造 3.6 似乎只能排除最大割的 $\approx \frac{1}{2}$ -近似算法。

我们可以通过构造 3.6 来如下表述这个问题：其中的**是** 实例之所以值较低，是因为它们过于“对称”。具体来说，我们还有$\mathsf{val}_{\Psi}(1+\mathbf{x}^*) =$

– 1 2。为了打破这种对称性，我们可以让 Alice 添加约束 (u, v)，其中 $x^*_u = 1, x^*_v = 0$。这些约束的作用是使$\mathbf{x}^*$ 更有利，并使 $1 + \mathbf{x}^*$处于劣势。但即使在**否** 情况下，这也会提高 $\mathbf{x}^*$ 的值（因为从期望上看，每个 Bob_t 的约束中有1 4 的部分会由$\mathbf{x}^*$ 满足）。为了弥补这一点，我们稍微修改游戏 sBPD，使得在**否** 情况下，Bob_t 的约束永远不会由$\mathbf{x}^*$满足；也就是说，当他添加$\{(u, v)$，$(v, u)\}$时，我们保证 $(x^*_u, x^*_v) \in \{(1, 1)$，$(0, 0)\}$。

4.2.2 A new problem and a new reduction

我们使用第 ii 项的一种近似变体来完成证明：sBPD：

定义 *4.14*。令 $\alpha \in (0, 1)$，且令 $T, n \in \mathbb{N}$。***sBPD′$_{\alpha,T}(n)$*** **的定义与** ***sBPD′$_{\alpha,T}(n)$*** **（定义 *3.4*）完全相同，不同之处在于，在否情形下，我们令 *Bob$_t$* 的向量 *z(t)* 取其在是情形下的值的相反数。也就是说，** $z(t) = \mathbf{1} + (M^{fold})x^*$。

现在我们可以正式陈述这一归约：

构造 *4.15*（从 *sBPD′* 到最大有向割的 *C2S* 归约）。*Alice* 的归约函数记为 R_0，，输出一个实例 Ψ_0，其中包含 $\frac{\alpha T n}{4}$ 个均匀随机约束 (u, v)，使得 $x^*_u = 1, x^*_v = 0$。对于每个 $t \in [T]$，*Bob$_t$* 的归约函数 R_t 按如下方式输出一个实例 Ψ_t：对于 M_t 中的每个 $e(t, \ell) = (u, v)$，当且仅当 $z(t)_\ell = 1$ 时，*Bob$_t$* 将 (u, v) 和 (v, u) 加入 Ψ_t。

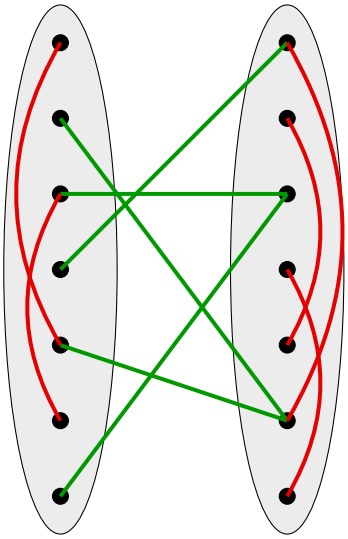
由最大有向割构造4.15产生的困难实例以图示形式呈现于图 4.1中。

幸运的是，通过“对称性”可以简单地证明 sBPD′ 也同样困难 :

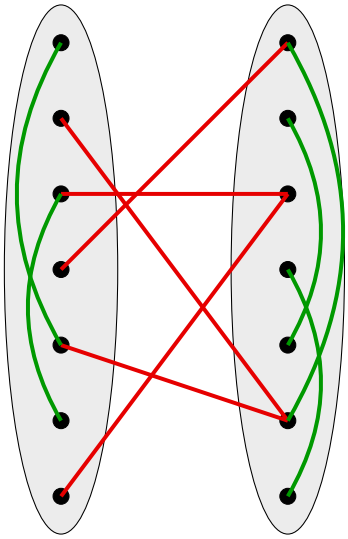
引理 4.16。假设对于某个 $\alpha \in (0, 1)$ 以及 $T, n \in \mathbb{N}$，存在一个 $\textit{sBPD}'_{\alpha, T}(n)$ 协议，其优势为 δ，通信量为 s。那么就存在一个 $\textit{sBPD}_{\alpha, T}(n)$ 协议，其优势为 $\frac{\delta}{2}$，通信量同样为 s。 –

证明。假设 Π 是一个 sBPD′ 协议，其优势为 δ。根据三角不等式， Π在区分以下某一对分布时的优势为 $\frac{\delta}{2}$： –

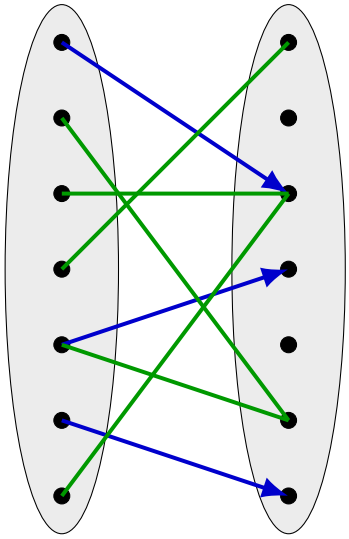
1. sBPD′ 的**是**实例与 sBPD 的**否**实例。
2. sBPD′ 的**否**实例与 sBPD 的**否**实例。



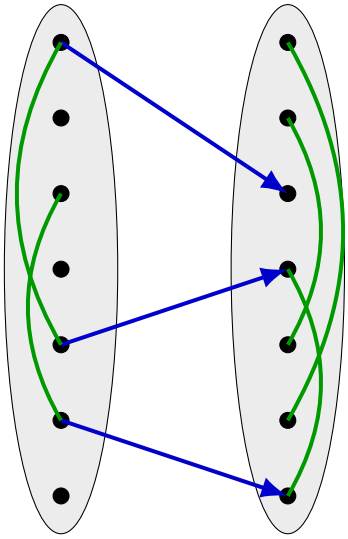
(a) 是 从 sBPD′ 中采样。



(b) 否从 sBPD′ 中抽样。



(c) 是最大有向割的实例。



(d) 最大有向割实例

图 4.1：图 4.1a 和图 4.1b 分别展示了来自 sBPD′ 的是分布和否分布的样本。sBPD′ 的是分布与 sBPD 的相同（图 3.1a）；也就是说，z(t) 标记了哪些边跨越割。然而，sBPD′ 的否分布标记的是哪些边没有跨越割，而 sBPD 的否分布标记的则是均匀随机选取的边（图 3.1b）。图 4.1a 和图 4.1b 中的图再次表示匹配 $M_1, \ldots, M_t$ 的并集；x* 将顶点划分为“左侧”（0）和“右侧”（1）；边的 z 值为“绿色”（1）或“红色”（0）。在从 sBPD′ 到最大割的归约中（构造 3.6），Alice 添加了从左向右跨越割的边（“蓝色”），而每个 Bob$_t$ 添加值为“绿色”（1）的边（其无向副本），其中 z 表示相应的值。我们选择参数，使“绿色”边的数量是“蓝色”边数量的四倍。在是情形中，x* 割断了所有“蓝色”边以及一半的（有向）“绿色”边，因此，是实例（图 4.1c）的最大有向割值为 $\approx \frac{3}{5}$。在否情形中，x* 割断了所有“蓝色”边，但没有割断任何“绿色”边；我们在引理 4.17 中证明，对于足够大的 T，这些实例（图 4.1d）的最大有向割值为 $\approx \frac{4}{15}$。50

情形 (1) 立即得出所需结果，因为 sBPD′ 和 sBPD 具有相同的**是** 实例。情形 (2) 也得出所需结果，因为将所有输入$\mathbf{z}(t)$ 向量都加 1，即可应用该“归约”：sBPD′ 的**否** 实例会变为 sBPD 的**是** 实例，而 sBPD′ 的**否** 实例仍是 sBPD 的**否** 实例。

□

最后，为了证明第 ii 项，只需证明以下引理（类似于引理 3.7）：

引理 *4.17.* 对所有 $\alpha \in (0, 1)$ 和 $\epsilon \in (0, 1 2)$，存在 $T, n_0 \in \mathbb{N}$，使得对每个 $n \geq n_0$，以下结论成立。令 $\mathcal{Y}$ 和 $\mathcal{N}$ 分别表示 $sBPD'_{\alpha,T}(n)$ 的是分布和否分布，并令 $(R0, \ldots, R_T)$ 为构造 *4.15* 中的归约函数。于是

$$\Pr_{\Psi\sim(R_0,\ldots,R_T)\circ\mathcal{Y}}\left[val_\Psi \leq \frac{3}{5} - \epsilon\right] \leq \exp(-n) \text{ and } \Pr_{\Psi\sim(R_0,\ldots,R_T)\circ\mathcal{N}}\left[val_\Psi \geq \frac{4}{15} + \epsilon\right] \leq \exp(-n).$$

不过，我们只给出启发式证明，省略集中界和独立性论证。完整证明可参见例如 [CGV20、§5]。

引理 4.17 的证明概要。回顾上一节中模板分布的定义；让我们分别计算 $\mathcal{D}^{\mathbf{x}^*}_\Psi$ 是与否情形下的期望模板分布，并将其分别记为 $\mathcal{D}_Y$和 $\mathcal{D}_N$。在期望意义下，Alice 添加 $\frac{\alpha}{4}Tn$ 个约束，而 Bob$_t$ 添加 αTn 个约束。在是与否情形下，Alice 引入的约束总是由 $\mathbf{x}^*$满足。在是情形下，Bob$_t$ 看到满足 $x^*_u \neq x^*_v$的边 (u, v)，并添加约束 $\{(u, v)、(v, u)\}$；因此，$\mathbf{x}^*$ 在其中一个子句中满足两个文字，而在另一个子句中两个文字都不满足。因此，$\mathcal{D}_Y\langle 2\rangle = \frac{1/4+1/2}{1/4+1} = \frac{3}{5}$ 和$\mathcal{D}_Y\langle 0\rangle = \frac{1/2}{1/4+1} = \frac{2}{5}$；所以 $\gamma(\mathcal{D}_Y) = \frac{3}{5}$。另一方面，在否情形下，Bob$_t$的边 (u, v) 满足 $x^*_u \neq x^*_v$；因此，$\mathbf{x}^*$ 在两个子句 (u, v) 和 (v, u) 中各满足一个文字。于是，在期望意义下，$\mathcal{D}_N\langle 2\rangle = \frac{1/4}{1/4+1} = \frac{1}{5}$和 $\mathcal{D}_N\langle 1\rangle = \frac{1}{1/4+1} = \frac{4}{5}$。现在

$$\lambda(\mathcal{D}_N, p) = \frac{4}{5}p(1-p) + \frac{2}{5}p^2 = \frac{1}{5}p(4-3p),$$

因此 $\lambda(\mathcal{D}_N, p)$ 在 $p = \frac{2}{3}$ 处达到最大值，得到 $\beta(\mathcal{D}_N) = \frac{4}{15}$。†

†另请注意，$\mu_S(\mathcal{D}_Y) = \mu_S(\mathcal{D}_N) = \frac{1}{5}$；因此，上一节（§4.1）中给出的算法无法解决（$4\,15, 3\,5$）-Max-2AND问题。

为证明 **是**实例的值定理 4.10 所声称的上界，意味着 $\mathrm{val}_\Psi(\mathbf{x}^*) \geq \gamma(\mathcal{D}_\Psi^{\mathbf{x}^*}) \approx \gamma(\mathcal{D}_Y) = \frac{3}{5}$。**否**实例值的上界则更棘手。关键观察是，分布 $(R_0, \ldots\ldots, R_T) \circ \mathcal{N}$ 在变量的排列下保持不变。因此，只需证明对于每个 $\ell \in \{0\} \cup [n]$，汉明重量为 ℓ 的均匀随机解的值都低于 $\frac{4}{15} + \epsilon$；但这种解的期望值恰好是 $\lambda(\mathcal{D}_\Psi^{\mathbf{x}^*}, \frac{\ell}{n}) \approx \lambda(\mathcal{D}_N, \frac{\ell}{n}) \leq \beta(\mathcal{D}_N) = \frac{4}{15}$。

□

4.3 Discussion

最后，我们再次讨论本章中归约和算法的各个方面。

4.3.1 Weaknesses of the reduction (it's Alice's fault)

回想一下我们在 Max-Cut（§4.3）中的讨论，Alice 在 Max-Cut 归约（构造 3.6）中没有添加任何约束，这一点对于将 Max-Cut 的困难性扩展到随机排序和线性空间情形 [KKS15; KK19] 至关重要。对于 Max-DiCut，情况就不那么乐观了，因为在 Max-DiCut 归约（Construction 4.15）中，Alice 发挥了重要作用，她创建了约 $1\,5$ 比例的约束。因此，如何导出随机排序的实例完全不清楚——即使每个 Bob_t 收到的是随机图而非随机匹配——因为 Alice 创建的约束分布与每个 Bob_t 创建的约束分布大不相同，而且这些约束是按序添加到数据流中的。同样也不清楚该如何定义适当的 siBPD 变体（请回想，siBPD 完全省略了 Alice！），以实现线性空间困难性归约。（不过，在这些情形下，Max-Cut 的 $(\frac{1}{2} + \epsilon)$-困难性确实蕴含 Max-DiCut 的 $(\frac{1}{2} + \epsilon)$-困难性：对于一个 Max-Cut 约束 (u, v)，该归约会随机输出 (u, v) 或 (v, u)，作为一个 Max-DiCut 约束。）

事实上，我们从与 Chen、Kol、Paramonov、Saxena、Song 和 Yu 的个人通信 [CKP+21] 以及与 Chou、Golovnev、Sudan、Velingker 和 Velusamy 的个人通信 [CGS+21] 中得知，构造 4.15 生成的困难实例，可通过流式算法在以下情形中区分：$O(\log n)$ 空间的随机顺序情形，以及 $o(n)$ 空间的对抗性顺序情形。在本小节余下部分，我们将粗略介绍这两种算法。

回顾 Max-2AND 实例 Ψ 中变量 i 的偏差 $\mathrm{bias}_\Psi(i)$ 的定义。我们可以将 Max-DiCut 实例视为 Max-2AND 实例，其中每个约束的否定模式均为 (0, 1)（因为 $\mathrm{DiCut}(a,b) = \mathrm{2AND}(a, b+1)$）。因此，根据定义，$\mathrm{bias}_\Psi(i)$ 是 i 出现在左侧与出现在右侧的约束总权重之差。另一方面，我们也可以将 Max-DiCut 实例视为一个包含 n 个顶点的（加权）图（见 §2.3）；在这种解释下，顶点 i 的偏差 $\mathrm{bias}_\Psi(i)$ 是其出权重与入权重之差。

现在让我们考察来自 [CGV20] 的 Max-DiCut **是**实例和**否**实例的分布（由 sBPD′ 中的构造 4.15 生成，见图 4.1）。令 $b \overset{\text{定义}}{=} \frac{\alpha T n}{4}$，我们可以看到，具有 $x^* = 1$ 的顶点具有非负偏差（期望值为 b），而具有 $x^* = 0$ 的顶点具有非正偏差（期望值为 $-b$）。此外，在**是**的情况下，所有边都从具有非负偏差的顶点指向具有非正偏差的顶点；而在**否**的情况下，则存在三种边的混合：从非负偏差顶点指向非正偏差顶点（占边的 $\approx \frac{1}{5}$ 比例）、从非负偏差顶点指向非负偏差顶点（占 $\approx \frac{2}{5}$ 比例），以及从非正偏差顶点指向非正偏差顶点（占 $\approx \frac{2}{5}$ 比例）。

The random-ordering algorithm. 如果我们能够随机抽样边并测量其端点的偏差，那么很快就能判断我们看到的是**是**还是**否**实例，而这在随机排序设置下是可以实现的。事实上，只需存储最先出现的 m' 条边（其中$m' = O$为某个较大的常数），并测量这些边所有端点的偏差即可。这种技术在思路上类似于用于连通分量计数和计算最小生成树的随机排序算法，相关工作见 [PS18]。值得注意的是，尽管在对抗顺序设置下仍然可以随机抽样边（例如，使用蓄水池抽样），但目前尚不清楚如何在抽样的同时测量这些边端点的偏差；事实上，对抗顺序下界表明这是不可能的。

The super-$\sqrt{n}$-space algorithm. 区分**是**和**否**实例的另一种策略，是随机抽取顶点的一个子集 $V \subseteq [n]$，并在数据流处理过程中，既测量 V 中每个顶点的偏差，又存储 V 上的诱导子图。[‡] 数据流结束时，我们只需检查该诱导子图中是否存在任何一条边，且这条边并非从非负偏差顶点指向非正偏差顶点。

[‡]由于归约生成的实例以高概率具有常数最大次数，因此我们可以用 $O(|V|)$ 空间存储诱导子图。

不过，要使这种方法奏效，$|V|$ 必须足够大；根据§3.4.3节中“生日悖论”的论证，随机选取足够多的顶点即可。

4.3.2 Duality, towards dichotomy

令人颇感意外的是，利用下界 $\mathsf{val}_\Psi \geq \lambda(\mathcal{D}_\Psi^{\mathbf{x}}, \frac{2}{3})$，而非更一般的$\mathsf{val}_\Psi \geq \beta(\mathcal{D}_\Psi^{\mathbf{x}})$，就足以证明 引理 4.4。特别是，利用后一个不等式无法得到更好的近似比，因为在给定 第 ii 项 的情况下，$\frac{4}{9}$ 已经是最优的。[§]不过，研究量 $\beta(\mathcal{D}$的一个重要原因是，它也出现在困难性结果的证明中（见引理 4.17证明概要的结尾）。

为了进一步理解这些量 $\beta(\mathcal{D}$和 $\gamma(\mathcal{D})$，我们稍微转换一下思路，转而考虑固定 β，$\gamma)$-Max-2AND 问题，并对固定的 $\beta < \gamma \in [0,1]$取值，解读用于该问题的§4.1 节中的算法。假设 (β, γ) 满足方程

$$\max_{\mathcal{D}\in\Delta(\mathcal{D}_2^2):\ \beta(\mathcal{D})\leq\beta} \mu_{\mathsf{S}}(\mathcal{D}) < \min_{\mathcal{D}\in\Delta(\mathcal{D}_2^2):\ \gamma(\mathcal{D})\geq\gamma} \mu_{\mathsf{S}}(\mathcal{D}) \tag{4.18}$$

并考虑一个固定阈值 τ，它介于这两个值之间。事实 4.10 和事实 4.12 分别意味着：(1) 存在 $\mathbf{x}^* \in \mathbb{Z}_2^n$，使得 $\mathsf{val}_\Psi = \gamma(\mathcal{D}_\Psi^{\mathbf{x}^*})$；(2) 对所有 $\mathbf{x} \in \mathbb{Z}_2^n$，都有 $\mathsf{val}_\Psi \geq \beta(\mathcal{D}_\Psi^{\mathbf{x}})$。因此，公式 (4.18) 表明，只需测量偏差$_\Psi = \max_{\mathbf{x}\in\mathbb{Z}_2^n} \mu_{\mathsf{S}}(\mathcal{D}_\Psi^{\mathbf{x}})$ 并将其与 τ 进行比较，就足以区分 $\mathsf{val}_\Psi \leq \beta$ 和 $\mathsf{val}_\Psi \geq \gamma$这两种情况。另一方面，从引理 4.4 和引理 4.5 的证明中，我们可以推出以下不等式

$$\beta(\mathcal{D}) \geq \frac{2}{9}(1+\mu_{\mathsf{S}}(\mathcal{D})) \text{ and } \gamma(\mathcal{D}) \leq \frac{1}{2}(1+\mu_{\mathsf{S}}(\mathcal{D})),$$

分别。因此，只要 $\frac{\beta}{\gamma} > \frac{4}{9}$，公式 (4.18) 成立，则（$\beta$，$\gamma$）-Max-2AND 问题就是可处理的！

另一方面，我们在§4.2中证明的下界（排除了 $(\frac{4}{9}+\epsilon)$-近似）是基于构造 $\mathcal{D}_N$，$\mathcal{D}_Y \in \Delta(\mathbb{Z}_2^2)$，其中 $\mu_{\mathsf{S}}(\mathcal{D}_N) = \mu_{\mathsf{S}}(\mathcal{D}_Y)$ 且 $\beta(\mathcal{D}_N)\gamma(\mathcal{D}_Y) = \frac{4}{9}$。因此，Max-DiCut 的算法与下界之间存在某种对偶性。

[§]不过，我们当然也可能做得更差！Guruswami等人的 $(\frac{2}{5}-\epsilon)$-近似使用 $p = 1$，也就是说，它贪心地将偏差为正的变量赋值为 1，将偏差为负的变量赋值为 0。该算法“过于自信”，改为设置 $p = \frac{2}{3}$ 会提高近似比。

事实上，只要 公式 (4.18)成立，算法就有效——也就是说， μ_S-值之间存在分离。另一方面，下界中的困难分布具有相匹配的 μ_S-值。于是一个自然的问题是：我们能否将这种“匹配的 μ_S-值”判据推广，从而为超越 最大有向割和最大割的约束满足问题建立算法或困难性二分？下一章我们将看到 [CGSV21a；CGSV21b]给出的答案：是！至少对于草图算法而言是如此。

5 已有结果：一般约束满足问题

我们的刻画核心是一个在流式设置下，采用线性草图化求解 Max-CSP($\mathcal{F}$) 的算法族。我们很快会介绍这个算法族，但证明的主要思路是：如果该算法族中的任何算法都无法求解 (β, γ)-Max-CSP($\mathcal{F}$)，那么我们就能提取出一对实例，大致包括一族 γ-可满足的**"是"**实例，以及一族至多 β-可满足的"否"实例，用以证明这种无能为力。接着，我们将说明如何把这对实例用作构造部件，从而得到一个否定性结果。

Chou、Golovnev、Sudan 和 Velusamy [CGSV21b]

A wide variety of CSPs fall under若干近期推广 [CGSV21a；CGSV21b；CGS+22] 对最大割 和 最大有向割 结果的推广，这些结果已在前两章中介绍。我们的首要目标是阐述这些结果的技术性论述，因为我们将在后文的第 6 章 和 第 7 章中使用它们。我们还将概述其中涉及的技术，并以此前两章中的工作为基础。

具体而言，在 §5.1中，我们介绍 Chou、Golovnev、Sudan 和 Velusamy 的结果 [CGSV21a；CGSV21b] 关于 $\sqrt{n}$空间流式算法，这些结果推广了我们已经见过的最大割 (定理 3.1，由 [KKS15]提出）和最大有向割 (定理 4.1，由

[CGV20]）的结果。它们包括一个所谓的二分定理，该定理完全刻画了 $\sqrt{n}$ 空间草图算法的 CSP 可近似性（见 §2.2），并以我们在第 4 章对最大有向割进行的“模板分布”分析为基础。这个二分定理随后将成为 [BHP+22] 对对称 $f\colon \mathbb{Z}_2^k \to \{0,1\}$ 的最大布尔约束满足问题（f）进行分析的基础，相关内容将在下文第 7 章介绍。接下来，在 §5.2 中，我们介绍 Chou、Golovnev、Sudan、Velingker 和 Velusamy 在 [CGS+22] 线性空间流处理设置下的结果，这些结果推广了我们已经见过的最大割结果（在 §3.4.3 中讨论，由 [KK19] 提出）。在第 6 章中，我们将运用这些结果，为我们合作研究的所谓“排序约束满足问题”证明线性空间流式近似抗性结果 [SSV21]。

5.1 $\sqrt{n}$-SPACE ALGORITHMS AND THE SKETCHING DICHOTOMY

对于 Max-2AND，我们在 §4.3.2 中讨论了，具有某些性质的“模板分布”的存在与否，分别意味着针对 (β,γ)-Max-2AND 问题的 $\Omega(\sqrt{n})$-空间流式下界（§4.2.2）和 $O(\log\ n)$-空间草图算法（§4.1.2）。Chou、Golovnev、Sudan 和 Velusamy [CGSV21b] 证明了一个二分定理，将这一结果推广到了每个 Max-CSP($\mathcal{F}$) 问题（以及每个 $\beta < \gamma \in [0,1]$）：要么 (β,γ)-Max-CSP($\mathcal{F}$) 存在一个 $O(\text{polylog}\ n)$-空间草图算法，要么对于每个 $\epsilon > 0$，$(\beta+\epsilon,\gamma-\epsilon)$-Max-CSP($\mathcal{F}$) 的草图算法都必须使用至少 $\Omega(\sqrt{n})$ 的空间！然而，重要的是，这个下界一般而言只适用于草图算法；不过，下面我们将讨论它适用于流式算法的一些重要特殊情形。

在 §5.1.1中，我们给出模板分布的精确定义、其性质，以及针对重要特殊情形 最大布尔约束满足问题(f) 问题由此得到的上界和下界。这些陈述来自 [CGSV21a]，，我们将在下文的 第 7 章 中用到它们；届时我们将介绍来自 [BHP+22] 的结果，进一步研究 $f\colon \mathbb{Z}_2^k \to \{0,1\}$为对称的情形。为一般的 最大约束满足问题($\mathcal{F}$) 问题定义模板及其性质，需要进行大量展开，超出了本文的范围；不过在§5.1.2中，我们概述这些概念，并对[CGSV21a和 CGSV21b]中使用的技术作一些结构概述。

5.1.1 Technical statements (Boolean case)

回顾一下， $\Delta(\mathbb{Z}_2^k)$ 表示 $\mathbb{Z}_2^k$上所有分布构成的空间。仿照 2AND (参见 §4.1.2) 的例子，对于"模板分布" $\mathcal{D} \in \Delta(\mathbb{Z}_2^k)$ 和谓词 $f : \mathbb{Z}_2^k \to \{0,1\}$，我们定义一个"规范实例" $\Psi^{\mathcal{D}}$：它是在 最大布尔约束满足问题(f) 中包含 k 个变量的实例，并在约束 ((1b) 上赋予权重$, \ldots, k)$, b)。接着我们定义

$$\lambda_f(\mathcal{D}, p) \stackrel{\text{def}}{=} \mathop{\mathbb{E}}_{\mathbf{a}\sim\mathcal{B}_p^k}[\mathsf{val}_{\Psi^{\mathcal{D}}}(\mathbf{a})], \quad \gamma_f(\mathcal{D}) \stackrel{\text{def}}{=} \lambda_f(\mathcal{D}, 1), \quad \text{and } \beta_f(\mathcal{D}) \stackrel{\text{def}}{=} \sup_{p\in[0,1]} (\lambda_f(\mathcal{D}, p)) . \quad (5.1)$$

正如我们在Max-2AND 的§4.1.2中所做的那样，我们可以将这些模板分布解释为针对某个实例的特定赋值的否定模式分布；参见下文§7.6.1 开头。

我们还定义一个边缘向量 $\boldsymbol{\mu}(\mathcal{D}) = (\mu(\mathcal{D})_1, \ldots, \mu(\mathcal{D})_k) \in [-1,1]^k$，其第 i个分量为$\mu(\mathcal{D})_i \stackrel{\text{def}}{=} -\mathbb{E}_{\mathbf{b}\sim\mathcal{D}}[(-1)^{a_i}]$.*†

现在，对于谓词 $f : \mathbb{Z}_2^k \to \{0,1\}$，我们定义两个边缘分布集合

$$K_{f,N}(\beta) \stackrel{\text{def}}{=} \{\boldsymbol{\mu}(\mathcal{D}_N) : \beta_f(\mathcal{D}_N) \le \beta\} \quad \text{and } K_{f,Y}(\gamma) \stackrel{\text{def}}{=} \{\boldsymbol{\mu}(\mathcal{D}_Y) : \gamma_f(\mathcal{D}_Y) \ge \gamma\}.$$

[CGSV21a] 的二分定理大致指出，(β,γ)-最大布尔约束满足问题(f)是困难的，当且仅当这两个集合有交集：

定理 5.2 (草图二分， [CGSV21a，定理 2。3])。对于每个 $f : \mathbb{Z}_2^k \to \{0,1\}$以及 $\beta < \gamma \in [0,1]$:

i. 若 $K_{f,N}(\beta) \cap K_{f,Y}(\gamma) = \emptyset$，则存在 $\tau > 0$ 以及一种(β,γ)-最大布尔约束满足问题(f) 线性草图算法，使用至多 $\tau \log n$ 空间。

ii. 若 $K_{f,N}(\beta) \cap K_{f,Y}(\gamma) \neq \emptyset$，则对于每个 $\epsilon > 0$，都存在 $\tau > 0$，使得任何针对 $(\beta + \epsilon, \gamma - \epsilon)$-*Max-BCSP*$(f)$ 的草图算法都至少需要 $\tau\sqrt{n}$ 空间（对于

*请注意，在 §4.1.2 中讨论的 2AND 情形下，对于 $\mathcal{D} \in \Delta(\mathbb{Z}_2^2)$，我们定义了一个标量量 $\mu\mathsf{S}(\mathcal{D}) = \mathcal{D}(1,1) - \mathcal{D}(0,0)$。然而，根据我们刚才给出的定义， $\boldsymbol{\mu}(\mathcal{D}) = (\mu(\mathcal{D})1, \mu(\mathcal{D})2)$，其中 $\mu(\mathcal{D})_1 = \mathcal{D}(1,1) + \mathcal{D}(1,0) - \mathcal{D}(0,1) - \mathcal{D}(0,0)$，且 $\mu(\mathcal{D})_2 = \mathcal{D}(1,1) + \mathcal{D}(0,1) - \mathcal{D}(1,0) - \mathcal{D}(0,0)$。因此，$\mu\mathsf{S}(\mathcal{D}) = 1\ 2\ (\mu(\mathcal{D})_1 + \mu(\mathcal{D})2)$。正如我们将在 §7.2 中讨论的，对于 Max-2AND，只需考虑"对称"的分布 $\mathcal{D}$ 和"标量"的边缘分布，因为 2AND 是一个对称谓词。

†我们额外添加一个负号，以便与我们在2AND 中确立的约定保持一致：§4.1.2"偏差为正的顶点希望被赋值为 1。"

足够大的 n）。

暂且撇开 K_f 符号不谈，第 ii 项是关于 §4.2.2 中“困难模板”的一个论断：若对于某个 $\mathcal{D}_N, \mathcal{D}_Y \in \Delta(\mathbb{Z}_2^k)$，有 $\boldsymbol{\mu}(\mathcal{D}_N) = \boldsymbol{\mu}(\mathcal{D}_Y)$，则对于每个 $\epsilon > 0$，对 $(\beta_f(\mathcal{D}_N) + \epsilon, \gamma_f(\mathcal{D}_Y) - \epsilon)$-最大布尔约束满足问题$(f)$进行草图化需要 $\Omega(\sqrt{n})$ 空间。

利用一个标准归约，定理 5.2 可推出一个关于近似问题的二分定理：

推论 5.3 ([CGSV21a，命题 2。10])。对于 $f\colon \mathbb{Z}_2^k \to \{0,1\}$，令

$$\alpha(f) \stackrel{\text{def}}{=} \inf_{\mathcal{D}_N, \mathcal{D}_Y \in \Delta(\mathbb{Z}_2^k):\ \boldsymbol{\mu}(\mathcal{D}_N) = \boldsymbol{\mu}(\mathcal{D}_Y)} \left(\frac{\beta_f(\mathcal{D}_N)}{\gamma_f(\mathcal{D}_Y)} \right).$$

于是：

i. 对于每个 $\epsilon > 0$，都存在 $\tau > 0$ 以及一个 τ 对数 n 空间的线性草图算法，它以 $(\alpha(f) - \epsilon)$近似最大布尔约束满足问题(f)。

ii. 对于每个 $\epsilon > 0$，都存在一个 $\tau > 0$，使得任何对 ***Max-BCSP***(f) 进行 $\alpha(f) + \epsilon)$-近似的草图算法，至少需要 $\tau\sqrt{n}$ 空间（当 n 足够大时）。

我们简要概述该证明，以便为我们合作研究中针对某些最大布尔约束满足问题(f)问题的更简单草图算法提供一个比较基准 [BHP+22]，相关内容将在下文§7.6中介绍。

证明思路。为证明第 ii 项，对于每个 $\epsilon > 0$，存在 $\mathcal{D}_N, \mathcal{D}_Y \in \Delta(\mathbb{Z}_2^k)$，使得 $\boldsymbol{\mu}(\mathcal{D}_N) = \boldsymbol{\mu}(\mathcal{D}_Y)$，满足 $\beta_f(\mathcal{D}_N)/\gamma_f(\mathcal{D}_Y) \le \alpha(f) + \epsilon/2$。令 $\beta' = \beta_f(\mathcal{D}_N) + \epsilon/2$ 且 $\gamma' = \gamma_f(\mathcal{D}_N) - \epsilon/2$，根据定理 5.2，$(\beta', \gamma')$-最大布尔约束满足问题$(f)$需要 $\Omega(\sqrt{n})$ 空间。但对于足够小的 $\epsilon > 0$，$\beta'/\gamma' \le \alpha(f) + \epsilon$，因此最大布尔约束满足问题$(f)$需要 $\Omega(\sqrt{n})$ 空间才能达到 $(\alpha(f) + \epsilon)$-近似。

第 i 项的证明使用了以下观察：如果一个用于 (β, γ)-最大布尔约束满足问题(f)的算法在实例 Ψ 上正确，那么输出**是**和**否**分别意味着 $\mathrm{val}_\Psi \ge \beta$ 和 $\mathrm{val}_\Psi \le \gamma$。[‡] 因此，给定一个实例 Ψ，一种合理的策略是选取若干对 $\{(\beta_s, \gamma_s)\}_{s \in S}$，使得对于每个 s，$K_{f,N}(\beta_s) \cap K_{f,Y}(\gamma_s) = \emptyset$；使用定理 5.2 计算

[‡]注意，由于 (β, γ)-最大布尔约束满足问题(f) 是一个承诺问题，如果 $\beta \le \mathrm{val}_\Psi \le \gamma$，那么算法的输出可以是任意的。

每个 (β_s, γ_s)-最大布尔约束满足问题(f) 的输出 A_s；[§]然后输出 β_{s^*}，其中 s^* 在 $\{s \in S$ 上使 β_s 最大：$A_s =$ 是$\}$。根据我们的观察，β_{s^*} 是 val_Ψ 的一个低估值，但我们如何保证它至少为 $(\alpha(f) - \epsilon)\mathsf{val}_\Psi$?

思路是选取一些 $\delta > 0$，并考虑一个"区分网格" $S = \{(b\delta, g\delta) : b, g \in [\lfloor 1/\delta \rfloor], K_{f,N}(b\delta) \cap K_{f,Y}(g\delta) = \emptyset\}$。然后，给定使 β_s over$\{s \in S :$ $A_s =$ 是$\}$ 最大化的 $s^* = (b^*, g^*)$，我们令 $b' = b + 1$ and $g' = \lceil (b+1)/\alpha \rceil$。根据构造，$g'/b' > \alpha$；因此根据假设，$K_{f,N}(b'\delta) \cap K_{f,Y}(g'\delta) = \emptyset$，于是 $s' = (b', g') \in S$。现在，由于β_{s^*}的极大性，我们有 $A_{(b',g')} =$否。因此

$$b^*\delta \le \mathsf{val}_\Psi \le g'\delta,$$

并且我们选择 g' 使得 $b^*/g' \approx \alpha$。令 $\delta = \epsilon\rho(f)/2$ 并调整算法，使其输出 $\max\{\beta_{s^*}, \rho(f)\}$ 即可；详情请参见 [CGSV21a，命题 210] 的证明。

□

虽然来自 [CGSV21a] 的下界（即定理 5.2 的第 ii 项，以及由此推得的推论 5.3 的第 ii 项）通常只适用于草图算法，但 [CGSV21a] 还给出了在满足某个条件时将下界推广到流式算法的结果。具体而言，该条件针对分布 $\mathcal{D}_N, \mathcal{D}_Y \in \Delta(\mathbb{Z}_2^k)$，且比条件 $\boldsymbol{\mu}(\mathcal{D}_N) = \boldsymbol{\mu}(\mathcal{D}_Y)$ 更强。如果 $\boldsymbol{\mu}(\mathcal{D}) = \mathbf{0}$，即对所有 $i \in [k]$, $\mathbb{E}_{\mathbf{a}\sim\mathcal{D}}[a_i] = 0$ 均成立，我们就称 $\mathcal{D} \in \mathbb{Z}_2^k$ 是单向独立的（或具有均匀边缘分布）。那么，如果存在 $\mathcal{D}_0, \mathcal{D}'_N, \mathcal{D}'_Y \in \Delta(\mathbb{Z}_2^k)$，且 $\eta \in [0,1]$ 满足以下条件，则 $(\mathcal{D}_N, \mathcal{D}_Y)$ 是一个填充单向配对：$\mathcal{D}'_N$ 和 $\mathcal{D}'_Y$ 具有均匀边缘分布，$\mathcal{D}_N = \eta\mathcal{D}_0 + (1-\eta)\mathcal{D}'_N$，并且 $\mathcal{D}_Y = \eta\mathcal{D}_0 + (1-\eta)\mathcal{D}'_Y$。于是：

定理 *5.4*（[*CGSV21a*，定理 *2.11*]）。对于任意 $f : \mathbb{Z}_2^k \to \{0,1\}$ 和填充单向配对 $\mathcal{D}_N, \mathcal{D}_Y \in \Delta(\mathbb{Z}_2^k)$，存在 $\tau > 0$，使得每个针对 $(\beta_f(\mathcal{D}_N) + \epsilon, \gamma_f(\mathcal{D}_Y) - \epsilon)$-最大布尔约束满足问题$(f)$的流式算法都至少需要 $\tau\sqrt{n}$ 空间（当 n 足够大时）。因此，对于任意 $\epsilon > 0$，每个以 $(\beta_f(\mathcal{D}_N)/\gamma_f(\mathcal{D}_Y) + \epsilon)$-近似 *Max-BCSP*$(f)$ 的流式算法都至少需要 $\tau\sqrt{n}$ 空间（当 n 足够大时）。

[§]由定理 5.2 给出的β_s、γ_s)-最大布尔约束满足问题(f) 算法是随机化的，因此每种算法都有一定的常数概率失败。不过，只要 $|S|$ 是常数（给定 ϵ），我们就可以提高每种算法的成功概率，并应用并集界。

例 5.5。在 §4.2.2 中，我们为最大有向割构造了一对困难模板分布：$\mathcal{D}_Y$，其取值为 (1, 1) 的概率是 3 5，取值为 (0, 0) 的概率是 2 5；以及 $\mathcal{D}_N$，其取值为 (1, 1) 的概率是 1 5，取值为 (0, 1) 和 (1, 0) 的概率各为 2 5。回想一下，Max-2AND 是 Max-Cut 的推广，因此我们可以结合定理 5.4，从 Max-2AND 的角度考察这对 $(\mathcal{D}_Y, \mathcal{D}_N)$。我们在 §4.2.2 中的计算表明，$\beta_{2AND}(\mathcal{D}_N) = \frac{4}{15}$，且 $\gamma_{2AND}(\mathcal{D}_Y) = \frac{3}{5}$。现在令 $\eta = \frac{1}{5}$，$\mathcal{D}_0$ 的取值为 (1, 1) 的概率是 1，$\mathcal{D}'_Y = \mathcal{U}_{\{(1,1),(0,0)\}}$，并令 $\mathcal{D}'_N = \mathcal{U}_{\{(1,0),(0,1)\}}$，可知 $\mathcal{D}_Y$ 和 $\mathcal{D}_N$ 构成填充单向配对。因此，定理 5.4 推出，$(\frac{4}{15} + \epsilon, \frac{3}{5} - \epsilon)$-Max-2AND 需要 $\Omega(\sqrt{n})$ 流式空间，因此以 $(\frac{4}{9} + \epsilon)$-近似 Max-2AND 需要 $\Omega(\sqrt{n})$。从本质上说，这重新得出了我们在 §4.2 中证明的最大有向割下界（定理 4.1 的第 ii 项），但形式上较弱（因为 Max-DiCut 的谓词集合较小）。要得到完整的下界，需要采用 [CGSV21b] 中更一般的框架。

另一方面，在 §4.1.2 中，我们证明了如果 $\frac{\beta}{\gamma} < \frac{4}{9}$，那么 $\max_{\mathcal{D}_N}: \beta_{2AND}(\mathcal{D}) \mu_S(\mathcal{D}) < \min_{\mathcal{D}_Y}: \gamma_{2AND}(\mathcal{D}) \mu_S(\mathcal{D})$，由此得出 $K_{2AND,N}(\beta) \cap K_{2AND,Y}(\gamma) = \emptyset$。因此，$\alpha(2AND) = \frac{4}{9}$。

例 5.6. 定理 5.4 的一个重要特殊情形是 $\mathcal{D}_N = \mathcal{U}_{\mathbb{Z}_2^k}$ 且 $\gamma_f(\mathcal{D}_Y) = 1$。在这种情况下，$\mathcal{D}_N$，$\mathcal{D}_Y$ 是单向独立的（因为根据定义，$\mu(\mathcal{U}_{\mathbb{Z}_2^k}) = \mathbf{0}$），因此它们构成一个平凡的填充单向配对（其中 $\eta = 0$）。此外，所有 $f: \mathbb{Z}_2^k \to \{0, 1\}$ 和 $p \in [0, 1]$，

$$\lambda_f(\mathcal{D}_N, p) = \mathop{\mathbb{E}}_{\mathbf{a} \sim \mathcal{U}_{\mathbb{Z}_2^k}, \mathbf{b} \sim \mathcal{B}_p^k} [f(\mathbf{a} + \mathbf{b})] = \mathop{\mathbb{E}}_{\mathbf{a} \sim \mathcal{U}_{\mathbb{Z}_2^k}} [f(\mathbf{a})] = \rho(f)$$

因此 $\beta_f(\mathcal{D}_N) = \rho(f)$。因此 定理 5.4 表明 最大布尔约束满足问题$(f)$ 是 流式计算近似抗性 (在 $\sqrt{n}$ 空间内)，即 $\sqrt{n}$-空间流式算法无法$(\rho(f) + \epsilon)$-近似 最大布尔约束满足问题(f) 对任意 $\epsilon > 0$。

如果存在一个单变量独立的 $\mathcal{D}_Y \in \mathbb{Z}_2^k$，满足 $\gamma_f(\mathcal{D}_Y) = 1$，我们就称谓词$f$ 支持单变量独立性，因为任何满足 $\mathcal{D}_Y \in \mathbb{Z}_2^k$ 且$\gamma_f(\mathcal{D}_Y) = 1$ 的分布，其支撑集必然包含在 f的支撑集中。因此，如果 f支持单变量独立性，那么最大布尔约束满足问题(f) 就是流式近似抗性的 [CGSV21a，定理 1。3]。

5.1.2 Discussion

在本小节中，我们（简要地）讨论上一小节中介绍的 [CGSV21a] 结果的各个方面，以及这些结果在 [CGSV21b] 中的扩展：该扩展涵盖了由定义在所有字母表上的一般谓词族所定义的约束满足问题。首先，我们提到，β，γ-最大布尔约束满足问题(f) 的定理 5.2 中的二分判据“可用实数的量化理论表达”，也就是说，它等价于一个关于实变量的量化多项式等式或不等式系统；因此，该判据已知是可判定的，特别是可以在相对于 f的真值表规模以及 β 和 γ (参见 [CGSV21a，定理 1。1]中的正式表述)位复杂度而言，在多项式空间内判定。定理 5.2定理 5.2 具有这一令人振奋的性质，因为相比之下，Raghavendra 的二分判据 [Rag08] （针对多项式时间算法，并假设唯一博弈猜想成立）尚不知是否可判定。

定理 5.2 第 i 项的证明与针对 Max-DiCut 的定理 4.1 第 i 项的证明颇为相似。回顾一下我们在 §4.3.2 中讨论的 (β,γ)-Max-2AND 的证明：我们利用 μ_{S} 值之间的“分离”（公式 (4.18) ），得到一个用于 (β,γ)-Max-2AND 的算法。现在，对于任意的 (β,γ)-Max-BCSP(f) 问题，我们仍然利用 $K_{f,N}(\beta)$ 与 $K_{f,Y}(\gamma)$ 的不相交性：如 [CGSV21a, §4], 中那样，我们考虑潜在赋值 $\mathbf{x}$ 的“模板分布” $\mathcal{D}_\Psi^{\mathbf{x}} \in \Delta(\mathbb{Z}_2^k)$；在确认集合 $K_{f,N}(\beta)$ 和 $K_{f,Y}(\gamma)$ 是紧致且凸的之后，对它们应用分离超平面定理（我们将其视为模板分布的集合）；然后利用 1-范数草图化（即定理 2.2）来“对 $\mathbf{x}$ 取最大值”。

来自 [CGSV21a] 的困难性结果（定理 5.2 的第 ii 项和定理 5.4）也与定理 4.1 的第 ii 项具有某些相似之处。事实上， [CGSV21a, §5] 考虑了 BPD（见定义 3.2）的一种变体，称为随机掩码检测（RMD）。在 $(\mathcal{D}_N,\mathcal{D}_Y)$-RMD$_\alpha(n)$ 问题中，Alice 获得一个隐藏赋值 $\mathbf{x}^* \in \mathbb{Z}_2^n$，并与 Bob 进行通信；Bob 获得一个随机超匹配 $M \sim \mathcal{M}_{k,\alpha}(n)$ 和一个向量 $\mathbf{z} = M^\top \mathbf{x}^* + \mathbf{b} \in (\mathbb{Z}_2^k)^{\alpha n}$，其中在是情形下 $\mathbf{b} \sim \mathcal{D}_Y^{\alpha n}$，而在否情形下 $\mathbf{b} \sim \mathcal{D}_N^{\alpha n}$。也就是说，对于每个边索引 $\ell \in [\alpha n]$，如果令 $\mathbf{z}(\ell) \in \mathbb{Z}_q^k$ 表示 $\mathbf{z}$ 中第 ℓ 个包含 k 个坐标的块，并令 $\mathbf{e}(\ell)$ 表示 M 中第 ℓ 条边，那么 $\mathbf{z}(\ell)$ 等于 $\mathbf{x}^*|_{\mathbf{e}(\ell)}$ 加上一个随机“掩码”，该掩码从 $\mathcal{D}_Y$ （是情形）或 $\mathcal{D}_N$ （否情形）中抽取。 [CGSV21a] 中的核心通信下界是 [GKK+08] 对 BPD 的困难性结果（定理 3.3）的一种类比：

定理 5.7 ([CGSV21a，定理 6。2])。 对于每个 $k \geq 2$ 和 $\mathcal{D} \in \Delta(\mathbb{Z}_2^k)$ 使得

$\boldsymbol{\mu}(\mathcal{D}) = \mathbf{0}$，存在 $\alpha_0 \in (0, 1)$ 使得对于所有 $\alpha \in (0, \alpha_0)$ $\delta \in (0, 1)$，存在$\tau > 0$和 $n_0 \in \mathbb{N}$ 使得对于所有 $n \geq n_0$，任何针对 $(\mathcal{U}_{\mathbb{Z}_2^k}, \mathcal{D})$-*RMD*$_\alpha(n)$ 且优势至少为 δ 的协议都需要 $\tau\sqrt{n}$ 通信。

我们简要说明，为什么 $\mathcal{D}$ 的单变量独立性对于证明这个下界很重要。在傅里叶分析归约（引理 3.9）的推广中，我们必须考虑 $h_\alpha(\ell, n)$ 的一个类似量，记作 $h_{k,\alpha}(\ell, n)$；它直观地衡量是否存在某个$\mathbf{s} \in \mathbb{Z}_2^{k\alpha n}$，使得对于$\mathbf{v} \in \mathbb{Z}_2^n$ 中汉明重量为 $\|\mathbf{v}\|_0 = \ell$ 的$\mathbf{v}$，有 $M^\top \mathbf{s} =$ 。遗憾的是，这个直观的事件发生的概率“过高”，因为只要 supp(v) 中的每个顶点都被 M触及，该事件就会发生；其概率约为 α^ℓ，即使对于包含来自引理 2.4的因子 n 的 $\ell = 2$ 项来说，这也不够小（见注释 3.14 ）。幸运的是，单变量独立性实际上允许我们限制所考虑的s向量集合。具体而言，我们可以推导出 Bob 的条件输入分布 $\mathcal{Z}_{A,M}$ 的傅里叶系数公式：

$$\widehat{\mathcal{Z}_{A,M}(\mathbf{s})} = \frac{1}{2^{k\alpha n}} \mathop{\mathbb{E}}_{\mathbf{x}^* \sim \mathcal{U}_A, \mathbf{b} \sim \mathcal{D}^{\alpha n}} [(-1)^{-\mathbf{s}\cdot(M\mathbf{x}^* + \mathbf{b})}]$$

（与引理 3.9 的证明相比）。由独立性，我们可以提出因子 $\mathbb{E}_{\mathbf{b}\sim\mathcal{D}^n}[(-1)^{\mathbf{s}\cdot\mathbf{b}}] = \prod_{\ell=1}^{\alpha n} \mathbb{E}_{\mathbf{b}\sim\mathcal{D}^n}[(-1)^{\mathbf{s}(\ell)\cdot\mathbf{b}}]$，其中 s $=$(s(1) . . . , s(αn))。假设 $\|\mathbf{s}(\ell)\|_0 = 1$ 对某个 ℓ 成立；不失一般性，s(1) $=$(1, 0, . . . , 0)，此时 $\widehat{\mathcal{Z}_{A\,M}}$，(s) 是 $\mathbb{E}_{\mathbf{b}\sim\mathcal{D}^n}[(-1)^{\mathbf{s}(1)\cdot\mathbf{b}}] = \mathbb{E}_{\mathbf{b}\sim\mathcal{D}^n}[(-1)^{b_1}] = -\mu(\mathbf{b})_1 = 0$ 的倍数。换言之，$\mathcal{Z}_{A、M}$ 的所有傅里叶系数，只要在任意一个块中恰好支撑集于一个坐标上，就都为零。因此，我们可以将 $h_{k、\alpha}(\ell, n)$ 重新定义为满足以下两项条件的 s $=$(s(1) . . . , s(αn)) 存在的概率：(1) 对所有 $\ell \in [\alpha n]$，s(ℓ) $= \mathbf{0}$ 或 $\|\mathbf{s}(\ell)\|_0 \geq 2$；(2) $M^\top$s $=$v。这样，$h_{k、\alpha}(\ell, n)$ 就会足够小，从而能够完成下界的证明。

此时，[CGSV21a] 困难性结果“分化”为定理 5.4 和定理 5.2 的第 ii 项。一方面，我们可以定义（T+1）方玩家的顺序版本（$\mathcal{D}_N, \mathcal{D}_Y$）-sRMD$_{\alpha,T}(n)$，它基于（$\mathcal{D}_N, \mathcal{D}_Y$）-RMD；与 sBPD 和 BPD 的情形类似，其中有 T 个玩家 Bob1, . . . , Bob$_T$，每位玩家都会收到相互独立的 Bob 输入。假设我们希望应用用于将 sBPD 规约到 BPD 的混合论证（引理 3.5，见 §3.3），将 sRMD 规约到 RMD。正如我们在 §3.4.4 中所说，这需要应用数据处理不等式，而该不等式成立的条件是

¶注意，与我们在引理 3.9中的分析不同，M 没有折叠，且$\mathbf{s}$ 的长度为 $k\alpha n$.

其中一个分布是均匀分布 $\mathcal{U}_{\mathbb{Z}_2^k}$。这样做之后，再使用我们用于证明 引理 4.16 的相同三角不等式论证，可以得出：如果$\boldsymbol{\mu}(\mathcal{D}_Y) = \boldsymbol{\mu}(\mathcal{D}_N) = 0$那么（$\mathcal{D}_N, \mathcal{D}_Y$）-sRMD$_{\alpha,T}(n)$ 同样需要 $\Omega(\sqrt{n})$ 空间。

现在，对于一个填充单向配对 $\mathcal{D}_N, \mathcal{D}_Y \in \Delta(\mathbb{Z}_2^k)$，其中 $\mathcal{D}_N = \eta\mathcal{D}_0 + (1-\eta)\mathcal{D}'_N$，$\mathcal{D}_Y = \eta\mathcal{D}_0 + (1-\eta)\mathcal{D}'_Y$，且 $\boldsymbol{\mu}(\mathcal{D}_N) = \boldsymbol{\mu}(\mathcal{D}_Y) = 0$，我们可以应用以下从 $(\mathcal{D}'_N, \mathcal{D}'_Y)$-sRMD 到 Max-BCSP($f$) 的 C2S 归约：令 $m = \alpha T n$。Alice 在 $[n]$ 上均匀采样一列 k-超边 $\mathsf{e}(0,1), \ldots, \mathsf{e}(0, \eta m/(1-\eta))$，并创建子实例 Ψ_0，其中包含约束 $(\mathsf{e}(0,\ell), \mathsf{x}^*|_{\mathsf{e}(0,\ell)} + \mathsf{b}(0,\ell))$，其中 $\mathsf{b}(0,\ell) \sim \mathcal{D}_0$，对 $\ell \in [\eta m/(1-\eta)]$ 成立。Bob$_t$ 在输入 $(M_t, \mathsf{z}(t))$（其中 M_t 的边为 $(\mathsf{e}(t,1), \ldots, \mathsf{e}(t, \alpha n))$）上，创建子实例$\Psi_t$，其中包含约束 $(\mathsf{e}(t,\ell), \mathsf{z}(t,\ell))$，对 $\ell \in [\alpha n]$ 成立。现在，由于 $\mathsf{z}(t,\ell) = \mathsf{x}^*|_{\mathsf{e}(t,\ell)} + \mathsf{b}(t,\ell)$，其中 $\mathsf{b}(t,\ell) \sim \mathcal{D}'_Y$（是情形）或 $\mathsf{b}(t,\ell) \sim \mathcal{D}'_N$（否情形），因此是实例和否实例的模板分布分别为 $\mathcal{D}_Y$（是情形）或 $\mathcal{D}_N$（否情形），这就大致证明了定理 5.4。

另一方面，如果 $\boldsymbol{\mu}(\mathcal{D}_Y) = \boldsymbol{\mu}(\mathcal{D}), \neq 0$会怎样？在这种情况下，[CGSV21a] 还证明了（$\mathcal{D}_N$，$\mathcal{D}_Y$）-RMD$_\alpha(n)$ 的困难性：

定理 *5.8*（[*CGSV21a*，定理 *5.3*]）。对于每个 $k \geq 2$和 $\mathcal{D}_N$，若 $\mathcal{D}_Y \in \Delta(\mathbb{Z}_2^k)$ 满足$\boldsymbol{\mu}(\mathcal{D}_N) = \boldsymbol{\mu}(\mathcal{D}_Y)$，则存在 $\alpha_0 \in (0,1)$，使得对于所有 $\alpha \in (0, \alpha_0)$ $\delta \in (0,1)$，都存在$\tau > 0$和 $n_0 \in \mathbb{N}$，使得对于所有 $n \geq n_0$，任何能够实现至少 δ 优势的（$\mathcal{D}_N, \mathcal{D}_Y$）-*RMD*$_\alpha(n)$ 协议都需要 $\tau\sqrt{n}$ 通信。

与其特殊情形定理 5.7相比，定理 5.8有一些“缺点”。首先，我们不能再使用混合论证来证明（$\mathcal{D}_N$, $\mathcal{D}_Y$）-sRMD$_{\alpha,\ T}(n)$ 的困难性
由于数据处理不等式不再适用。因此，我们只能设法证明并行随机掩码检测问题（$\mathcal{D}_N, \mathcal{D}_Y$）-pRMD$_{\alpha,T}(n)$ 的下界。这是一个由（$T+1$）名玩家参与的博弈，结构如下：Bob1, . . . , Bob$_T$ 各自获得一个独立的 RMD 输入，并向“裁判”Carol 发送一条消息；Carol 必须判断他们属于哪种情况。尤其是，与 sRMD 博弈不同，Bob$_t$ 们之间不能以任何方式通信。根据独立性，RMD 的困难性（即定理 5.8）可立即推广到 pRMD 的困难性，但这种“并行”通信博弈只能排除草图算法。

此外，定理 5.8 的证明要复杂得多。基本思路如下。我们可以把 $\mathbb{Z}_2^k$ 看作一个格：它具有一个偏序，即逐项比

较，记为 $\leq$，其中我们定义 $0 \leq 1$。此外，我们可以将 $\mathbf{u} \wedge \mathbf{v}$、$\mathbf{u} \vee \mathbf{v} \in \mathbb{Z}_2^k$定义为 $\mathbf{u}$、$\mathbf{v}$ 的逐项 AND 和 OR。 $\in \mathbb{Z}_2^k$.[‖] 如果 $\mathbf{u} \not\leq \mathbf{v}$ 且 $\mathbf{v} \not\leq \mathbf{u}$，我们称 $\mathbf{u}$ 和 $\mathbf{v}$ 不可比较，记为 $\mathbf{u} \parallel \mathbf{v}$。现在，给定一个支撑集为两个不可比较元素 $\mathbf{u} \parallel \mathbf{v}$ 的分布 $\mathcal{D} \in \Delta(\mathbb{Z}_2^k)$，我们可以考虑极化分布 $\mathcal{D}_{\mathbf{u},\mathbf{v}}$。令 $\epsilon = \min\{\mathcal{D}(\mathbf{u}), \mathcal{D}(\mathbf{v})\}$，将 $\mathcal{D}(\mathbf{u})$ 和 $\mathcal{D}(\mathbf{v})$ 减少 ϵ，并将 $\mathcal{D}(\mathbf{u} \wedge \mathbf{v})$ 和 $\mathcal{D}(\mathbf{u} \vee \mathbf{v})$ 增加 ϵ。注意，极化保留边缘分布，即 $\boldsymbol{\mu}(\mathcal{D}) = \boldsymbol{\mu}(\mathcal{D}_{\mathbf{u},\mathbf{v}})$。[CGSV21a] 证明了关于此操作的两个关键定理：

i. $(\mathcal{D}, \mathcal{D}_{\mathbf{u},\mathbf{v}})$-RMD$_\alpha(n)$ 需要 $\Omega(\sqrt{n})$ 的通信。这本质上是因为我们可以将 $\mathcal{D}$ 和 $\mathcal{D}_{\mathbf{u},\mathbf{v}}$ 写成同一基础分布的“混合”

$$\mathcal{D} = (1-2\epsilon)\mathcal{D}_0 + 2\epsilon\,\mathcal{U}_{\{\mathbf{u},\mathbf{v}\}} \text{ and } \mathcal{D}_{\mathbf{u},\mathbf{v}} = (1-2\epsilon)\mathcal{D}_0 + 2\epsilon\,\mathcal{U}_{\{\mathbf{u}\wedge\mathbf{v},\mathbf{u}\vee\mathbf{v}\}}$$

$\mathcal{D}_0 \in \Delta(\mathbb{Z}_2^k)$，这（大致上）使我们能够从 $(\mathcal{U}_{\{\mathbf{u},\mathbf{v}\}}, \mathcal{U}_{\{\mathbf{u}\wedge\mathbf{v},\mathbf{u}\vee\mathbf{v}\}})$-RMD$_\alpha(n)$ 归约。此外，在 $\mathbf{u}$ 和 $\mathbf{v}$不同的坐标上，$\mathcal{U}_{\{\mathbf{u},\mathbf{v}\}}$ 和 $\mathcal{U}_{\{\mathbf{u}\wedge\mathbf{v},\mathbf{u}\vee\mathbf{v}\}}$ 的边缘分布均为零；因此，我们可以（大致上）将这些坐标上的“限制”归约，并应用定理 5.7。

ii. 存在某个常数 $C \in \mathbb{N}$，使得在最多应用 C 次极化操作后，$\mathcal{D}$ 将不再可极化，即其支撑集是一个链。此外，对于每个初始边缘向量 $\boldsymbol{\mu} \in [-1,1]^k$，这个最终分布都是唯一的；我们称之为“典范分布”，记作 $\mathcal{D}_{\boldsymbol{\mu}}$。

综合第 i 项和第 ii 项即可证明定理 3.3。事实上，给定两个具有相匹配边缘分布 $\boldsymbol{\mu}(\mathcal{D}_N) = \boldsymbol{\mu}(\mathcal{D}_Y)$ 的初始分布 $\mathcal{D}_N, \mathcal{D}_Y \in \Delta(\mathbb{Z}_2^k)$，我们可以利用第 ii 项反复对二者 $\mathcal{D}_Y$ 和 $\mathcal{D}_N$ 进行极化，从而得到一条长度至多为 $2C$ 的分布“路径”，经由它们共有的典范分布将二者连接起来，并且每一对相邻分布都是极化的结果；接着，第 i 项意味着每一对这样的分布都具有 RMD 困难性；最后，我们应用三角不等式，得出路径端点具有 RMD 困难性，即 $\mathcal{D}_Y$ 和 $\mathcal{D}_N$。更多细节请参见 [CGSV21a, §7]。

最后，我们提到，[CGSV21b]在更一般的[CGSV21a] 设定下，重新证明了迄今为止我们讨论过的所有算法结果和困难性结果，即 最大约束满足问题$(\mathcal{F})$

[‖]在格的语境中，$\wedge$ 和 $\vee$ 通常分别称为并 和交 运算。

由一般字母表 $\mathbb{Z}_q$ 上的谓词族定义的问题。我们简要介绍其中一些结果。对于分布 $\mathcal{D} \in \Delta(\mathbb{Z}_q^k)$，令 $\boldsymbol{\mu}(\mathcal{D}) \in (\Delta(\mathbb{Z}_q))^k$ 表示将其投影到各个坐标后得到的“边缘分布”向量。若 $\mathcal{D}$ 满足 $\boldsymbol{\mu}(\mathcal{D}) = (\mathcal{U}_{\mathbb{Z}_q})^k$，则称其具有单变量独立性；若存在 $\mathcal{F}' \subseteq \mathcal{F}$ 使得 $\rho(\mathcal{F}') = \rho(\mathcal{F})$，且对每个 $f \in \mathcal{F}'$，都存在一个支撑在 $f^{-1}(1)$ 上的单变量独立分布 $\mathcal{D}_f \in \Delta(\mathbb{Z}_q^k)$，则称其弱支撑单变量独立性。在这种情况下，[CGSV21b, Theorem 2.17] 表明，最大约束满足问题$(\mathcal{F})$在 $\sqrt{n}$ 空间中具有流式近似抗性。更一般地，[CGSV21b] 沿着定理 5.2 的思路，基于满足如下条件的分布 $\mathcal{D}_N, \mathcal{D}_Y \in \Delta(\mathcal{F} \times \mathbb{Z}_q^k)$，为最大约束满足问题$(\mathcal{F})$证明了一个二分定理：投影到每个 $f \in \mathcal{F}$ 后，边缘分布 $\boldsymbol{\mu}$ 相匹配。为这些分布定义 λ, β, γ 超出了本论文的讨论范围——参见 [CGSV21b, §2.1] ——但我们要指出，算法结果现在要求计算一个 $n \times k$ 矩阵所谓的“$(1, \infty)$-范数”，即由每行最大元素组成的向量的 1-范数；这对应于贪心地将每个变量赋值为它“最想要”的 $\mathbb{Z}_q$ 中的元素，而困难性结果则通过一种更复杂的“极化”版本得以证明。

5.2 Lower bounds for linear-space streaming

本节讨论 Chou、Golovnev、Sudan、Velingker 和 Velusamy 最近提出的线性空间流处理下界 [CGS+22]，该结果将 Kapralov 和 Krachun 的最大割下界 [KK19] 推广到一大类所谓的“宽”约束满足问题。我们将先介绍这些下界的一些表述，以便证明针对排序约束满足问题的下界，相关内容见第 6 章。（具体而言，我们主要限定在单谓词情形 $|\mathcal{F}| = 1$；一般形式见 [CGS+22]。）

固定 k，$q \in \mathbb{N}$，并令 $\mathcal{C} \subseteq [q]^k$ 表示常数向量构成的子空间（即，对于 $a \in \mathbb{Z}_q$，向量 $(a, \ldots\ldots, a)$）。粗略来说，谓词 $f\colon \mathbb{Z}_q^k \to \{0,1\}$ 称为“宽”，是指其支撑集与 $\mathbb{Z}_q^k$ 中的 $\mathcal{C}$ 的某个陪集有较大的交集。更准确地说，对于 $\mathbf{b} \in [q]^k$，令

$$\omega_{\mathbf{b}}(f) \stackrel{\text{def}}{=} \mathop{\mathbb{E}}_{\mathbf{c} \sim \mathcal{U}_{\mathcal{C}}} [f(\mathbf{c} + \mathbf{b})], \tag{5.9}$$

并将 f 的宽度定义为

$$\omega(f) \stackrel{\text{def}}{=} \max_{\mathbf{b} \in \mathbb{Z}_q^k} (\omega_{\mathbf{b}}(f)) .$$

CGS 中宽 [谓词+22] 的下界基于以下通信问题，该问题称为顺序隐式随机化移位检测（*siRSD*）：**

定义 5.10 (siRSD)。 设 $2 \le q, k \in \mathbb{N}$, $\alpha \in (0, 1)$，以及 $T, n \in \mathbb{N}$。那么，(k, q)-*siRSD*$_{\alpha, T}(n)$ 是如下的 T 人单向通信问题，参与者为 *Bob*$_1$、……、*Bob*$_T$：

- 示例 $\mathbf{x}^* \sim \mathcal{U}_{\mathbb{Z}_q^n}$。
- 每个 *Bob*$_t$ 都会收到一个从 $\mathcal{M}_{k,\alpha}(n)$ 中采样得到的邻接矩阵 $M_t \in \{0,1\}^{k\alpha n \times n}$，以及一个向量 $z(t) \in \mathbb{Z}_q^{k\alpha n}$，它为 M_t 的每条边标注如下：– 是情形：$z(t) = M_t x^* + b(t)$，其中 $b(t) \sim \mathcal{U}_C^{\alpha n}$。– 否情形：$z(t) \sim (\mathcal{U}_{\mathbb{Z}_q}^k)^{\alpha n}$。
- 每个 *Bob*$_t$ 都可以向 *Bob*$_{t+1}$发送一条消息，最后，*Bob*$_T$ 必须判断他们处于是情形还是否 情形。

为了对这个定义作一些解释，对于每个玩家 Bob$_t$ 和边索引$\ell \in [\alpha n]$，令 $\mathbf{e}(t, \ell)$ 表示 M_t 中的第 ℓ条边，并将 $\mathbf{z}(t) = (\mathbf{z}(t, 1) \ldots, \mathbf{z}(t, \alpha n))$ 记作 $\mathbf{z}(t, \ell) \in \mathbb{Z}_q^k$。在是情形中，每个块 $\mathbf{z}(t, \ell)$ 都等于 $\mathbf{x}^*|_{\mathbf{e}(t,\ell)}$ 加上一个随机偏移量（即 $\mathcal{C}$中的一个随机元素）；在否情形中，每个块 $\mathbf{z}(t, \ell)$ 都是均匀随机的。另请注意，这个问题是“隐式的”，就像我们在 §3.4.3 中描述的 siBPD 问题一样，也就是说，没有 Alice 知道隐藏赋值。

此外，考虑 $k = q = 2$ 的情形。对于 $t \in [T], \ell \in [\alpha n]$，如果 $\mathbf{e}(t, \ell) = (u, v)$，那么在是情形中，Bob$_t$ 的第 ℓ个块 $\mathbf{z}(t, i) = (x^*_u + b(t)_\ell, x^* + b(t)_\ell)$，其中 $b(t)_\ell \sim \mathcal{B}_{\frac{1}{2}}$；– 因此，$\mathbf{z}(t, \ell)$ 在信息论意义上等价于比特 $x^*_u + x^*_v$。另一方面，在否情形中，$\mathbf{z}(t, i)$ 就是均匀随机的。因此，在 $k = q = 2$ 情形下，(k, q)-siRSD$_{\alpha,T}(n)$ 等价于我们在 §3.4 中描述的 siBPD$_{\alpha,T}(n)$ 问题；该问题曾被 [KK19] 用于证明近似最大割的线性空间困难性。

下界的技术核心 [CGS+22] 是针对以下siRSD的困难性结果：

定理 5.11 ([CGS+22，定理 3。2])。 对于每个 $2 \le q$，$k \in \mathbb{N}$，存在 $\alpha_0 \in (0, 1)$使得对于每个 $\delta \in (0, 1)$，$\alpha \in (0, \alpha_0)$，$T \in \mathbb{N}$，存在 $\tau > 0$ 和 $n_0 \in \mathbb{N}$，使得

**[CGS+22] 更一般地定义了一种“（序贯）隐式随机掩码检测”问题，但仅证明了当掩码为均匀移位（即 $\mathcal{C}$ 中的均匀分布元素）时的困难性。

对于所有 $n \geq n_0$，任何针对(k, q)-*siRSD*$_{\alpha,\ \tau}(n)$ 且优势至少为 δ 的协议，都需要τn 通信。

以下构造及分析分别推广了 构造 3.6 和 引理 3.7 关于最大割的结果：

构造 *5.12*（从 *siRSD* 到 *Max-CSP*($\{f\}$) 的通信到流式归约）。令 $\mathbf{b} \in \mathbb{Z}_q^k$ *and* $f : \mathbb{Z}_q^k \to \{0,1\}$。对于每个 $t \in [T]$，*Bob*$_t$ 的归约函数 R_t 按如下方式输出一个实例 Ψ_t：对于每个 $e(t,\ell) \in M_t$，以及 $z(t)$ 中对应的块 $z(t,\ell) \in \mathbb{Z}_q^k$，当且仅当 $z(t,\ell) - \mathbf{b} \in \mathcal{C}$ 时，*Bob*$_t$ 将 $e(t,\ell)$ 添加到 Ψ_t。

引理 *5.13*。对于所有 $f: \mathbb{Z}_q^k \to \{0,1\}$, $\alpha \in (0,\ 1)$，$\epsilon \in (0,\ 1\ 2)$，以及 $\mathbf{b} \in \mathbb{Z}_q^k$，存在$T$，$n_0 \in \mathbb{N}$，使得对每个 $n \geq n_0$，以下结论成立。令 $\mathcal{Y}$ 和 $\mathcal{N}$ 分别表示 (k, q)-*siRSD*$_{\alpha,T}(n)$ 的是分布和否分布，并令 $(R_0, \ldots, R_T)$ 为构造 *5.12* 中的归约函数。则

$$\Pr_{\Psi\sim(R_0,\ldots,R_T)\circ\mathcal{Y}}[val_\Psi \leq \omega_{\mathbf{b}}(f) - \epsilon] \leq \exp(-n) \ \ and \ \ \Pr_{\Psi\sim(R_0,\ldots,R_T)\circ\mathcal{N}}[val_\Psi \geq \rho(f) + \epsilon] \leq \exp(-n).$$

综上，定理 5.11 和引理 5.13 可得以下推论（稍加努力即可将其推广到所有谓词族）：

推论 *5.14* ([CGS+22，定理 4.3])。对于每个 $f: \mathbb{Z}_q^k \to \{0,1\}$ 和常数$\epsilon > 0$，任何以 $(\rho^{\omega(f)}_f() + \epsilon)$-近似最大约束满足问题$(\{f\})$的流式算法都需要 $\Omega(n)$ 空间。此外，对于每个谓词族 $\mathcal{F}$，以 $(\rho^{\omega}(\mathcal{F}) + \epsilon)$- 近似最大约束满足问题 $(\mathcal{F})$ 的流式算法都需要 $\Omega(n)$ 空间，其中 $\omega(\mathcal{F})\ def = min_{f\in\mathcal{F}}\omega(f)$。

注意到根据定义，对于每个 f:-$\mathbb{Z}_q^k \to \{0,1\}$，都有 $\omega(f) \geq \frac{1}{q}$，因此我们得到另一个推论，将每个谓词族 $\mathcal{F}$ 的线性空间流处理可近似性限制在区间 $[\rho(\mathcal{F})\ q \cdot \rho(\mathcal{F})]$ 内：

推论 5.15 ([CGS+22，定理 1。2])。对于每个谓词族 $\mathcal{F}$ 定义在 $\mathbb{Z}_q$ 上，以及每个 $\epsilon > 0$，任何以 $(q \cdot \rho(\mathcal{F}) + \epsilon)$ 近似 最大约束满足问题$(\mathcal{F})$ 的流式算法，至少需要 $\Omega(n)$空间。

最后，我们指出，从定性角度看，证明线性空间下界（即 定理 5.11，或其特殊情形 定理 3.18 （针对）最大割）的主要障碍在于“证——

明低傅里叶权重界以 $\left(\frac{\zeta c}{\ell}\right)^{\ell/2}$”相比于引理 2.4 更为困难。（关于最大割的 siBPD 特殊情形，参见评注 3.14。）尽管引理 2.4 本身是紧的，但如果我们考虑 Bob_t 的第二个输入的分布 $\mathcal{Z}_{A_t,M_t}$，其中 M_t 是 Bob_t 的匹配，而 A_t 是与 Bob_{t-1} 输出的消息一致的 $\mathbf{x}^*$ 的集合，并直接应用引理 2.4，我们就会立即无法证明线性空间下界。关键观察是，我们可以做得比直接应用引理 2.4 更好，因为 $\mathcal{Z}_{A_t,M_t}$ 是一个“结构化”的分布：当我们抽取 $\mathbf{z}(t) \sim \mathcal{Z}_{A_t,M_t}$时，$\mathbf{z}(t)$ 的每个条目只告诉我们 $\mathbf{x}^*$ 中若干条目之和的信息。最终，证明通过归纳展示集合 A_t 的指示变量满足某些傅里叶权重界（以高概率），从而取得成功；具体做法是将引理 2.4 应用于 $\mathcal{Z}_{A_t,M_t}$ 的一个经过谨慎定义的“约化”版本。然而，精确表述这些界，并提出用于证明它们的恰当归纳假设，远比 BPD 情形复杂；详情参见 [CGS+22, §5]。

II

贡献

6

排序约束满足问题

> 一个自然的思路是将 MAS [问题] 表述为一个约束满足问题。MAS 与约束满足问题颇为相似：每个顶点都是一个变量，其取值来自定义域 $[n]$，而每条有向边都是两个变量之间的一个约束。不过，约束满足问题的定义域 $[n]$ 并非固定不变，而是会随着输入规模的增大而扩大。我们在此强调，这并非表面上的区别，而是该问题的本质特征。
>
> ——Guruswami, H˚astad, Raghavendra, Manokaran 和 Charikar [GHM+11]

Scheduling problems can be modeled作为 排序约束满足问题（*OCSP*），它是约束满足问题的变体，其中赋值对应于 n 对象的排序，而约束则规定对象小集合中允许的排序。也就是说，在调度解释中，OCSP 的目标是为 n “任务”找到最佳“调度”，并满足 诸如“任务 j 必须排在任务 i 和任务 k之间”之类的优先约束。在本章中，我们证明了一个适用于每种 OCSP 的强流式近似抗性结果，该结果来自我们与 Sudan 和 Velusamy 的合作研究 [SSV21]：对于每种 OCSP，线性空间流式算法都无法优于平凡近似比（见

定理 6.1 下文）。不过，我们首先正式定义 OCSP 及其两个具体例子： 最大无环子图 和 最大介数 问题。

6.1 OCSPs: Definitions, motivations, history

向量 $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n) \in [n]^n$ 是一个排列，当且仅当其所有元素都互不相同，也就是说，如果$\sigma_i = \sigma_{i'}$，那么 $i = i'$。令 $\mathfrak{S}_n \subseteq [n]^n$ 表示所有排列的集合。* 我们将排列 $\boldsymbol{\sigma} \in \mathfrak{S}_n$ 解释为对 n 个对象的一种排序，这些对象的标签为 1 到 n，并将第i个对象放在位置 σ_i。†

设$\mathbf{a} = (a_1, \ldots, a_k) \in \mathbb{Z}^k$ 是一个由 k 个整数组成的元组。我们定义符号$\mathbf{ord(a)} \in \mathfrak{S}_k \cup \{\perp\}$来表示$\mathbf{a}$各项的排序，定义如下：如果$\mathbf{a}$的各项并非全都互不相同，那么 $\mathbf{ord(a)} = \perp$；否则，$\mathbf{ord(a)}$ 是唯一满足$a_{\pi_1^{-1}} < \cdots < a_{\pi_k^{-1}}$的排列 $\boldsymbol{\pi} \in \mathfrak{S}_k$，其中 $\boldsymbol{\pi}^{-1}$ 是 $\boldsymbol{\pi}$ 的逆排列。特别地，如果$\mathbf{a} \in \mathfrak{S}_k$是一个排列，那么$\mathbf{ord(a)} = \mathbf{a}$。

对于排列 $\boldsymbol{\sigma} \in \mathfrak{S}_n$和一组由互不相同的索引组成的 k 元组 $\mathbf{j} = (j_1, \ldots, j_k) \in [n]^k$，我们定义诱导排列 $\boldsymbol{\sigma}|_{\mathbf{j}} \stackrel{\text{def}}{=} \mathbf{ord}(\sigma_{j_1}, \ldots, \sigma_{j_k})$。例如，排列 $\boldsymbol{\sigma} = (5,1,3,2,4) \in \mathfrak{S}_5$ 将第三个对象放在第三个位置；又由于 $\boldsymbol{\sigma}|_{(1,5,3)} = (3,2,1) \in \mathfrak{S}_3$，可知若只取第一个、第三个和第五个对象，那么第五个对象处于第二个位置。

对于 $k \leq 2 \in \mathbb{N}$，排序谓词 $\Pi : \mathfrak{S}_k \to \{0,1\}$ 将排序约束满足问题 Max-OCSP(Π)定义如下。一个作用于 $n \in \mathbb{N}$ 个变量的约束由一个 k 元组$\mathbf{j} = (j_1, \ldots, j_k) \in [n]^k$ 构成，其中包含互不相同的索引。‡ 若赋值 $\boldsymbol{\sigma} \in \mathfrak{S}_n$ 满足 $C = \mathbf{j}$，当且仅当 $\Pi(\boldsymbol{\sigma}|_{\mathbf{j}}) = 1$。Max-OCSP($\Pi$) 的一个实例 Φ 由 m 个约束 $(C_\ell = (\mathbf{j}(\ell))_{\ell \in [m]}$ 构成；赋值 $\boldsymbol{\sigma} \in \mathfrak{S}_n$ 在 Φ 上的值，记作 $\mathsf{ordval}_\Phi(\boldsymbol{\sigma})$，是由 $\boldsymbol{\sigma}$ 满足的约束的（分数）权重，即，

$$\mathsf{ordval}_\Phi(\boldsymbol{\sigma}) \stackrel{\text{def}}{=} \frac{1}{m} \sum_{\ell=1}^{m} \Pi(\boldsymbol{\sigma}|_{\mathbf{j}(\ell)}).$$

*我们对排列采用这种非标准的“向量记法”，以强调它与 CSP 赋值的类比；CSP 赋值来自 $[q]^n$。

†即，这是一种诠释性约定；另一种约定则是：第 σ_i 个对象位于位置 i。

‡为简便起见，同时由于我们要证明下界，因此这里只定义无权的排序约束满足问题实例。

Φ 的值记作 ordval_Φ，它是任意赋值可取得的最大值，即，

$$\mathsf{ordval}_\Phi \stackrel{\text{def}}{=} \max_{\boldsymbol{\sigma}\in\mathfrak{S}_n} \left(\mathsf{ordval}_\Phi(\boldsymbol{\sigma})\right).$$

我们在流式设置下，考虑 α-近似最大排序约束满足问题(Π)，以及区分问题 (β,γ)-最大排序约束满足问题(Π)；其设置与标准的非排序约束满足问题情形相同（参见第 2.1 节和2.2 节）。排序约束满足问题与（非排序）约束满足问题之间的一个重要区别在于，排序约束满足问题的解空间具有超指数级的规模 $|\mathfrak{S}_n| = n! \geq (n/e)^n$，而定义在 $\mathbb{Z}_q$ 上的约束满足问题的解空间规模则为指数级 $|\mathbb{Z}_q^n| = q^n$。

最大无环子图问题（MAS）是典型的排序约束满足问题。MAS 是谓词 Π_{MAS}：$\mathfrak{S}_2 \to \{0,1\}$ 对应的 Max-OCSP(Π_{MAS}) 问题，该谓词的支撑集为 (1, 2)。因此，当且仅当 $\sigma_u < \sigma_v$.[§] 时，排序 $\boldsymbol{\sigma} \in \mathfrak{S}_n$ 满足一个 MAS 约束 (u, v)。在调度解释中，当且仅当 u 在 $\boldsymbol{\sigma}$ 中的调度时间早于 v 时，调度 $\boldsymbol{\sigma} \in \mathfrak{S}_n$ 满足约束 (u, v)。Karp 对 21 个 NP 完全问题的经典枚举 [Kar72] 包含这样一个问题：给定 MAS 的一个实例 Φ 和 $\gamma \in [0,1]$，判断 $\mathsf{ordval}_\Phi \geq \gamma$.[¶]。已有多项研究 [New00; AMW15; BK19] 探讨了 MAS 近似问题的 NP 困难性；[BK19] 证明，对于任意 $\epsilon > 0$，$(\frac{2}{3} + \epsilon)$-近似 MAS 都是 NP-困难的。

另一个值得关注的排序约束满足问题是最大介数问题 Max-Btwn def = Max-OCSP(Π_{Btwn})，其中 Π_{Btwn}：$\mathfrak{S}_3 \to \{0,1\}$ 在 (1, 2, 3) 和 (3, 2, 1) 上受支撑。因此，当且仅当 $\sigma_u < \sigma_v < \sigma_w$ 或 $\sigma_w < \sigma_v < \sigma_u$ 时，排序 $\boldsymbol{\sigma} \in \mathfrak{S}_n$ 满足 Max-Btwn 约束 (u, v, w)。该有序约束满足问题由 Opatrny [Opa79], 提出，他证明了即便要判定 $\mathsf{ordval}_\Phi = 1$ 是否成立也是 NP-困难的。文献 [CS98；AMW15] 研究了 Max-Btwn 的 NP 困难近似性；后者表明，对任意 $\epsilon > 0$，将 Max-Btwn 近似到 $(\frac{1}{2} + \epsilon)$ 是 NP-困难的。

[§]与标准的 CSP 情形一样，MAS 的一个实例 Φ 对应于一个有向约束图$G(\Psi)$，其中每个约束 (u, v) 都对应一条有向边。任意排序 $\boldsymbol{\sigma} \in \mathfrak{S}_n$ 都会在 $G(\Psi)$ 中诱导出一个无环子图，该子图由相对于 $\boldsymbol{\sigma}$ 的所有正向边组成，也就是说，这些边满足$\sigma_u < \sigma_v$。因此，val_Ψ 对应于衡量 $G(\Psi)$ 中最大无环子图的大小，这也解释了“最大无环子图”这一名称。

[¶]此外，在经典情形下，可以使用深度优先搜索来判断 $\mathsf{val}_\Psi = 1$，即检验 $G(\Psi)$ 是否为 无环。然而，在流式设置下，已知无环性检测需要 $\Theta(n^2$ 空间 [CGMV20]。

然而，与约束满足问题的情形类似，对于每个 $\Pi : \mathfrak{S}_k \to \{0,1\}$，定义$\rho(\Pi)$ def $= \mathbb{E}_{\boldsymbol{\pi} \sim \mathcal{U}_{\mathfrak{S}_k}}[\Pi(\boldsymbol{\pi})]$, ，每个 Max-OCSP(Π) 实例的值至少为 $\rho(\Pi)$，因此每个 Max-OCSP(Π) 都可以平凡地近似到 $\rho(\Pi)$。同样，对于各种谓词 Π 和算法类别 $\mathcal{S}$，我们考察 Max-OCSP(Π) 是否具有近似抗性（对于每个 $\epsilon > 0$， $\mathcal{S}$ 中没有算法能将 Max-OCSP(Π) 近似到 $(\rho(\Pi) + \epsilon)$），或是否可实现非平凡近似（存在一种 $(\rho(\Pi) + \epsilon)$-近似算法）。注意，$\rho(\Pi_{\mathsf{MAS}}) = \frac{1}{2}$，而且$\rho(\Pi_{\mathsf{Btwn}}) = \frac{1}{3}$；因此，[AMW15；BK19] 的结果不足以证明 MAS 或 Max-Btwn 的非平凡近似是 NP-困难的。不过，Guruswami、H˚astad、Manokaran、Raghavendra 和 Charikar [GHM+11] 证明，对于任意 $\Pi : \mathfrak{S}_k \to \{0,1\}$ 和 $\epsilon > 0$，将 Max-OCSP(Π) 近似到 $(\rho(\Pi) + \epsilon)$ 是唯一游戏困难的。

我们的工作 [SSV21] 的结果是，最大排序约束满足问题(Π) 在流式设置中同样具有近似抗性，即使面对 线性空间 算法：

定理 6.1 ([SSV21])**.** 对于任意 $k \leq 2 \in \mathbb{N}$、谓词 $\Pi : \mathfrak{S}_k \to \{0,1\}$，以及 $\epsilon > 0$，存在 $\tau > 0$ 使得，任何以$(\rho(\Pi) + \epsilon)$近似最大排序约束满足问题(Π) 的流式算法，至少使用 τn 空间。

该定理中的空间界在对数因子范围内是最优的；事实上，正如~约束满足问题的情形一样，备注 3.19 上文指出，对每个 $1 - \epsilon$，都存在 $\epsilon > 0$，使得在 $O(n)$ 空间内即可实现近似！

下一节中，我们首先为该定理提供一些直观解释，并指出它与 [GHM+11]的经典证明之间令人惊讶的相似之处。

6.2 Proof outline for MAS

以下观察归功于 Guruswami 等人 [GHM+11]。由于 $\mathfrak{S}_n \subseteq [n]^n$，我们可以将 MAS 视为字母表为 $[n]$、谓词为 $f_{\mathsf{MAS}} : [n]^2 \to \{0,1\}$ 定义为 $f_{\mathsf{MAS}}(b_1, b_2) = \mathbb{1}_{b_1 < b_2}$的约束满足问题。接下来，我们希望利用约束满足问题工具来分析这个谓词。遗憾的是，这个谓词实际上并未定义一个约束满足问题，因为字母表大小n 不是常数。不过，我们可以尝试通过将字母表大小缩减为一个较大的常数来挽救这一策略，并“看看会发生什么”。具体而言，对于 $q \in \mathbb{N}$，令$\iota_q : \mathbb{Z}_q \to [q]$ 表示将 $\mathbb{Z}_q$ 中的元素映射到其在 $\{1, \ldots, q\}$中的代表元的映射。

我们将谓词 $\Pi^{\downarrow q}{}_{\mathsf{MAS}}$： $\mathbb{Z}_q^2 \to \{0,1\}$ 定义为 $\Pi^{\downarrow q}{}_{\mathsf{MAS}}(b_1,\ b_2) = \mathbb{1}_{\iota_q(b_1)<\iota_q(b_2)}$，‖并考虑问题 Max-CSP($\Pi^{\downarrow q}{}_{\mathsf{MAS}}$)。

在上一节中，我们观察到，MAS 可以被解释为一个调度问题，其中，当且仅当 u 的位置早于 v 的位置时，约束 (u,v) 才得到满足。在这种视角下，Max-CSP($\Pi^{\downarrow q}{}_{\mathsf{MAS}}$) 是一种“批处理式”调度问题，其目标是将 n 任务分配到 $q = O(1)$ 个批次中，并且，当且仅当 u 所属的批次早于 v 所属的批次时，约束 (u,v) 才得到满足。因此，Max-CSP($\Pi^{\downarrow q}{}_{\mathsf{MAS}}$) 是 MAS 的一个更粗粒度的版本，因为在 MAS 中，即使在同一个批次内，我们也可以灵活地分配执行顺序。

为使这一点更加精确，对于 MAS 的每个实例 Φ 和 $q \in \mathbb{N}$，令 $\Phi^{\downarrow q}$ 表示具有完全相同约束列表的 Max-CSP($\Pi^{\downarrow q}{}_{\mathsf{MAS}}$) 实例。反过来，给定 Max-CSP($\Pi^{\downarrow q}{}_{\mathsf{MAS}}$) 的一个实例 Ψ，令 $\Psi^{\uparrow}$ 表示具有相同约束列表的 MAS 实例。操作 $\downarrow q$(q-粗化) 和 $\uparrow$(细化) 互为逆操作。此外，对于 Max-CSP($\Pi^{\downarrow q}{}_{\mathsf{MAS}}$) 的一个赋值 $\mathbf{x} = (x_1,\dots,x_n) \in \mathbb{Z}_q^n$ 和 $b \in \mathbb{Z}_q$，令 $\mathbf{x}^{-1}(b) \stackrel{\text{def}}{=} \{i \in [n] : x_i = b\}$。（如果 $\mathbf{x}$ 是一个分批调度，那么 $\mathbf{x}^{-1}(b)$ 就是批次 b 中的作业集合。）于是，我们有以下结论：

命题 6.2。对于每个 $q \in \mathbb{N}$ 以及最大约束满足问题($\Pi^{\downarrow q}{}_{\mathsf{MAS}}$)的实例 Ψ，

$$\mathit{val}_{\Psi} \le \mathit{ordval}_{\Psi^{\uparrow}}.$$

证明。对于 $\mathbf{x} \in \mathbb{Z}_q^n$，令 $s_b = |\mathbf{x}^{-1}(b)|$，对每个 $b \in \mathbb{Z}_q$ 均如此。我们通过如下方式构造一个排序 $\mathbf{x}^{\uparrow} \in \mathfrak{S}_n$：将 $\mathbf{x}^{-1}(1)$ 分配到最前面的 s_0 个位置（顺序任意），然后迭代地将接下来的 s_b 个位置分配给 $\mathbf{x}^{-1}(b)$，其中 $b \in \{2,\dots,q\}$。于是，若 $\iota_q(x_u) < \iota_q(x_v)$，则根据构造，$\mathbf{x}^{\uparrow}_u < \mathbf{x}^{\uparrow}_v$。因此，$\mathrm{val}_{\Psi}(\mathbf{x}) \le \mathrm{ordval}_{\Psi^{\uparrow}}(\mathbf{x}^{\uparrow})$，命题 6.2 得证。 □

那么，粗化这一概念如何帮助我们证明MAS 具有流式近似抗性呢？回顾 Chou 等人 [CGS+22] 排除了对 $\omega(\mathcal{F})/\rho(\mathcal{F}) + \epsilon$近似的线性空间流式下界，这些下界针对的是 最大约束满足问题$(\mathcal{F})$（参见 推论 5.14 以及上文 §5.2 中的定义）。固定一个较大的常数 $q \in \mathbb{N}$。那么，平凡的近似阈值

‖请注意，比较运算符并非先验地 为 $\mathbb{Z}_q$ 定义，而只为 $\mathbb{Z}$ 定义。按照我们刚刚选定的约定，$\iota(0) = q$，尤其是 $\iota(0) > \iota(1)$。此选择是为了与记号$[n] = \{1,\dots,n\}$兼容，可以放心忽略。

对于最大约束满足问题($\Pi^{\downarrow q}_{\mathsf{MAS}}$)，其值为

$$\rho(\Pi^{\downarrow q}_{\mathsf{MAS}}) = \Pr_{(b_1,b_2)\sim\mathcal{U}_{\mathbb{Z}_q^2}}[\iota_q(b_1) < \iota_q(b_2)] = \frac{q(q-1)}{2q^2} \approx \frac{1}{2}.$$

另一方面，对于 $\mathbf{b} = (1,2) \in \mathbb{Z}_q^2$，我们有

$$\omega_{\mathbf{b}}(\Pi^{\downarrow q}_{\mathsf{MAS}}) = \Pr_{c\sim\mathcal{U}_{\mathbb{Z}_q}}[\iota_q(c) < \iota_q(c+1)] = \frac{q-1}{q} \approx 1,$$

因为 $\iota_q(c) \not< \iota_q(c+1)$ 的唯一可能情况是 $c = 0$。因此，最大约束满足问题($\Pi^{\downarrow q}_{\mathsf{MAS}}$) 对线性空间流式算法几乎具有近似抗性！事实上，定理 5.11、构造 5.12和引理 5.13 共同给出了两个分布 $\mathcal{Y}'$ 和 $\mathcal{N}'$，它们定义在 Max-CSP($\Pi^{\downarrow q}_{\mathsf{MAS}}$) 的实例上，并且 (1) 区分它们需要 $\Omega(n)$ 空间；(2) 它们的值分别以高概率接近 $\omega_{\mathbf{b}}(\Pi^{\downarrow q}_{\mathsf{MAS}}) \approx 1$ 和 $\rho(\Pi^{\downarrow q}_{\mathsf{MAS}}) \approx \frac{1}{2}$。

现在回到 MAS，命题 6.2 表明，对于 $\Psi \sim \mathcal{Y}'$，$\mathrm{ordval}_{\Psi\uparrow} \geq \mathrm{val}_{\Psi}$，因此以高概率有 $\mathrm{ordval}_{\Psi\uparrow} \approx 1$。因此，要证明 MAS 具有近似抗性，只需证明对于 $\Psi \sim \mathcal{N}'$，$\mathrm{ordval}_{\Psi\uparrow} \approx \frac{1}{2}$——也就是说，命题 6.2中的不等式并非过于宽松——以高概率成立。为此，我们需要实际考察 $\mathcal{N}'$ 的结构。回想一下，$\mathcal{N}'$ 是通过将构造 5.12 与 $\mathrm{siRSD}_{T,\alpha}$ 的**否**分布复合而定义的。** 我们提出以下（非正式）命题：

命题 6.3。对于固定的 $\epsilon > 0$，并且在 q 的取值足够大时，

$$\Pr_{\Psi\sim\mathcal{N}'}[\mathit{ordval}_{\Psi\uparrow} > \mathit{val}_{\Psi} + \epsilon] \leq \exp(-n).$$

命题 6.3 足以完成证明，因为我们知道$\mathrm{val}_{\Psi} \approx \frac{1}{2}$ 以高概率（关于 $\Psi \sim \mathcal{N}'$）。命题 6.3 将在下文作为 引理 6.7针对一般有序约束满足问题正式陈述并证明，但现在我们先给出证明概要。对于任意 $\boldsymbol{\sigma} \in \mathfrak{S}_n$，定义赋值$\boldsymbol{\sigma}^{\downarrow q} \in \mathbb{Z}_q^n$ 如下：$\sigma_i^{\downarrow q} = \lceil q\sigma_i/n \rceil$。在调度解释中，$\boldsymbol{\sigma}^{\downarrow q}$的第一批包含由 $\boldsymbol{\sigma}$调度的前 $\approx n/q$ 个任务，第二批包含接下来的 $\approx n/q$ 个任务，依此类推。于是我们有：

一个自然的想法是，沿用 **否-情形分析，例如 最大割 (参见 §3.1)，利用集中界证明：对于每个固定的排序 $\boldsymbol{\sigma} \in \mathfrak{S}_n$，$\Pr_{\Psi\sim\mathcal{N}'}[\mathrm{ordval}_{\Psi\uparrow}(\boldsymbol{\sigma}) > \frac{1}{2} + \epsilon] \leq \exp(-n)$，然后对 $\boldsymbol{\sigma}$ 取并集界。然而，$|\mathfrak{S}_n| = n!$ 的增长速度快于 $\exp(n)$，因此并集界失效。

证明思路：命题 6.3。只需证明，对于 $1-\exp(-n)$ 的选择，以 Ψ 的概率，对每个 $\boldsymbol{\sigma} \in \mathfrak{S}_n$，$\mathsf{ordval}_{\Psi\uparrow} < \mathsf{val}_\Psi + \epsilon$。约束 (u, v) 被 $\boldsymbol{\sigma}$（在 $\Psi^\uparrow$ 中）满足，但不被 $\boldsymbol{\sigma}^{\downarrow q}$（在 Ψ 中）满足，当且仅当 $\sigma_u < \sigma_v$ 但 $\sigma_u^{\downarrow q} = \sigma_v^{\downarrow q}$。因此，只需对 $[n]$ 的每种划分进行上界估计：将其划分为大小为 $\leq q$ 的子集时，两个变量落在同一子集中的约束所占比例。

考察 siRSD 的定义（定义 5.10）以及生成 $\mathcal{N}'$ 的归约（构造 5.12），我们看到，从 $\mathcal{N}'$ 抽取的 Max-CSP（$\Pi^{\downarrow q}$ MAS）实例中的约束对应于特定模型中的随机图：我们先抽取若干随机匹配的并集，再以概率 q^{-1} 独立地对每条边进行子抽样。高概率下，这个图是一个“小集合扩展器”，具体来说：对于任意大小至多为 q 的子集 $S \subseteq [n]$，至多有 $O(q^{-2})$ 比例的边完全位于 S 内部。（这一事实可以通过集中不等式证明，不过子抽样会让计算略显繁琐——与最大割的分析一样（见 §3.1）。）这种小集合扩展性质还蕴含另一种性质，我们称之为“平衡划分扩展”：对于将 $[n]$ 划分为大小至多为 q 的子集 S_1、……、S_t 的任意划分，至多有 $O(q^{-1})$ 比例的边没有跨越两个不同的子集。因此，令 $q = \Omega(\epsilon^{-1})$ 即可得到所需的界。

□

我们将在下文精确定义小集合扩展和平衡划分扩展（包括超图的情形）；参见 §6.4。

总之，我们可以通过以下方式证明：MAS 具有流式近似抗性：(1) 定义一个恰当的谓词 $\Pi^{\downarrow q}$ MAS，其定义在 $\mathbb{Z}_q$ 上，且比MAS “更粗”（按照命题 6.2中的含义）；(2) 借助已有的约束满足问题工具（即最大约束满足问题（$\Pi^{\downarrow q}$ MAS）的相应问题几乎具有近似抗性，具体依据 [CGS+22]的结果）；(3) 确保将否 实例转化为最大约束满足问题（$\Pi^{\downarrow q}$ MAS）的实例并进行细化时，其值不会增加“太多”（MAS （命题 6.3）。†† 在下一小节中，我们将对这一证明进行形式化，并将其推广到排序约束满足问题。

††同样的“粗化”构造也出现在 Guruswami 等人 [GHM+11] 的经典唯一游戏困难性证明中，但其用法要复杂得多。具体而言，[GHM+11]证明遵循典型的唯一游戏困难性范式：利用给定的谓词（此处为 MAS）构造所谓的独裁测试；这些测试的构造及其可靠性分析基于 Raghavendra 的约束满足问题二分定理 [Rag08]，并将其应用于粗化后的约束满足问题 Max-CSP($\Pi^{\downarrow q}$ MAS)。关于这一经典唯一游戏困难性方法的介绍，可参阅 Khot [Kho10] 和 Trevisan [Tre12] 的综述，以及 [O'D14, §7 和 §11.7]。

6.3 Linear-space approximation resistance of all OCSPs: Proving Theorem 6.1

本节的目标是证明定理 6.1，该定理指出，每个有序约束满足问题对于线性空间流式算法都具有近似抗性。我们首先将上一小节中“粗化”和“细化”的定义推广到所有有序约束满足问题。考虑任意一个排序谓词 $\Pi : \mathfrak{S}_k \to \{0,1\}$，以及字母表大小 $q \in \mathbb{N}$。我们将粗化谓词 $\Pi^{\downarrow q} : \mathbb{Z}_q^k \to \{0,1\}$ 定义为 $\Pi^{\downarrow q}(a_1, \ldots, a_k) = \Pi(\mathbf{ord}(\iota_q(a_1) \ldots, \iota_q(a_k)))$。‡‡对于每个 Max-OCSP(Π) 实例 Φ 和 $q \in \mathbb{N}$，令 $\Phi^{\downarrow q}$ 表示具有相同约束的 Max-CSP($\Pi^{\downarrow q}$) 实例；给定 Max-CSP($\Pi^{\downarrow q}$) 实例 Ψ，令 $\Psi^{\uparrow}$ 表示具有相同约束的 MAS 实例。于是有如下命题 6.2 的对应结论：

引理 6.4。 对于每个 $k, q \leq 2 \in \mathbb{N}$, $\Pi : \mathfrak{S}_k \to \{0,1\}$，以及 *Max-CSP* 的实例 $\Psi\,(\Pi^{\downarrow q})$，

$$val_{\Psi} \leq ordval_{\Psi^{\uparrow}}.$$

证明。对于 $\mathbf{x} \in \mathbb{Z}_q^n$，我们按照命题 6.2 的证明构造 $\mathbf{x}^{\uparrow} \in \mathfrak{S}_n$，它具有“单调性”这一性质，即 $\iota_q(x_u) < \iota_q(x_v) \implies x_u^{\uparrow} < x_v^{\uparrow}$。考虑某个约束 $\mathbf{j} = (j_1, \ldots, j_k)$。如果 x 满足 j（作为 Max-CSP($\Pi^{\downarrow q}$) 约束），那么 $\Pi(\mathbf{ord}(\iota_q(x_{j_1}) \ldots, \iota_q(x_{j_k}))) = 1$。根据单调性，$\mathbf{ord}(\iota_q(x_{j_1}) \ldots, \iota_q(x_{j_k})) = \mathbf{x}^{\uparrow}|_{\mathbf{j}}$，因此 $\mathbf{x}^{\uparrow}$ 满足 j（作为 Max-OCSP(Π) 约束）。因此，$\mathrm{val}_{\Psi}(\mathbf{x}) \leq \mathrm{ordval}_{\Psi^{\uparrow}}(\mathbf{x}^{\uparrow})$。 □

现在，我们从 §5.2“引入”所需的 [CGS+22] 线性空间困难性结果。具体而言，对于 $\Pi : \mathfrak{S}_k \to \{0,1\}$ 和 $k \leq q \in \mathbb{N}$，我们定义一对定义在 Max-CSP($\Pi^{\downarrow q}$) 实例上的困难分布；经过细化（↑）后，它们将成为 Max-OCSP(Π) 的困难实例。固定 $\mathbf{b} \in \mathrm{supp}(\Pi)$，并令 $\mathbf{R}_1, \ldots, \mathbf{R}_T$ 表示构造 5.12 中的归约函数（使用 b 和 Max-CSP($\Pi^{\downarrow q}$)）。对于 $\alpha \in (0,1)$ 和 $T, n \in \mathbb{N}$，令 (k,q)-$\mathcal{Y}_{\alpha,T}(n)$ 和 (k,q)-$\mathcal{N}_{\alpha,T}(n)$ 分别表示 (k,q)-siRSD$_{\alpha,T}(n)$ 的是分布和否分布。接着，令 $(\Pi, \mathbf{b}\ q)$-$\mathcal{Y}'_{\alpha,T}(n)$ $\mathrm{def} = (\mathbf{R}_1, \ldots, \mathbf{R}_T) \circ (k,q)$-$\mathcal{Y}_{\alpha,T}(n)$，并令 $(\Pi, \mathbf{b}\ q)$-$\mathcal{N}'_{\alpha,T}(n)$ $\mathrm{def} = (\mathbf{R}_1, \ldots, \mathbf{R}_T) \circ (k,q)$-$\mathcal{N}_{\alpha,T}(n)$。这些是定义在 Max-CSP($\Pi^{\downarrow q}$) 实例上的分布，线性空间算法无法区分它们（推论 5.14）；并且当 T 和 n 足够大时，它们的值分别以高概率接近 $\omega_{\mathbf{b}}(\Pi^{\downarrow q})$ 和 $\rho(\Pi^{\downarrow q})$（引理 5.13）。

‡‡$\Pi^{\downarrow q}(a_1, \ldots, a_k) = 0$ 在 $\mathbf{ord}(\iota_q(a_1) \ldots, \iota_q(a_k)) = \perp$ 的情况下，即 $a_1, \ldots, a_k$ 并非两两不同。

现在我们有

$$\omega_{\mathbf{b}}(\Pi^{\downarrow q}) \geq 1 - \frac{k-1}{q} \tag{6.5}$$

由于根据定义 $\omega_{\mathbf{b}}(\Pi^{\downarrow q}) = \mathbb{E}_{\mathbf{c}\sim\mathcal{C}}[\Pi^{\downarrow q}(\mathbf{b}+\mathbf{c})]$（见方程 (5.9)），$\Pi^{\downarrow q}(\mathrm{ord}(\mathbf{b})) = 1$根据定义成立，并且 $\mathrm{ord}(\mathbf{b}+\mathbf{c}) = \mathrm{ord}(\mathbf{b})$，除非 $c \geq q-(k-1)$（其中 $\mathbf{c} = (c,\ldots,c)$）。另一方面，

$$\rho(\Pi^{\downarrow q}) = \frac{q!}{(q-k)!q^k}\rho(\Pi) \leq \rho(\Pi), \tag{6.6}$$

由于根据定义 $\rho(\Pi^{\downarrow q}) = \mathbb{E}_{\mathbf{a}\sim\mathcal{U}_{\mathbb{Z}_q^k}}[\Pi^{\downarrow q}(\mathbf{a})]$；$\mathbf{ord}(\mathbf{a}) \neq \perp$（即，$\mathbf{a}$的各项互不相同），其概率为 $\frac{q\cdots(q-(k-1))}{q^k} = \frac{q!}{(q-k)!\,q^k} \leq 1$；如果 $\mathbf{a}$的各项互不相同，则它以概率 $\Pi^{\downarrow q}$ $\rho(\Pi)$满足。我们还提出以下引理，它推广了命题 6.3：

引理 6.7。对于每个 $\Pi : \mathfrak{S}_k \to \{0,1\}$、$\mathbf{b} \in \mathit{supp}(\Pi)$以及 $\epsilon > 0$，存在 $q_0 \in \mathbb{N}$ 和 $\alpha_0 > 0$，使得对于所有 $q \geq q_0 \in \mathbb{N}$ 和 $\alpha \in (0,\alpha_0)$，都存在 $T_0 \in \mathbb{N}$，使得对于所有 $T \geq T_0 \in \mathbb{N}$ 和 $n \in \mathbb{N}$，

$$\Pr_{\Psi\sim(\Pi,\mathbf{b},q)\text{-}\mathcal{N}'_{\alpha,T}(n)}[\mathit{ordval}_{\Psi^\uparrow} \geq \mathit{val}_\Psi + \epsilon] \leq \exp(-n).$$

除去 引理 6.7的证明外，我们现在可以证明 定理 6.1：

定理 6.1 的证明。设 $\epsilon' = \epsilon/4$。选取 $q_0 \in \mathbb{N}$，使得引理 6.7 以 ϵ' 的错误概率成立，并令 $q = \max\{q_0,(k-1)/\epsilon'\}$。现在令 α 为推论 5.14 和引理 6.7 中较小的 α_0，并令 T 为引理 6.7 和 5.13 在错误概率为 ϵ' 时所得的 T_0 中较大的一个。令 $n_0 \in \mathbb{N}$ 为推论 5.14 和引理 5.13 中较大的 n_0。

现在固定 $\mathbf{b} \in \mathrm{supp}(\Pi)$。对于 $n \geq n_0 \in \mathbb{N}$，令 $\mathcal{Y}^\uparrow$ 和 $\mathcal{N}^\uparrow$ 分别表示 Max-OCSP(Π) 实例 $\Psi^\uparrow$的分布，其中 $\Psi \sim (\Pi,\mathbf{b},q)\text{-}\mathcal{Y}'_{\alpha,T}(n)$ 和 $(\Pi,\mathbf{b},q)\text{-}\mathcal{N}'_{\alpha,T}(n)$。根据推论 5.14，区分 $\mathcal{Y}^\uparrow$和 $\mathcal{N}^\uparrow$需要空间 τn，其中某个 $\tau > 0$。另一方面，根据引理 6.4 和 5.13 以及方程（6.5），

$$\Pr_{\Phi\sim\mathcal{Y}^\uparrow}[\mathrm{ordval}_\Phi \leq 1-\epsilon/2] \leq \exp(-n),$$

而根据引理 6.7和5.13 以及公式（6.6），

$$\Pr_{\Phi\sim\mathcal{N}^{\uparrow}}[\mathsf{ordval}_{\Phi} \geq \rho(\Pi) + \epsilon/2] \leq \exp(-n).$$

因此，($\rho(\Pi) + \epsilon$近似 最大排序约束满足问题(Π) 至少需要 τn 空间，符合预期（见命题 2.8）。 □

还需证明引理 6.7；我们将在最后一节中完成证明。

6.4 The coarsening analysis: Proving Lemma 6.7

本节的目标是证明 引理 6.7。我们通过实施基于“平衡划分扩展器”的方案来完成这一目标，正如 命题 6.3 的证明概要中所述。

给定一个包含 n 个变量的 Max-CSP($\Pi^{\downarrow q}$) 实例 Ψ 以及一个子集 $S \subseteq [n]$，我们用 $N(\Psi, S)$ 表示在 Ψ 中“接触 S 两次”的约束 $\mathbf{j} = (j_1, \ldots, j_k)$ 的数量，即对于某个 $i \neq i'$，满足 $j_i, j_{i'} \in S$ 的约束。

定义 6.8 （小集合扩展（SSE））。 设 Ψ 是一个具有 n 个变量和 m 个约束的 *Max-CSP*($\Pi^{\downarrow q}$) 实例。对于 $\gamma, \epsilon \in (0,1)$，若对每个大小至多为 γn 的子集 $S \subseteq [n]$，都有 $N(\Psi, S) \leq \epsilon m$，则称 Ψ 是一个(γ, ϵ)-小集合扩展器（SSE）。

定义 6.9 （平衡划分扩展（BPE））。 设 Ψ 是一个具有 n 个变量和 m 个约束的最大约束满足问题（$\Pi^{\downarrow q}$）实例。对于 $\gamma, \epsilon \in (0,1)$，若对每个 $\mathbf{b} \in \mathbb{Z}_q^n$，其中每个块 $\mathbf{b}^{-1}(a)$ 的大小至多为 γn，则 Ψ 是一个（γ, ϵ）平衡划分扩展（BPE），

$$\sum_{a\in\mathbb{Z}_q} N(\Psi, \mathbf{b}^{-1}(a)) \leq \epsilon m.$$

现在我们给出几个引理，将这些概念与上一小节中的否分布 $\mathcal{N}'$ 联系起来：

引理 6.10。 设 $\Pi : \mathfrak{S}_k \to \{0,1\}$, $\mathbf{b} \in \mathit{supp}(\Pi)$, $q \in \mathbb{N}$ 和 $\gamma > 0$。存在 $\alpha_0 \in \mathbb{N}$，使得对每个 $\alpha \in (0, \alpha_0)$，都存在 $T_0 \in \mathbb{N}$，使得对于 $T \geq T_0 \in \mathbb{N}$ 以及每个 $n \in \mathbb{N}$,

$$\Pr_{\Psi\sim(\Pi,\mathbf{b},q)\text{-}\mathcal{N}'_{\alpha,T}(n)} \left[\Psi \textit{ is not a } (\gamma, 8k^2\gamma^2)\textit{-SSE}\right] \leq \exp(-n).$$

我们将引理 6.10 的证明推迟到本小节末尾，因为其中涉及一些相当繁杂的集中界。

引理 6.11（好的 SSE 是好的 BPE）。对于任意 $\gamma, \epsilon \in (0,1)$，如果 Ψ 是一个 (γ, ϵ)-*SSE*，那么它就是一个 $(\gamma, 3\gamma/\epsilon)$-*BPE*。

证明。考虑任意一个 $\in \mathbb{Z}_q^n$，其中每个块 $\mathbf{b}^{-1}(a)$ 的大小至多为 γn。首先注意，如果两个块的大小 $|\mathbf{b}^{-1}(a)|$、$|\mathbf{b}^{-1}(a')|$ 都小于 $\frac{\gamma n}{2}$，我们可以将 $\mathbf{b}^{-1}(a')$ 重新分配给 a，因为这只会增加总和 $\sum_{a\in\mathbb{Z}_q} N(\Psi, \mathbf{b}^{-1}(a))$，且每个块的大小仍至多为 γn。因此，不失一般性，我们可以假设 $\mathbf{b}$ 由空块、一个大小至多为 $\frac{\gamma n}{2}$ 的块，以及大小介于 $\frac{\gamma n}{2}$ 和 γn 之间的块组成。非空块的数量至多为 $\frac{n}{\lfloor \gamma n/2 \rfloor} + 1 \le 3\gamma$，并且根据 SSE 假设，每个这样的块都满足 $N(\Psi, \mathbf{b}^{-1}(a)) \le \epsilon m$。

□

引理 6.12（在 BPE 中，粗略细化基本保留值）。设 $\Pi : \mathfrak{S}_k \to \{0,1\}$，$q \in \mathbb{N}$ 且 $\epsilon > 0$。若 Ψ 是一个最大约束满足问题 $(\Pi^{\downarrow q})$ 实例，且它是一个 $(1/q, \epsilon)$-*BPE*，那么

$$\mathit{ordval}_{\Psi^\uparrow} \le \mathit{val}_\Psi + \epsilon.$$

证明。设 n 和 m 分别表示 Ψ 中的变量数和约束数。考虑任意一种排序 $\boldsymbol{\sigma} \in \mathfrak{S}_n$，并像命题 6.3 的证明概要中那样，令 $\boldsymbol{\sigma}^{\downarrow q} \in \mathbb{Z}_q^n$ 由 $\sigma_i^{\downarrow q} = \lceil q\sigma_i/n \rceil$ 定义。只需证明 $\mathrm{ordval}_{\Psi^\uparrow}(\boldsymbol{\sigma}) \le \mathrm{val}_\Psi(\boldsymbol{\sigma}^{\downarrow q}) + \epsilon$。$\boldsymbol{\sigma}^{\downarrow q}$ 具有“单调性”性质：对于任意 u、$v \in [n]$，若 $\sigma_u < \sigma_v$，则 $\sigma_u^{\downarrow q} \le \sigma_v^{\downarrow q}$；并且每个块 $(\boldsymbol{\sigma}^{\downarrow q})^{-1}(a)$ 的大小至多为 $\frac{n}{q}$。

假设约束 $\mathbf{j} = (j_1, \ldots, j_k)$ 在 $\boldsymbol{\sigma}$（在 $\Psi^\uparrow$ 中）得到满足。若 $\sigma_{j_1}^{\downarrow q}, \ldots, \sigma_{j_k}^{\downarrow q}$ 互不相同，则根据单调性，$\mathbf{ord}(\boldsymbol{\sigma}^{\downarrow q}|_{\mathbf{j}}) = \boldsymbol{\sigma}|_{\mathbf{j}}$，因此 $\mathbf{j}$ 在 $\boldsymbol{\sigma}^{\downarrow q}$（在 Ψ 中）得到满足。因此，只需证明至多有 ϵm 个约束 $\mathbf{j}$ 满足 $\sigma_{j_1}^{\downarrow q}, \ldots, \sigma_{j_k}^{\downarrow q}$ 不全相同；这正是 Ψ 的 BPE 性质。

□

在证明引理 6.10 的基础上，我们现在可以证明引理 6.7：

引理 *引理 6.7*的证明。设 $q_0 = \lceil 24k^2/\epsilon \rceil$；考虑 $q \ge q_0 \in \mathbb{N}$ 并设 $\gamma = 1/q$；令 α_0 如引理 6.10所述；对于任意 $\alpha \in (0, \alpha_0)$，令 T_0 如引理 6.10所述；并考虑任意 $T \ge T_0 \in \mathbb{N}$。

如果 Ψ 是一个 $(\gamma, 8k^2\gamma^2)$-SSE，那么根据 引理 6.11 它是一个 $(\gamma, 24k^2\gamma)$-BPE，此时根据 引理 6.12 有 $\mathrm{ordval}_{\Psi^\uparrow} \leq \mathrm{val}_\Psi + 24k^2\gamma$，并且根据假设有 $24k^2\gamma \leq \epsilon$。但是根据引理 6.10，$\Psi \sim (\Pi, \mathbf{b}\ q)$-$\mathcal{N}'_{\alpha,T}(n)$ 是一个 $(\gamma, 8k^2\gamma^2)$-SSE，除非发生概率为 $\exp(-n)$ 的例外。

□

最后，我们证明引理 6.7。

引理 6.7 的证明。回想一下，我们首先从 (k,q)-$\mathcal{N}_{\alpha,T}(n)$ 的 (k,q)-$\mathrm{siRSD}_{\alpha,T}(n)$ 否分布中抽样（见定义 5.10），然后应用构造 5.12 中的归约函数 $\mathrm{R}1, \ldots, \mathrm{R}_T$，并选取某个固定的基向量 $\mathbf{b} \in \mathrm{supp}(\Pi)$，从而抽取实例 $\Psi \sim (\Pi, \mathbf{b}\ q)$-$\mathcal{N}'_{\alpha,T}(n)$。

为具体起见，我们在此重述这一情形下的定义。对于每个 $t \in [T]$，我们得到一个实例 Ψ_t（由 Bob_t 生成）：

1. 抽取一个匹配 $M_t \sim \mathcal{M}_{k,\ \alpha}(n)$ 和一个向量 $\mathbf{z}(t) \sim (\mathcal{U}^k_{\mathbb{Z}_q})^{\alpha n}$，我们将其视为由 αn 个独立抽取的块 $\mathbf{z}(t,\ \ell) \sim \mathcal{U}^k_{\mathbb{Z}_q}$ 组成。

2. 当且仅当$\mathbf{z}(t,\ell) - \mathbf{b} \in \mathcal{C}$时，将 M_t 中的第 ℓ条超边$\mathbf{e}(t,\ell) = (e(t,\ell)_1, \ldots, e(t,\ell)_k)$作为 Ψ_t 中的一个约束，其中 $\mathcal{C} = \{(c, \ldots, c) :\ c \in \mathbb{Z}_q\}$。

然后 $\Psi = \Psi_1 \cup \cdots \cup \Psi_T$。由于$\mathbf{z}(t,\ell)$是 $\mathbb{Z}_q^k$中的均匀分布向量，且 $\mathcal{C}$ 是 $\mathbb{Z}_q^k$的一个一维子空间，因此 M_t 中的每条超边都以概率$q^{-(k-1)}$独立地被包含在 Ψ_t 中。

令 m_t 表示对于每个 t，Ψ_t 中的约束数量，并令 $m = \sum_{t=1}^T m_t$ 表示 Π中的约束数量。因此，每个 m_t 都服从 αn 个相互独立的$\mathcal{B}(q^{-(k-1)})$随机变量之和的分布。现在考虑事件 $m \geq \alpha T n/(2q^{k-1})$。由于 m服从 $\alpha T n$ 个相互独立的 $\mathcal{B}(q^{-(k-1)})$之和的分布，根据切尔诺夫界，该事件不发生的概率至多为 $\exp(-\alpha T n/(8q^{k-1}))$；当 T_0充分大时，这等于 $\exp(-n)$。因此，只需在固定的 $m_1, \ldots, m_T$满足 $m \geq \alpha T n/(2q^{k-1})$的条件下证明该引理。在此条件下，每个子实例 Ψ_t 都是通过一个更简单的抽样过程得到的：其约束是从$\mathcal{M}_{k,m/n}(n)$中抽取的一个超匹配中的超边。

现在固定任意一个大小至多为 γn 的 $S \subseteq [n]$ 集合。（稍后我们将对所有S应用并集界。）将每个 M_t 的超边标记为 $\mathbf{e}(t,\ 1)\ldots\ldots,\ \mathbf{e}(t,\ m_t)$。考虑由 m 构成的集合

随机变量 $\{X_{t,\ell}\}_{t\in[T],\ \ell\in[m_t]}$，其中每个变量都是如下事件的指示变量：$\mathsf{e}(t,\ \ell)$ 中的两个不同顶点属于 S。根据定义，$N(\Psi,\ S)=\sum_{t=1}^{T}\sum_{\ell=1}^{m_t}X_{t,\ \ell}$。

对于固定的 $t\in[T]$，我们首先对每个 $\ell\in[m_t]$ 给出 $\mathbb{E}[X_{t,\ell}\mid X_{t,1},\ldots,X_{t,\ell-1}]$ 的上界。在条件 t、1）.....、t、$\ell-1$）与 k（$\ell-1$）个顶点的某个子集 $V_{t,\ \ell}\subseteq[n]$）相 incident 的超边 $\mathsf{e}(t,\ell)$ 均匀分布于 $[n]\setminus V_{t,\ \ell}$ 的条件下，只需对不同的顶点对 $\{j_1,j_2\}\in\binom{[k]}{2}$ 作并合界，估计超边 $\mathsf{e}(t,\ell)$ 的第 j_1 个和第 j_2 个顶点位于 S 中的概率（给定 $X_{t,\ }$0、.....、$X_{t,\ \ell-1}$）。我们可以先抽取超边 $\mathsf{e}(t,\ell)$ 的第 j_1 个和第 j_2 个顶点，然后忽略其余顶点。令 $\alpha_0=1/$（$2k$），便得到上界

$$\begin{aligned}\mathbb{E}[X_{t,\ell}\mid X_{t,1},\ldots,X_{t,\ell-1}]&\le\binom{k}{2}\cdot\frac{|S|(|S|-1)}{(n-k(\ell-1))(n-k(\ell-1)-1)}\\&\le\binom{k}{2}\cdot\left(\frac{|S|}{n-k(\ell-1)}\right)^2\\&\le\binom{k}{2}\cdot\left(\frac{|S|}{n-km_t}\right)^2\\&\le 4k^2\gamma^2,\end{aligned}$$

因为 $m_t\le\alpha n\le n/(2k)$。

现在 $X_{t,\ \ell}$ 与$X_{t',\ \ell'}$ 独立，如果 $t\ne t'$ 因为 M_t 且 $M_{t'}$ 相互独立。因此，引理 2.5 意味着

$$\Pr_{\Psi\sim(\Pi,\mathbf{b},q)\text{-}\mathcal{N}'_{\alpha,T}(n)}\left[N(\Psi,S)\ge 8k^2\gamma^2m\mid m_1,\ldots,m_T\right]\le\exp\left(-2k^2\gamma^2m\right).$$

最后，我们使用不等式 $m\ge\alpha Tn/(2k^2)$，对 $S\subseteq[n]$ 应用并集界，并将 setT_0 设得足够大，以确保 $2^n\exp(-\gamma^2\alpha Tn)\le\exp(-n)$。 □

7

对称布尔谓词

> 在我们的算法中 [针对Max-kAND]„ 我们采用 Hast [Has05]的方法：首先求得一个“初步”解 $z_1, \ldots, z_n \in \{-1, 1\}^n$，然后独立地翻转 z_i 的值，使用一个略有偏差的分布（即，以略高于 z_i 的概率保留 $1/2$的旧值）。
>
> ——Charikar、Makarychev 和 Makarychev [CMM09]

Max-kAND is the simplest k-ary Boolean CSP 它不仅非平凡可近似，而且在某种意义上也是最容易近似的（参见下文的备注 7.9 ）。本章将介绍我们与 Boyland、Hwang、Prasad 和 Velusamy 的合作成果 [BHP+22]，该成果研究了关于 [CGSV21a; CGS+22] （上文第 5 章）中关于 最大k与以及其他最大布尔约束满足问题（f）问题的若干结果：

1. [CGSV21a] 中的二分定理（即定理 5.2）能否用于求出非平凡可近似问题 α（f）的闭式草图可近似比最大布尔约束满足问题（f），而不局限于Max-2AND （例 5.5）？据我们所知，在经典情形下，Raghavendra 的 UG 二分定理 [Rag08]

从未被用于此目的，不过我们或许对利用 [CGSV21a]的二分定理更有“希望”，因为它至少是可判定的（见上文§5.1.2开头）。

2. [CGS+22] 证明，对于任意谓词 $f\colon \mathbb{Z}_2^k \to \{0,1\}$ 和 $\epsilon > 0$，$(2\rho(f) + \epsilon)$- 近似 最大布尔约束满足问题$(\overline{f})$所需的流式算法空间为 $\Omega(n)$（推论 5.15）。这个近似比上界有多紧?

3. [CGSV21a]基于填充单向配对的流式下界（定理 5.4）是否足以确定对每个谓词 最大布尔约束满足问题$(\overline{f})$ 的流式近似性? $f\colon \mathbb{Z}_2^k \to \{0,1\}$?

4. 对于任意谓词 $f\colon \mathbb{Z}_2^k \to \{0,1\}$，CGSV21a] 在 $\alpha(f) - \epsilon$)- 近似比下，为 最大布尔约束满足问题$(\overline{f})$ 给出了最优的草图化（[CGSV21a], ），但该算法会并行运行一个由 $O(1/\epsilon^2)$ 个区分器组成的“网格”，用于处理 (β, γ)-最大布尔约束满足问题$(\overline{f})$ 区分问题（参见 推论 5.3 及其证明概要）。对于有趣的谓词，我们能否得到更简单的最优草图近似算法?

具体而言，我们研究了当 $f\colon \mathbb{Z}_2^k \to \{0,1\}$ 是一个对称谓词时，Max-BCSP$(\overline{f})$ 的草图化（以及流式计算）可近似性；也就是说，f 仅取决于其输入 $\mathbf{b}$ $\|\mathbf{b}\|_0$ 的汉明重量（即 1 的数量） $\in \mathbb{Z}_2^k$。对于一个集合 $S \subseteq [k]$，令 $f_{S,k}\colon \mathbb{Z}_2^k \to \{0,1\}$ 表示由 $f_{S,k}(\mathbf{b}) = \mathbb{1}_{\|\mathbf{b}\|_0 \in S}$ 定义的对称谓词。该类中经过深入研究的一些谓词示例包括 kAND $= f_{\{k\},k}$、 以及阈值函数 $\mathrm{Th}_k^t = f_{\{t,t+1,\ldots,k\},k}$。正如我们将在下文第 7.2 节看到的，我们考虑对称谓词，是因为对于这类谓词， [CGSV21a] 结果（具体来说是推论 5.3 和定理 5.4）具有明显更简单的形式。

本章中的若干证明涉及代数运算，我们借助计算机辅助完成；相关代码可在 Mathematica Notebook Archive 上获取，网址为 https://notebookarchive.org/2022-03-a5vpzhg。

7.1 Results

我们首先介绍本工作的主要结果 [BHP+22]。

7.1.1 The sketching approximability of Max-kAND

回顾例 5.5，$\sqrt{n}$空间下Max-2AND 的草图近似性为$\alpha(\text{2AND}) = \frac{4}{9}$，并且即使对于使用填充单变量对判据的$\frac{4}{9}+\epsilon$近似，也可以排除 $\sqrt{n}$空间流式计算算法（定理 5.4）。在此结果的基础上，我们为每个 $\sqrt{n}$空间下$\alpha(k\text{AND})$ 的草图近似比推导出闭式表达式。对于奇数 k，定义常数 $k \geq 3$

$$\alpha'_k \stackrel{\text{def}}{=} \left(\frac{(k-1)(k+1)}{4k^2}\right)^{(k-1)/2} = 2^{-(k-1)} \cdot \left(1-\frac{1}{k^2}\right)^{(k-1)/2}. \tag{7.1}$$

接下来，在§7.5.1中，我们证明如下结论：

定理 7.2。 对于奇数 $k \geq 3$, $\alpha(k\mathit{AND}) = \alpha'_k$，以及偶数 $k \geq 2$, $\alpha(k\mathit{AND}) = 2\alpha'_{k+1}$。

例如，$\alpha(\text{3AND}) = \alpha'_3 = \frac{2}{9}$。由于 $\rho(k\text{AND}) = 2^{-k}$，定理 7.2 还有以下重要推论：

推论 7.3。 $\lim_{k\to\infty} \frac{\alpha(k\mathit{AND})}{2\rho(k\mathit{AND})} = 1$。

回顾 Chou、Golovnev、Sudan、Velusamy 和 Velingker [CGS+22] 证明了，任何谓词 f 即使使用线性空间流式算法，也无法达到（$2\rho(f)+\epsilon$）近似（参见推论 5.15）。另一方面，在下文的§7.1.3 中，我们介绍简单的 $O(\log n)$空间草图算法，用于Max-kAND，其近似比达到 [CGSV21a]中的最优值。因此，正如 $k \to \infty$所示，这些算法即使与线性空间流式算法相比，也能达到渐近最优的近似比！

7.1.2 The sketching approximability of other symmetric predicates

我们还分析了其他一些对称布尔谓词的草图近似性。例如，我们证明：

定理 7.4. 对于偶数 $k \geq 2$，$\alpha(\mathit{Th}_k^{k-1}) = \frac{k}{2}\alpha'_{k-1}$.

我们在 定理 7.4 中§7.5.2 证明该定理，所用技术与我们证明定理 7.2时类似。我们还给出关于$f_{\{(k+1)/2\},\ k}$的部分结果，包括较小 k 时的闭式，以及对 $\alpha(f_{\{(k+1)/2\},\ k})$的渐近分析：

定理 7.5 （定理 7.38的非正式表述）。对于奇数 $k \in \{3, \ldots, 51\}$，可以将 α（$f_{\{(k+1)/2\},k}$）显式表示为 k的函数。

定理 7.6。$\lim_{odd\ k\to\infty} \alpha\left(f_{\{(k+1)/2\},k}\right)\rho\left(f_{\{(k+1)/2\},k}\right) = 1$。

我们在 §7.5.3 中证明定理 7.5 和 7.6。最后，在 §7.5.4 中，我们明确解决了另外十五种情形（例如$f_{\{2,3\},3}$ 和 $f_{\{4\},5}$），这些情形未涵盖在定理 7.2、7.4 和 7.5中。

7.1.3 Simple approximation algorithms for threshold functions

回顾 §4.1 中的结论： [CGV20] 给出了针对 $\frac{4}{9} - \epsilon$ 的最优 (Max-2AND 近似草图算法，其依据是测量输入实例 的偏差$_\Psi \in [0,1]$ Ψ （参见方程 (4.3)），使用 1-范数草图算法 [Ind06; KNW10]。在 §7.6 中，我们将偏差的定义推广到任意约束满足问题，并为阈值谓词给出简单且最优的、基于偏差的近似算法：

定理 7.7. 设 $k \in \mathbb{N}, i \leq k$。那么，对于每个 $\epsilon > 0$，都存在一个分段线性函数 γ：$[-1,1] \to [0,1]$ 以及一个常数 $\epsilon' > 0$，使得以下算法是针对最大布尔约束满足问题(Th_k^t)的草图化($\alpha(Th_k^t) - \epsilon$)-近似算法：输入 Ψ 时，计算 $\widehat{\text{偏差}}_\Psi$ 的一个估计值 $\widehat{b}$，误差至多为乘法$(1 \pm \epsilon')$，并输出 $\gamma(b)$。

我们的构造将 [CGV20] 中针对2AND 的算法推广到了所有阈值谓词，而且也进行了简化，因为 [CGV20] 算法计算的是一个更复杂的函数$\widehat{\ b}$；参见 备注 4.13。

对于本章中我们确定了可近似性的所有约束满足问题，我们都采用一种称为“极大极小方法”的分析技术；详见§7.3.2 下文。对于这类约束满足问题，我们的算法可以扩展为求解输出近似最优赋值的问题，而不只是估计值，这与我们在Max-2AND 一例中所讨论的方法一致，详见§4.1.2节。实际上，对于这个问题，我们给出了一种简单的随机化流式算法，其空间和运行时间均为 $O(n)$：

定理 *7.8*（定理 *7.43* 的非正式版本）。设 Th_k^t 是一个适用极大极小方法的阈值谓词，例如 k*AND*，或 Th_k^{k-1} （对于偶数 k）。那么存在一个常数 $p^* \in [0,1]$，使得以下算法在输入 Ψ时，输出的赋值的期望值至少为 $\alpha(Th_k^t)val_\Psi$：若 $bias_\Psi(i) \geq 0$，则将变量 i 赋值为 *1*，否则赋值为 *0*；然后以概率 p^*独立地翻转每个变量的赋值。

特别是，这并非先验地由 [CGSV21a；CGSV21b] 所蕴含的 p^* 将其设为固定常数就足够了（而 [CGV20] 在2AND情形中并未注意到这一点）；我们认为这是增进对约束满足问题草图化可近似性一般理解的一项重要贡献。此外，我们的算法有望借助通用哈希族实现去随机化，正如 Biswas 和 Raman 最近对 [BR21]中Max-2AND算法所做的那样，见 [CGV20]。

7.1.4 Sketching vs. streaming approximability

定理 7.2 意味着 α(3AND) $= \frac{2}{9}$，因此对于每个 $\epsilon > 0$，Max-3AND 都可以由 $O(\log n)$-空间线性草图算法进行 $(\frac{2}{9} - \epsilon)$-近似，但无法由 $\sqrt{n}$-空间草图算法进行 $(\frac{2}{9}+\epsilon)$-近似。我们证明，Chou、Golovnev、Sudan 和 Velusamy [CGSV21a] 的填充单变量对判据（定理 5.4）不足以完全解决 Max-3AND 的流式近似性问题，即无法证明对于每个 $\epsilon > 0$，$\sqrt{n}$-空间流式算法都不能对 Max-3AND 进行 $(\frac{2}{9} + \epsilon)$-近似；然而，该判据确实表明，$\sqrt{n}$-空间流式算法无法对 Max-3AND 进行 0.2362-近似。我们将在下文 §7.3.3 中正式陈述这些结果。另一方面，定理 7.4 意味着 $\alpha(\mathrm{Th}_4^3) = \frac{4}{9}$，并且可以利用填充单变量对判据证明，在流式设置下，对 Max-BCSP(Th_4^3) 进行 $(\frac{4}{9} + \epsilon)$-近似需要 $\Omega(\sqrt{n})$ 空间（参见下文观察 7.34）。

Related work

Max-kAND 的经典可近似性一直备受深入研究，研究内容既包括算法 [GW95; FG95; Zwi98; Tre98a; TSSW00; Has04; Has05; CMM09]，也包括近似困难性 [H˚as01; Tre98b; ST98; ST00; EH08; ST09]，，因为它与 k-位概率可检验证明有着密切联系。Charikar、Makarychev 和 Makarychev [CMM09]构造了一个对 Max-kAND 的 $\Omega(k2^{-k})$-近似，而 Samorodnitsky 和 Tre- visan [ST09] 证明，$k2^{-(k-1)}$-近似和 $(k+1)2^{-k}$-近似分别是 NP 困难和 UG 困难。

有趣的是，回想一下 $\alpha(k$与$) \to 2\rho(k$与$) = 2^{-(k-1)}$ 当 $k \to \infty$，在大k规模极限下，我们简单的随机化算法（见定理 7.8）与 Trevisan 的 [Tre98a] 基于线性规划、可并行化的算法在 k与上的表现相匹配，而（据我们所知，

这是首个研究一般 k与问题的工作！后续工作[Has04；Has05；CMM09]取代了 [Tre98a]，采用了涉及半定规划的更复杂技术，但在结构上与我们定理7.8中的算法相似：它们都包含“猜测”一个赋值$\mathbf{x} \in \mathbb{Z}_2^n$，然后以常数概率扰动每一位。

注 *7.9*。*Trevisan [Tre98a*，定理 *18]* 指出，对于每个谓词 $f : \mathbb{Z}_2^k \to \{0,1\}$, $\alpha(f)/\rho(f) \leq \alpha(k\mathrm{AND})/\rho(k\mathrm{AND})$（在经典情形下成立，但证明很容易推广到草图化情形）。因此，相对于非平凡可近似性的阈值，$\alpha(f)$ 是所有布尔函数中“最容易近似的”。直观地说，这是因为 kAND 是最“有信息量”的谓词：它精确规定了变量应被赋予哪些值。更准确地说，给定任意谓词 $f : \mathbb{Z}_2^k \to \{0,1\}$，令 $t = |\mathrm{supp}(f)|$。给定 *Max-BCSP(f)* 的任意实例 Ψ，我们可以通过将 Ψ 中的每个约束 C 替换为与 C 的满足赋值对应的 Ψ' 个约束，构造 *Max-BCSP(*k*AND)* 的一个实例 Ψ'；也就是说，$C = (b, j\ w)$ 变为 $C_1 = (b + a(1) + 1, j\ w) \ldots, C_t = (b + a(t) + 1, j\ w)$，其中 $\mathrm{supp}(f) = \{a(1) \ldots, a(t)\}$。每个赋值 $x \in \mathbb{Z}_2^n$ 要么满足约束 $\{C_1, \ldots, C_t\}$ 中的一个，要么一个也不满足，这分别对应于它满足或不满足 C。因此，对于每个 $x \in \mathbb{Z}_2^n$，$val_\Psi(x) = tval_{\Psi'}(x)$。该不等式由 $\rho(f)/\rho(k\mathrm{AND}) = t$ 这一事实推出。

文献[CHIS12；ABM12；GL17]研究了多种对称谓词类别的经典可近似性。

7.2 Setup for the symmetric case

我们首先说明，当谓词是对称谓词时，如何更简单地实例化 [CGSV21a] 的结果（具体而言，即推论 5.3 和定理 5.4）（正如 [CGSV21a] 在 2AND 情形中所观察到的）。对于对称谓词f_S，k（见方程 (5.1)），令 $\lambda_S(\mathcal{D}, p)$ $\gamma_S(\mathcal{D}_Y)$ $\beta_S(\mathcal{D}_N)$分别表示 [CGSV21a], 中的 λ、γ、β函数。我们将在下文 §7.4 中证明，一般而言，$\lambda_S(\mathcal{D}, p)$ 是关于 p 和$\mathcal{D}\langle 0\rangle$，……，$\mathcal{D}\langle k\rangle$的多变量多项式，其次数为$k$，且关于 $\mathcal{D}\langle t\rangle$是线性的。

若汉明重量相同的字符串等概率出现，则分布 $\mathcal{D} \in \Delta(\mathbb{Z}_2^k)$ 是对称的，即 $\|\mathbf{a}\|_0 = \|\mathbf{a}'\|_0 \implies \mathcal{D}(\mathbf{a}) = \mathcal{D}(\mathbf{a}')$。令 $\Delta_k \subseteq \Delta(\mathbb{Z}_2^k)$ 表示……的空间

……上的对称分布。对于分布 $\mathcal{D} \in \Delta(\mathbb{Z}_2^k)$ 和 $i \in [k] \cup \{0\}$，令$\mathcal{D}\langle i\rangle \stackrel{\text{def}}{=} \sum_{\|\mathbf{a}\|_0=i} \mathcal{D}(i)$ 表示汉明重量为 i 的字符串上的总概率质量。我们可以将对称分布 $\mathcal{D} \in \Delta_k$ 视为……上的分布，其取值为 i 的概率为 $\mathcal{D}\langle i\rangle$。此外，通过对称化操作，还可以自然地将 $\Delta(\mathbb{Z}_2^k)$ 投影到 Δ_k 上：对于分布 $\mathcal{D} \in \Delta(\mathbb{Z}_2^k)$，令 $\mathrm{Sym}(\mathcal{D}) \in \Delta_k$ 表示唯一的对称分布，使得对所有 $i \in [k] \cup \{0\}$ 都有 $\mathrm{Sym}(\mathcal{D})\langle i\rangle = \mathcal{D}\langle i\rangle$。（换言之，对称化会将 $\mathcal{D}$ 中的概率重新分配到所有汉明重量相同的字符串上。）最后，若 $\mathcal{D} \in \Delta_k$ 对称，则定义 $\mu(\mathcal{D}) = \mathbb{E}_{\mathbf{a}\sim\mathcal{D}}[(-1)^{a_1+1}]$；此时，$\boldsymbol{\mu}(\mathcal{D})$ 是常数向量 $(\mu(\mathcal{D}) \ldots, \mu(\mathcal{D}))$。

以下命题指出，要使用 [CGSV21a]（即定理 5.2 和5.4 以及推论 5.3）中的工具处理对称谓词 $f\colon \mathbb{Z}_2^k \to \{0,1\}$，只需考察对称分布：

命题 7.10。 *i.* 对于每个对称谓词 $f_{S,\,k}\colon \mathbb{Z}_2^k \to \{0,1\}$, $\mathcal{D} \in \Delta(\mathbb{Z}_2^k)$，以及 $p \in [0,1]$, $\lambda_S(\mathcal{D}, p) = \lambda_S(\mathit{Sym}(\mathcal{D})\ p)$。

ii. 对所有边缘分布匹配的 $\mathcal{D}_N, \mathcal{D}_Y \in \Delta(\mathbb{Z}_2^k)$（即 $\boldsymbol{\mu}(\mathcal{D}_N) = \boldsymbol{\mu}(\mathcal{D}_Y)$），$\mu(\mathit{Sym}(\mathcal{D}_N)) = \mu(\mathit{Sym}(\mathcal{D}_Y))$。

iii. 对所有填充单边对 $\mathcal{D}_N, \mathcal{D}_Y \in \Delta(\mathbb{Z}_2^k)$，$\mathit{Sym}(\mathcal{D}_N)$ 和 $\mathit{Sym}(\mathcal{D}_Y)$ 也构成一个填充单边对。

证明。 省略（由定义和期望的线性性立即可得）。 □

特别地，结合推论 5.3 可得：

推论 7.11。 对于每个对称谓词 $f\colon \mathbb{Z}_2^k \to \{0,1\}$,

$$\alpha(f) = \inf_{\mathcal{D}_N, \mathcal{D}_Y \in \Delta_k:\ \mu(\mathcal{D}_N)=\mu(\mathcal{D}_Y)} \left(\frac{\beta_f(\mathcal{D}_N)}{\gamma_f(\mathcal{D}_Y)}\right).$$

于是：

i. 对于每个 $\epsilon > 0$，存在 $\tau > 0$ 和一个 $\tau \log n$-空间线性草图算法，它以$(\alpha(f) - \epsilon)$近似最大布尔约束满足问题(f)。

ii. 对于每个 $\epsilon > 0$，存在 $\tau > 0$，使得任何以$(\alpha(f) + \epsilon)$近似最大布尔约束满足问题(f)的草图算法至少需要 $\tau\sqrt{n}$空间（当 n 足够大时）。

我们关注对称谓词，f 是因为与推论 7.11相比，推论 5.3 对于一般谓词的形式更简单。由于在下确界中我们只需考虑对称分布，$\mathcal{D}_Y$ 和 $\mathcal{D}_N$ 各自只由 $k+1$个变量参数化（而不是 2^k 个变量），且只有一个线性等式约束（而不是 k 个约束）。

接下来，我们给出对称分布 $\mathcal{D} \in \Delta_k$下 $\mu(\mathcal{D})$ 的显式公式。对于$i \in [k]$，令 $\epsilon_{i,k}$ 定义为 $= -1 + \frac{2i}{k}$。

引理 7.12。对于任意 $\mathcal{D} \in \Delta_k$，

$$\mu(\mathcal{D}) = \sum_{i=0}^{k} \epsilon_{i,k}\, \mathcal{D}\langle i\rangle.$$

证明。回忆一下，我们定义了 $\epsilon_{i,k} = -1 + \frac{2i}{k}$。根据定义，$\mu(\mathcal{D}) = \mathbb{E}_{\mathbf{b}\sim\mathcal{D}}[b_1]$。利用期望的线性性，权重为 i 的向量对 $\mu(\mathcal{D})$ 的贡献为 $\mathcal{D}\langle i\rangle \cdot \frac{1}{k}(i \cdot 1 + (k-i)\cdot(-1)) = \epsilon_{i,k}\,\mathcal{D}\langle i\rangle$。

□

例 *7.13*。在例 *5.6* 中，我们证明了：如果谓词 $f : \mathbb{Z}_2^k \to \{0,1\}$ 支撑单变量独立性，也就是说，存在支撑于 $\mathrm{supp}(f)$ 上的 $\mathcal{D}_Y \in \Delta(\mathbb{Z}_2^k)$，使得 $\mu(\mathcal{D}_Y) = \mathbf{0}$，那么对于 $\sqrt{n}$ 空间的流式算法，*Max-BCSP(f)* 具有近似抗性。*[CGSV21a*，引理 *2.14]*表明，如果 $f = f_{S,k}$ 是对称的，那么对于 $\sqrt{n}$ 空间的流式近似抗性，这一条件也是必要的。根据命题 *7.10*，这一条件等价于存在一个支撑于S 上的对称分布 $\mathcal{D}_Y \in \Delta_k$（也就是说，对于所有 $s \notin S$，$\mathcal{D}_Y\langle s\rangle = 0$），使得 $\mu(\mathcal{D}_Y) = 0$。

现在，如果 k 是偶数且 $k/2 \in S$，那么分布 $\mathcal{D}_Y \in \Delta_k$（其中 $\mathcal{D}_Y\langle k/2\rangle = 1$）满足 $\mu(\mathcal{D}_Y) = 0$（根据引理 *7.12*），且其支撑集为 S；因此，*Max-BCSP*$(f_{S,k})$ 具有流式近似抗性。此外，如果 S 包含元素 $s \le k/2$ 和 $t \ge k/2$，我们可以令 $\delta = \frac{\epsilon_t}{\epsilon_t - \epsilon_s}$（注意 $\epsilon_{t,k} > 0$ 且 $\epsilon_{s,k} < 0$），并令 $\mathcal{D}_Y \in \Delta_k$ 由 $\mathcal{D}_Y\langle s\rangle = \delta$ 和 $\mathcal{D}_Y\langle t\rangle = 1-\delta$ 定义。于是同样有 $\mu(\mathcal{D}_Y) = 0$，且 $\mathcal{D}_Y$ 的支撑集为 S，因此 *Max-BCSP*$(f_{S,k})$ 具有流式近似抗性。

给定 例 7.13，本章余下部分将重点讨论 S 的所有元素都大于或小于 $k/2$ 的情形。另请注意，如果 $S' = \{k - s : s \in S\}$，则 Max-BCSP($f_{S,k}$) 的每个实例都可以视为 Max-BCSP($f_{S',k}$) 的一个具有相同值的实例，因为对于任意约束 $C = (\mathbf{b}, \mathbf{j}, w)$ 和赋值 $\mathbf{x} \in \mathbb{Z}_2^n$，都有 $f_{S,k}(\mathbf{b} + \mathbf{x}|_{\mathbf{j}}) = f_{S',k}(\mathbf{b} + (\mathbf{x} + \mathbf{1})|_{\mathbf{j}})$。因此，我们将关注范围进一步缩小到 S 的每个元素都大于 $k/2$ 的情形。

7.3 Techniques

7.3.1 Formulations of the optimization problem

为了证明 $\alpha(\text{2AND}) = \frac{4}{9}$，Chou、Golovnev、Sudan 和 Velusamy [CGSV21a在例 1] 中使用了以下对推论 5.3中优化问题的重新表述。对于对称谓词 $f_{S,\,k}$ 和 $\mu \in [-1, 1]$，令

$$\beta_{S,k}(\mu) = \inf_{\mathcal{D}_N \in \Delta_k:\ \mu(\mathcal{D}_N)=\mu} \beta_S(\mathcal{D}_N) \text{ and } \gamma_{S,k}(\mu) = \sup_{\mathcal{D}_Y \in \Delta_k:\ \mu(\mathcal{D}_Y)=\mu} \gamma_S(\mathcal{D}_Y); \tag{7.14}$$

then

$$\alpha(f_{S,k}) = \inf_{\mu \in [-1,1]} \left(\frac{\beta_{S,k}(\mu)}{\gamma_{S,k}(\mu)} \right). \tag{7.15}$$

方程 (7.15) 右侧的优化问题看起来比推论 5.3 中的优化问题更简单，因为它是单变量的，但其中隐藏着一个难点：要找到显式解，需要给出 $\beta_{S,k}(\mu)$ 和$\gamma_{S,k}(\mu)$ 的显式公式。对于 2AND $= f_{\{2\}}$,2，Chou、Golovnev、Sudan 和 Velusamy [CGSV21a] 首先证明 $\gamma_{\{2\}}$, 2(μ) 是关于 μ 的线性函数。然后，为了求出 $\beta_{S,k}(\mu)$，他们在 $p \in [0, 1]$ 上最大化二次函数 $\lambda_{\{2\}}(\mathcal{D}_N, p)$，从而求得 $\beta_{\{2\}}(\mathcal{D}_N)$（见例 5.5）；接着对 $\mathcal{D}_N$ 进行优化，使得$\mu(\mathcal{D}_N) = \mu$，从而求得 $\beta_{\{2\}}$,2(μ)。

虽然我们将在下文§7.4 看到，$\gamma_{S,\,k}(\mu)$ 对所有对称谓词 μ 而言，都是$f_{S\text{关于}k}$的分段线性函数，但我们不知道如何求出$\beta_{S,\,k}(\mu)$ 的闭式表达，即使对于3AND (尽管$\gamma_{S,\,k}(\mu)$ 通常是 μ的分段线性函数，见下文引理 7.22)。因此，在这项工作中，我们提出了另一种优化问题表述：

$$\alpha(f_{S,k}) = \inf_{\mathcal{D}_N \in \Delta_k} \left(\frac{\beta_S(\mathcal{D}_N)}{\gamma_{S,k}(\mu(\mathcal{D}_N))} \right). \tag{7.16}$$

我们认为直接对 $\mathcal{D}_N \in \Delta_k$ 进行优化是一个重要的概念转变。尤其是，我们的表述强调，计算 $\beta_S(\mathcal{D}_N)$ 是核心难点，但我们仍可利用计算 $\gamma_{S,k}(\mu)$ 相对简单这一优势。

7.3.2 Our contribution: The max-min method

原则上，求解方程 (7.16) 右侧的优化问题仍然需要计算 $\beta_S(\mathcal{D}_N)$，其中涉及求一个次数为 k 的多项式的最大值。为克服这一困难，我们有了一个关键发现：即使在 2AND 情形下，Chou、Golovnev、Sudan 和 Velusamy [CGSV21a] 也未曾注意到这一点（见备注 4.13）。令 $\mathcal{D}_N^*$ 最小化方程 (7.16) 的右侧，并令 p^* 最大化 $\lambda_S(\mathcal{D}_N^*, \cdot)$。将 $\beta_S(\mathcal{D}) = \sup_{p\in[0,1]} \lambda_S(\mathcal{D}, p)$ 代入方程 (7.16)，并应用极大极小不等式，我们得到

$$\begin{aligned}\alpha(f_{S,k}) = \inf_{\mathcal{D}_N\in\Delta_k} \sup_{p\in[0,1]} \left(\frac{\lambda_S(\mathcal{D}_N,p)}{\gamma_{S,k}(\mu(\mathcal{D}_N))}\right) &\geq \sup_{p\in[0,1]} \inf_{\mathcal{D}_N\in\Delta_k} \left(\frac{\lambda_S(\mathcal{D}_N,p)}{\gamma_{S,k}(\mu(\mathcal{D}_N))}\right) \\ &\geq \inf_{\mathcal{D}_N\in\Delta_k} \left(\frac{\lambda_S(\mathcal{D}_N,p^*)}{\gamma_{S,k}(\mu(\mathcal{D}_N))}\right).\end{aligned} \tag{7.17}$$

给定 p^*，方程 (7.17) 右侧的计算相对简单，它是关于 $\mathcal{D}_N$ 的线性函数与分段线性函数之比。我们发现，在各种各样的情形下，方程 (7.17) 右侧的量等于 $\alpha(f_{S,k})$；也就是说，$(\mathcal{D}_N^*, p^*)$ 是 $\lambda_S(\mathcal{D}_N,p)\,\gamma_{S,k}(\mu(\mathcal{D}_N))$ 的鞍点 .*

这产生了一种新颖的技术，我们称之为“极大极小方法”，用于求解 $\alpha(f_{S,k})$ 的闭式表达。首先，我们猜测 $\mathcal{D}_N^*$ 和 p^*，然后通过解析方法证明 $\lambda_S(\mathcal{D}_N,p)\,\gamma_{S,k}(\mu(\mathcal{D}_N))$ 在 $(\mathcal{D}_N^*, p^*)$ 处~~具有一个~~鞍点，并且 $\lambda_S(\mathcal{D}_N, p)$ 在 p^* 处取得最大值。这些结果分别意味着，$\lambda_S(\mathcal{D}_N^*,p^*)$ 和 $\gamma_{S,k}(\mu(\mathcal{D}_N^*))$ 是 $\alpha(~~f_{S,k}~~)$ ~~的下~~界和上界。例如，在 §7.5.1 中，为了给出奇数 k 情况下 $\alpha(k\text{AND})$ 的闭式表达（即定理 7.2 的奇数情形），我们猜测 $\mathcal{D}_N^*\langle(k+1)/2\rangle = 1$ 和 $p^* = \frac{k+1}{2k}$（通过使用 Mathematica 计算较小的实例得到）~~，~~然后在两个独立的引理中分别验证鞍点条件和最大化条件（引理 7.23

*这一术语源自优化文献；这类点也被称为满足“强极大极小性质”（例如参见 [BV04，第 115, 238]页）。对于分别在第一个和第二个参数上为凹函数和凸函数的函数，冯·诺伊曼的极小极大定理保证了鞍点性质，但我们所知的这一定理及其推广甚至不适用于 3AND。

和7.24，分别）。然后，我们通过分析适当代入后的 $\alpha(k$与$) = \alpha'_k$ 右侧，证明方程(7.17)。对于 k与偶数 k 的情形（另见定理 7.2），以及第 7.5.2 节至7.5.4节中的其他各种情形，我们也采用类似的技术。

在上述所有情形中，我们构造的 $\mathcal{D}^*_N$ 最多支撑在两个不同的汉明权重上，而这一性质使得求解 $\mathcal{D}^*_N$ 变得可行（借助计算机辅助）。不过，这种技术并非“万灵药”：并非所有对称布尔 CSP 的草图近似性，都能通过寻找支撑在两个元素上的最优 $\mathcal{D}^*_N$，并使用极大极小方法来精确计算。事实上（如§7.5.4中所述），我们借助计算机辅助验证了，4的情形并非如此。

最后，我们指出，鞍点性质正是为 p^*所需的值的定义，它用于我们的简单经典算法，以输出 最大布尔约束满足问题(Th^t_k) 的近似最优赋值，其中 $f_{S,k} = \mathsf{Th}^t_k$ 是一个阈值函数（见 定理 7.43）。

为了实际执行极大极小方法，我们依赖以下用于优化线性函数比值的简单不等式：

命题 7.18。设 $f\colon \mathbb{R}^n \to \mathbb{R}$ 由方程 $f(x) = a\cdot x\ b\cdot x$ 定义，其中某些 $a, b \in \mathbb{R}^n_{\geq 0}$。对于任意 $y(1), \ldots, y(r) \in \mathbb{R}^n_{\geq 0}$，以及任意满足每个 $x_i \geq 0$ 的 $x = \sum_{i=1}^r \alpha_i y(i)$，我们有 $f(x) \geq \min_i f(y(i))$。特别地，取 $r = n$，并令 $y(1), \ldots, y(n)$ 为 $\mathbb{R}^n$的标准基，则对于任意 $x \in \mathbb{R}^n_{\geq 0}$，我们有 $f(x) \geq \min_i \frac{a_i}{b_i}$。

证明。首先，我们证明不失一般性，只需考虑 $r = n$ 和 $\mathbf{y}(1), \ldots, \mathbf{y}(n)$ 是 $\mathbb{R}^n$ 的标准基这一特殊情形。事实上，假设这一特殊情形成立，并注意到对于一般情形，我们可以令 $\mathbf{a}' = (\mathbf{a}\cdot\mathbf{y}(1), \ldots, \mathbf{a}\cdot\mathbf{y}(r))$、$\mathbf{b}' = (\mathbf{b}\cdot\mathbf{y}(1), \ldots, \mathbf{b}\cdot\mathbf{y}(r))$、$\mathbf{x}' = (x_1, \ldots, x_r)$，并令 $\mathbf{y}'(1), \ldots, \mathbf{y}'(r)$ 为 $\mathbb{R}^r$ 的标准基。于是 $\mathbf{x}' = \sum_{i=1}^r \alpha_i \mathbf{y}'(i)$ 且

$$f(\mathbf{x}) = \frac{\sum_{i=1}^r (\mathbf{a}\cdot\mathbf{y}(i))\alpha_i}{\sum_{i=1}^r (\mathbf{b}\cdot\mathbf{y}(i))\alpha_i} = \frac{\mathbf{a}'\cdot\mathbf{x}'}{\mathbf{b}'\cdot\mathbf{x}'} \geq \min_{i\in[r]} \frac{\mathbf{a}'\cdot\mathbf{y}'(i)}{\mathbf{b}'\cdot\mathbf{y}'(i)} = \min_{i\in[r]} \frac{\mathbf{a}\cdot\mathbf{y}(i)}{\mathbf{b}\cdot\mathbf{y}(i)}.$$

现在我们证明特殊情形：假设 $r = n$ 且 $\mathbf{y}(1), \ldots, \mathbf{y}(n)$ 是 $\mathbb{R}^n$ 的标准基。我们有 $f(\mathbf{y}(i)) = \frac{a_i}{b_i}$。不失一般性，假设 $f(\mathbf{y}(1)) = \min\{f(\mathbf{y}(i)) \colon i \in [n]\}$，即 $\frac{a_1}{b_1} \leq \frac{a_i}{b_i}$ 对所有 $i \in [n]$ 都成立。那么 $a_i \geq \frac{a_1 b_i}{b_1}$ 对所有 $i \in [n]$ 都成立，因此

$$\mathbf{a}\cdot\mathbf{x} \geq \sum_{i=1}^n \frac{a_1 b_i}{b_1}\alpha_i = \frac{a_1}{b_1}(\mathbf{b}\cdot\mathbf{x}).$$

因此

$$f(\mathbf{x}) = \frac{\mathbf{a}\cdot\mathbf{x}}{\mathbf{b}\cdot\mathbf{x}} \geq \frac{a_1}{b_1} = f(\mathbf{y}(1)),$$

正如所需。 □

7.3.3 Streaming lower bounds

基于这一设定，我们也可以陈述关于 [CGSV21a]的流式下界对 Max-3AND的适用性（或不适用性）的结果：

定理 7.19。 不存在定义在 Δ_3 上的无限序列 $(\mathcal{D}_Y^{(1)}, \mathcal{D}_N^{(1)}), (\mathcal{D}_Y^{(2)}, \mathcal{D}_N^{(2)}) \ldots$，由填充单向配对构成，使得

$$\lim_{t\to\infty} \frac{\beta_{\{3\}}(\mathcal{D}_N^{(t)})}{\gamma_{\{3\}}(\mathcal{D}_Y^{(t)})} = \frac{2}{9}.$$

不过，利用填充单向配对，我们仍然可以得到不错的界：

观察 7.20。 填充单向配对 $\mathcal{D}_N = (0, 0.45, 0.45, 0.1)$ $\mathcal{D}_Y = (0.45, 0, 0, 0.55)$（通过数值搜索发现）确实为 *3AND* 证明了一个流式可近似性上界 $\approx .2362$，这仍然相当接近 $\alpha(3\text{-}AND) = \frac{2}{9}$。

定理 7.19 的形式化证明见 §7.7；以下是证明概要：

证明概要。 如§7.3.2所述，由于 $k = 3$为奇数，要证明定理 7.2，我们使用极大极小方法证明 $\mathcal{D}_N^* = (0, 0, 1, 0)$使$^{\beta_{\{3\}}(\cdot)\,\gamma_{\{3\},\,3}(\mu(\cdot))}$最小。我们可以证明，相应的$\gamma_{\{3\},\,3}$值由 $\mathcal{D}_Y^* = (\frac{1}{3}, 0, 0, \frac{2}{3})$取得。特别地，$(\mathcal{D}_N^*, \mathcal{D}_Y^*)$不是填充单向配对。

我们可以证明，对于某个特定的 μ，$\gamma_{\{3\}}$ 的极小化者通常是唯一的。因此，只需进一步证明 $\mathcal{D}_N^*$ 是 $^{\beta_{\{3\}}(\cdot)\,\gamma_{\{3\},3}(\mu(\cdot))}$ 的唯一极小化者。为此，极大极小方法并不足够，因为 $^{\lambda_{\{3\}}(\cdot,p^*)\,\gamma_{\{3\},3}(\mu(\cdot))}$ 在 $\mathcal{D}_N^*$ 处并非唯一取到极小值（此处我们选择了 $p^* = \frac{2}{3}$）。直观而言，这是因为 p^* 并不能很好地估计 $\lambda_{\{3\}}(\mathcal{D}_N, \cdot)$ 的极大化者。为了解决这一问题，我们注意到 $\lambda_{\{3\}}((1, 0, 0, 0) \cdot)$ $\lambda_{\{3\}}((0, 1, 0, 0) \cdot)$、$\lambda_{\{3\}}((0, 0, 1, 0) \cdot)$ 和 $\lambda_{\{3\}}((0, 0, 0, 1) \cdot)$ 分别在 0、1 3 、2 3 和 1 处取到极小值。因此，我们改为在 $\frac{1}{3}\mathcal{D}_N\langle 1\rangle + \frac{2}{3}\mathcal{D}_N\langle 2\rangle + \mathcal{D}_N\langle 3\rangle$ 处求值，以此给出 $\lambda_{\{3\}}(\mathcal{D}_N, \cdot)$ 的下界；这足以证明 $\mathcal{D}_N^*$ 的唯一性。随后由连续性论证即可得出定理。

□

7.4 Explicit formulas for λ_S and $\gamma_{S,k}$

本节陈述并证明 $\lambda_S(\mathcal{D},\ p)$ 和 $\gamma_{S,\ k}(\mu)$ 的显式公式，这些公式将在后续章节中发挥作用。

引理 7.21。 对于任意 $\mathcal{D} \in \Delta_k$ 和 $p \in [0,1]$，我们有

$$\lambda_S(\mathcal{D},p) = \sum_{s\in S}\sum_{i=0}^{k}\left(\sum_{j=\max\{0,s-(k-i)\}}^{\min\{i,s\}}\binom{i}{j}\binom{k-i}{s-j}q^{s+i-2j}p^{k-s-i+2j}\right)\mathcal{D}\langle i\rangle$$

其中 q 定义为$= 1-p$。

证明。 根据期望的线性性和对称性，只需固定 s 和 i 并计算：给定一个汉明重量为 i 的固定字符串 $\mathbf{a} = (a_1,\ \ldots\ldots,\ a_k)$，以及一个随机串 $\mathbf{b} = (b_1,\ \ldots\ldots,\ b_k) \sim \mathcal{B}_p^k$，事件 $\|\mathbf{a}+\mathbf{b}\|_0 = s$发生的概率。

令 $A = \text{sup}\ \ \mathbf{p(a)} = \{t \in [k] : a_t = 1\}$，类似地 $B = \mathbf{supp(b)}$。我们有 $|A| = i$ 并且

$$s = \|\mathbf{a}+\mathbf{b}\|_0 = |A\cap B| + |([k]\setminus A)\cap([k]\setminus B)|.$$

设 $j = |A\cap B|$，并根据 j 分情况讨论。

给定固定的 j，必有 $|A\cap B| = j$ 和 $|([k]\setminus A)\cap([k]\setminus B)| = s-j$。因此，若 j 满足 $j \le i,\ s-j \le k-i,\ j \ge 0,\ j \le s$，则 $\binom{i}{j}$ 有种选择方式，$A\cap B$ 和 $\binom{k-i}{s-j}$ 有种选择方式，$([k]\setminus A)\cap([k]\setminus B)$；这些选择共同完全确定了 B。此外 $\|\mathbf{b}\|_0 = |B| = |B\cap A| + |B\cap([k]\setminus A)| = j + (k-i) - (s-j) = k-s-i+2j$，从而得到所需公式。

□

引理 7.22。 设 $S \subseteq [k]$，并设 s 为其最小元素，t 为其最大元素（两者不必不同）。那么对于 $\mu \in [-1,1]$，

$$\gamma_{S,k}(\mu) = \begin{cases} \frac{1+\mu}{1+\epsilon_{s,k}} & \mu \in [-1,\epsilon_{s,k}) \\ 1 & \mu \in [\epsilon_{s,k},\epsilon_{t,k}] \\ \frac{1-\mu}{1-\epsilon_{t,k}} & \mu \in (\epsilon_{t,k},1] \end{cases}$$

（也等于 最小值 $\left\{\frac{1+\mu}{1+\epsilon_{s\ ,\ k}},\ \mathbf{1},\ \frac{1-\mu}{1-\epsilon_{t\ ,\ k}}\right\}$）。

证明。 对于 $\mu \in [-1,1]$，在（方程 (7.14)）中，我们定义了

$$\gamma_{S,k}(\mu) = \sup_{\mathcal{D}_Y \in \Delta_k : \mu(\mathcal{D}_Y)=\mu} \gamma_S(\mathcal{D}_Y),$$

其中方程 (5.1)，$\gamma_S(\mathcal{D}_Y) = \sum_{i\in S} \mathcal{D}_Y\langle i\rangle$。对于 $\mathcal{D}_Y \in \Delta_k$，令$\mathsf{supp}(\mathcal{D}_Y) = \{i \in [k] : \mathcal{D}_Y\langle i\rangle > 0\}$。我们根据 μ分情况讨论。

Case 1: $\mu \in [-1, \epsilon_{s,k}]$. 我们的策略是将问题归约到 $\mathsf{supp}(\mathcal{D}_Y) \subseteq \{0, s\}$ 的情形，同时保持边缘分布 μ 不变，并使 γ_S 的值非严格递增。

考虑对分布 $\mathcal{D}_Y \in \Delta_k$ 进行以下操作：对于 $u < v < w \in [k]$，将 $\mathcal{D}_Y\langle u\rangle$ 增加 $\mathcal{D}_Y\langle v\rangle \frac{w-v}{w-u}$，将 $\mathcal{D}_Y\langle w\rangle$ 增加 $\mathcal{D}_Y\langle v\rangle \frac{v-u}{w-u}$，并将 $\mathcal{D}_Y\langle v\rangle$ 设为零。注意，这会得到一个边缘分布相同的新分布，因为

$$\mathcal{D}_Y\langle v\rangle \frac{w-v}{w-u}\epsilon_{u,k} + \mathcal{D}_Y\langle v\rangle \frac{v-u}{w-u}\epsilon_{w,k} = \mathcal{D}_Y\langle v\rangle\, \epsilon_{v,k}.$$

给定初始分布 $\mathcal{D}_Y$，我们可以应用此操作，通过重新分配到 $\mathcal{D}_Y\langle 0\rangle$ 和 $\mathcal{D}_Y\langle s\rangle$，将 $\mathcal{D}_Y\langle v\rangle$ 对于 $v \in \{1, \dots, s-1\}$ 置零，同时保持边缘分布，并且只会增加 γ_S 的值（因为 $v \notin S$，而 $s \in S$）。类似地，当 $v \in \{t+1, \dots, k-1\}$ 时，我们可以将 $\mathcal{D}_Y\langle v\rangle$ 重新分配到 $\mathcal{D}_Y\langle t\rangle$ 和 $\mathcal{D}_Y\langle k\rangle$；当 $v \in \{s+1, \dots, t-1\}$ 时，则可以重新分配到 $\mathcal{D}_Y\langle s\rangle$ 和 $\mathcal{D}_Y\langle t\rangle$。因此，我们只需考虑 $\mathsf{supp}(\mathcal{D}) \subseteq \{0, s, t, k\}$ 的情形。为简单起见，我们假设 $0, s, t, k$ 各不相同。

根据$\epsilon_{i,k}$ 的定义，我们有

$$\mu(\mathcal{D}) = -\mathcal{D}_Y\langle 0\rangle + \mathcal{D}_Y\langle s\rangle \left(-1 + \frac{2s}{k}\right) + \mathcal{D}_Y\langle t\rangle \left(-1 + \frac{2t}{k}\right) + \mathcal{D}_Y\langle k\rangle \le -1 + \frac{2s}{k}$$

（根据此情况的假设）。代入 $\mathcal{D}_Y\langle s\rangle = 1 - \mathcal{D}_Y\langle 0\rangle - \mathcal{D}_Y\langle t\rangle - \mathcal{D}_Y\langle k\rangle$ 并两边同乘$\frac{k}{2}$，我们有

$$k\mathcal{D}_Y\langle k\rangle - s\mathcal{D}_Y\langle 0\rangle - s\mathcal{D}_Y\langle t\rangle - s\mathcal{D}_Y\langle k\rangle + t\mathcal{D}_Y\langle t\rangle \le 0;$$

定义 $\delta = \mathcal{D}_Y\langle t\rangle(\frac{t}{s} - 1) + \mathcal{D}_Y\langle k\rangle(\frac{k}{s} - 1)$ 后，我们可以重新整理得到 $\mathcal{D}_Y\langle 0\rangle \ge \delta$。然后，给定$\mathcal{D}_Y$，我们可以将 $\mathcal{D}_Y\langle t\rangle$ 和 $\mathcal{D}_Y\langle k\rangle$置零，将 $\mathcal{D}_Y\langle 0\rangle$ 减少 δ，并相应地增加

$\mathcal{D}_Y\langle s\rangle$ $\mathcal{D}_Y\langle t\rangle + \mathcal{D}_Y\langle k\rangle + \delta$。这保持了边缘分布，因为

$$(\delta + \mathcal{D}_Y\langle t\rangle + \mathcal{D}_Y\langle k\rangle)\,\epsilon_{s,k} = -\delta + \mathcal{D}_Y\langle t\rangle\,\epsilon_{t,k} + \mathcal{D}_Y\langle k\rangle$$

且只能增大 γ_S。

因此，只需考虑 $\mathrm{supp}(\mathcal{D}_Y) \subseteq \{0, s\}$ 的情况。这唯一确定了$\mathcal{D}_Y$（因为 μ 固定）；我们有 $\mathcal{D}_Y\langle 0\rangle = \begin{smallmatrix} \epsilon_s & k-\mu \\ \epsilon_s & k+1 \end{smallmatrix}$，并且 $\mathcal{D}_Y\langle s\rangle = \begin{smallmatrix} 1+\mu \\ \epsilon_s & k+1 \end{smallmatrix}$，从而得到所需的 γ_S值。

Case 2: $\mu \in [\epsilon_{s,k}, \epsilon_{t,k}]$. 我们只需构造 $\mathcal{D}_Y$，使其满足 $\mathcal{D}_Y\langle s\rangle = \begin{smallmatrix} \epsilon_t & k-\mu \\ \epsilon_s & k-\epsilon_t \end{smallmatrix}$ 以及 $\mathcal{D}_Y\langle t\rangle = \begin{smallmatrix} \mu-\epsilon_s & k \\ \epsilon_s & k-\epsilon_t \end{smallmatrix}$；我们有 $\mu(\mathcal{D}_Y) = \mu$，且 $\gamma_S(\mathcal{D}_Y) = 1$。

Case 3: $\mu \in [\epsilon_{t,k}, 1]$. 按照与情形1相同的对称逻辑，我们考虑 $\mathcal{D}_Y$ 支撑于 $\{t, k\}$，并设定 $\mathcal{D}_Y\langle t\rangle = \begin{smallmatrix} 1-\mu \\ 1-\epsilon_t & k \end{smallmatrix}$ 和 $\mathcal{D}_Y\langle k\rangle = \begin{smallmatrix} \mu-\epsilon_t & k \\ 1-\epsilon_t & k \end{smallmatrix}$，从而得到 $\mu(\mathcal{D}_Y) = \mu$ 和$\gamma_S(\mathcal{D}_Y) = \mathcal{D}_Y\langle t\rangle$。 □

7.5 Sketching approximation ratio analyses

7.5.1 Max-kAND

本节中，我们证明 定理 7.2 （关于 Max-kAND 的草图近似性）。回顾一下，在 方程 (7.1) 中，我们定义了

$$\alpha'_k = \left(\frac{(k-1)(k+1)}{4k^2}\right)^{(k-1)/2}.$$

定理 7.2 可由以下两个引理直接推出：

引理 7.23。 对于所有奇数 $k \geq 3$, α（k*AND*） $\leq \alpha'_k$。对于所有偶数 $k \geq 2$, α（k*AND*） $\leq 2\alpha'_{k+1}$。

引理 7.24。 对于所有奇数 $k \geq 3$, $\alpha(k$与$) \geq \alpha'_k$。对于所有偶数 $k \geq 2$, $\alpha(k$与$) \geq 2\alpha'_{k+1}$。

首先，我们给出$\gamma_{\{k\}、k}(\mu(\mathcal{D}))$ 和 $\lambda_{\{k\}}(\mathcal{D}, p)$ 的显式公式。注意， $\{k\}$ 的最小元素是 k，且$\epsilon_{k,k} = 1$。因此，对于 $\mathcal{D} \in \Delta_k$，由引理 7.12 和7.22

that

$$\gamma_{\{k\},k}(\mu(\mathcal{D})) = \frac{1 + \sum_{i=0}^{k}(-1 + \frac{2i}{k})\,\mathcal{D}\langle i\rangle}{2} = \sum_{i=0}^{k} \frac{i}{k}\,\mathcal{D}\langle i\rangle. \tag{7.25}$$

类似地，我们可以将引理 7.21 应用于 $s = k$；对于每个 $i \in [k] \cup \{0\}$，$\max\{0, s-(k-i)\} = \min\{i, k\} = i$，因此我们只需考虑 $j = i$，于是 $\binom{i}{j} = \binom{k-i}{s-j} = 1$。因此，对于 $q = 1 - p$，我们有

$$\lambda_{\{k\}}(\mathcal{D}, p) = \sum_{i=0}^{k} q^{k-i} p^{i}\,\mathcal{D}\langle i\rangle \tag{7.26}$$

现在，我们直接证明引理 7.23：

引理 7.23 的证明。 考虑 k 为奇数的情形。定义 $\mathcal{D}_N^*$ 如下：$\mathcal{D}_N^*\langle (k+1)/2\rangle = 1$，并令 $p^* = \frac{1}{2} + \frac{1}{2k}$。由于

$$\alpha(k\mathsf{AND}) \le \frac{\beta_{\{k\}}(\mathcal{D}_N^*)}{\gamma_{\{k\},k}(\mu(\mathcal{D}_N^*))} \text{ and } \beta_{\{k\}}(\mathcal{D}_N) = \sup_{p\in[0,1]} \lambda_{\{k\}}(\mathcal{D}_N^*, p),$$

根据方程 (5.1) 和(7.16)，分别只需验证 p^* 使 $\lambda_{\{k\}}(\mathcal{D}_N^*, \cdot)$取最大值，且

$$\frac{\lambda_{\{k\}}(\mathcal{D}_N^*, p^*)}{\gamma_{\{k\},k}(\mu(\mathcal{D}_N^*))} = \alpha_k'.$$

事实上，根据公式 (7.26),

$$\lambda_{\{k\}}(\mathcal{D}_N^*, p) = (1-p)^{(k-1)/2} p^{(k+1)/2}.$$

为证明 p^* 使 $\lambda_{\{k\}}(\mathcal{D}_N^*, \cdot)$取最大值，我们计算其导数：

$$\frac{d}{dp}\left[(1-p)^{(k-1)/2} p^{(k+1)/2}\right] = -(1-p)^{(k-3)/2} p^{(k-1)/2}\left(kp - \frac{k+1}{2}\right),$$

其零点仅为 0、1、和 p^*。因此，$\lambda_{\{k\}}(\mathcal{D}_N^*, \cdot)$ 的临界点仅为 0、1、和 p^*，且其在 p^* 处取得最大值，因为它在 0 和 1 处为零。最后，根据方程 (7.25)和(7.26) 以及 α_k'的定义，

$$\frac{\lambda_{\{k\}}(\mathcal{D}_N^*, p^*)}{\gamma_{\{k\},k}(\mu(\mathcal{D}_N^*))} = \frac{\left(\frac{1}{2} - \frac{1}{2k}\right)^{(k-1)/2}\left(\frac{1}{2} + \frac{1}{2k}\right)^{(k+1)/2}}{\frac{1}{2}\left(1 + \frac{1}{k}\right)} = \alpha_k',$$

如所需。

类似地，考虑 k 为偶数的情况；在此，我们将 $\mathcal{D}_N^*$ 定义为 $\mathcal{D}_N^*\langle k/2\rangle = \left(\frac{k}{2}+1\right)^2\left(\frac{k}{2}\right)^2 + \left(\frac{k}{2}+1\right)^2$ 和 $\mathcal{D}_N^*\langle \frac{k}{2}+1\rangle = \left(\frac{k}{2}\right)^2\left(\frac{k}{2}\right)^2 + \left(\frac{k}{2}+1\right)^2$，并令 $p^* = \frac{1}{2} + \frac{1}{2(k+1)}$。利用公式 (7.26) 计算 $\lambda_{\{k\}}(\mathcal{D}_N^*, \cdot)$ 的导数，得到

$$\frac{d}{dp}\left[\frac{\left(\frac{k}{2}+1\right)^2}{\left(\frac{k}{2}\right)^2+\left(\frac{k}{2}+1\right)^2}(1-p)^{k/2}p^{k/2} + \frac{\left(\frac{k}{2}\right)^2}{\left(\frac{k}{2}\right)^2+\left(\frac{k}{2}+1\right)^2}(1-p)^{k/2-1}p^{k/2+1}\right]$$
$$= -\frac{k}{2+2k+2k^2}(1-p)^{k/2-2}p^{k/2-1}\left(\frac{k}{2}+1-2p\right)\left((k+1)p - \left(\frac{k}{2}+1\right)\right),$$

因此，$\lambda_{\{k\}}(\mathcal{D}_N^*, \cdot)$ 在 0、1、$\frac{1}{2}+\frac{k}{4}$ 和 p^* 处有临界点；p^* 是区间 $[0,1]$ 中唯一使 $\lambda_{\{k\}}(\mathcal{D}_N^*, \cdot)$ 为正的临界点，因此它是其最大值。最后，可以通过代数计算验证 方程 (7.25) 和 方程 (7.26) 得出 $\lambda_{\{k\}}(\mathcal{D}_N^*, p^*) \gamma_{\{k\},k}(\mu(\mathcal{D}_N^*)) = 2\alpha'_{k+1}$，如所需。

□

我们用引理 7.24的极大极小方法证明。

引理 7.24的证明。首先，假设 $k \geq 3$ 是奇数。令 $p^* = \frac{1}{2} + \frac{1}{2k} = \frac{k+1}{2k}$。我们要证明

$$\begin{aligned}
\alpha'_k &\leq \inf_{\mathcal{D}_N \in \Delta_k} \frac{\lambda_{\{k\}}(\mathcal{D}_N, p^*)}{\gamma_{\{k\},k}(\mu(\mathcal{D}_N))} && \text{(max-min inequality, i.e., Eq. (7.17))} \\
&= \inf_{\mathcal{D}_N \in \Delta_k} \frac{\sum_{i=0}^k (1-p^*)^{k-i}(p^*)^i \mathcal{D}_N\langle i\rangle}{\sum_{i=0}^k \frac{i}{k}\mathcal{D}_N\langle i\rangle}. && \text{(Eqs. (7.25) and (7.26))}
\end{aligned}$$

根据命题 7.18，只需验证

$$\forall i \in [k]\cup\{0\}, \quad (1-p^*)^{k-i}(p^*)^i \geq \alpha'_k \cdot \frac{i}{k}.$$

根据 α'_k 的定义，我们有 $\alpha'_k = (1-p^*)^{(k-1)/2}(p^*)^{(k-1)/2}$。定义 $r = \frac{p^*}{1-p^*} = \frac{k+1}{k-1}$（使得 $p^* = r(1-p^*)$），提出 $(1-p^*)^k$ 并化简后，可将所需的不等式改写为

$$\forall i \in [k]\cup\{0\}, \quad \frac{1}{2}(k-1)r^{i-\frac{k-1}{2}} \geq i. \tag{7.27}$$

当 $i=(k+1)/2$ 或 $(k-1)/2$ 时，方程 (7.27) 中等号成立。我们通过归纳法推广到 i 的其他值。事实上，当 $i \geq (k+1)/2$ 时，“i 满足方程 (7.27)”蕴含“$i+1$ 满足方程 (7.27)”，因为 $ri \geq i+1$；而当 $i \leq (k-1)/2$ 时，“i 满足方程 (7.27)”蕴含“$i-1$ 满足方程 (7.27)”，因为 $\frac{1}{r}i \geq i-1$。

同样，当 $k \geq 2$ 为偶数时，我们令$p^* = \frac{1}{2} + \frac{1}{2(k+1)}$并令$r = \frac{p^*}{1-p^*} = \frac{k+2}{k}$此时，对于 $i \in [k] \cup \{0\}$，可以推导出方程 (7.27)的如下类似结果：

$$\forall i \in [k] \cup \{0\}, \quad \frac{1}{2} k r^{i-\frac{k}{2}} \geq i,$$

这些不等式可通过相同的归纳论证得到。 □

7.5.2 Th_k^{k-1} FOR EVEN k

在本小节中，我们证明定理 7.4(关于Th_k^{k-1} 在 $k \geq 2$为偶数时的草图近似性)。证明以下两个引理是充要的：

引理 7.28。对于所有偶数 $k \geq 2$, $\alpha(Th_k^{k-1}) \leq \frac{k}{2}\alpha'_{k-1}$。

引理 7.29。对于所有偶数 $k \geq 2$, $\alpha(Th_k^{k-1}) \geq \frac{k}{2}\alpha'_{k-1}$。

首先，我们给出$\gamma_{\{k-1,k\},k}$ 和 $\lambda_{\{k-1,k\}}$的显式公式。我们有$\mathsf{Th}_k^{k-1} = f_{\{k-1,k\},k}$和$\epsilon_{k-1,k} = -1 + \frac{2}{(k-1)k} = 1 - \frac{2}{k}$。因此，引理 7.12 和7.22 给出

$$\gamma_{\{k-1,k\},k}(\mu(\mathcal{D})) = \min\left\{\frac{1+\sum_{i=0}^{k}(-1+\frac{2i}{k})\,\mathcal{D}\langle i\rangle}{2-\frac{2}{k}}, 1\right\} = \min\left\{\sum_{i=0}^{k}\frac{i}{k-1}\,\mathcal{D}\langle i\rangle, 1\right\}. \quad (7.30)$$

接下来，我们用 $\lambda_{\{k-1,k\}}(\mathcal{D}, p)$结合引理 7.21计算。设 $q=1-p$，并考察 $\mathcal{D}\langle i\rangle$上的系数。$s=k$ 贡献 $q^{k-i}p^k$。在 $i \leq k-1$的情形下，$s=k-1$ 贡献 $(k-i)\,q^{k-i-1}p^{i+1}$，其中 $j=i$；而在 $i \geq 1$的情形下，$s=k-1$ 贡献 $iq^{k-i+1}p^{i-1}$，其中$j=i-1$。因此，综上可写为

$$\lambda_{\{k-1,k\}}(\mathcal{D}, p) = \sum_{i=0}^{k} q^{k-i-1}p^{i-1}\left((k-i)p^2 + pq + iq^2\right)\mathcal{D}\langle i\rangle. \quad (7.31)$$

现在，我们证明引理 7.28 和 7.29。

引理 *7.28* 的证明。 如同引理 7.23的证明，只需构造 $\mathcal{D}_N^*$ 和 p^*，使得 p^* 最大化 $\lambda_{\{k-1,k\}}(\mathcal{D}_N^*, \cdot)$ 且 $\lambda_{\{k-1,k\}}(\mathcal{D}_N^*, p^*)\gamma_{\{k-1,k\},k}(\mu(\mathcal{D}_N^*)) = \frac{k}{2}\alpha'_{k-1}$。

我们再次令 $p^* = \frac{1}{2} + \frac{1}{2}(k-1)$，但将 $\mathcal{D}_N^*$ 定义为 $\mathcal{D}_N^*\langle k/2\rangle = (\frac{k}{2})^2(\frac{k}{2})^2+(\frac{k}{2}-1)^2$，并令 $\mathcal{D}_N^*\langle \frac{k}{2}+1\rangle = (\frac{k}{2}-1)^2(\frac{k}{2})^2+(\frac{k}{2}-1)^2$。根据方程 (7.31)，$\lambda_{\{k-1,k\}}(\mathcal{D}_N^*, \cdot)$ 的导数现在是

$$\frac{d}{dp}\left[\frac{\left(\frac{k}{2}\right)^2}{\left(\frac{k}{2}\right)^2+\left(\frac{k}{2}-1\right)^2}(1-p)^{k/2-1}p^{k/2-1}\left(\frac{k}{2}p^2+pq+\frac{k}{2}q^2\right)+\right.$$
$$\left.\frac{\left(\frac{k}{2}-1\right)^2}{\left(\frac{k}{2}\right)^2+\left(\frac{k}{2}-1\right)^2}(1-p)^{k/2-2}p^{k/2}\left(\left(\frac{k}{2}-1\right)p^2+pq+\left(\frac{k}{2}+1\right)q^2\right)\right]$$
$$= -\frac{1}{8(k^2-2k+2)}(1-p)^{k/2-3}p^{k/2-2}(-k+(2(k-1)p)\xi(p),$$

其中 $\xi(p)$ 是三次多项式。

$$\xi(p) = -8k(k-1)p^3 + 2(k^3+k^2+6k-12)p^2 - 2(k^3-4)p + k^2(k-2).$$

因此，$\lambda_{\{k-1,k\}}$ 在区间 $[0,1]$ 上的临界点为 0，1，p^*，以及 ξ 在该区间内的任意根。我们声称 ξ 在区间 (0，1) 内没有其他根。直接计算 $k = 2, 4$ 的根即可验证这一点，因此不妨设 $k \geq 6$。

假设 $\xi(p) = 0$ 对某个 $p \in (0,1)$ 成立，并令 $x = \frac{1}{p} - 1 \in (0,\infty)$。于是 $p = \frac{1}{1+x}$；将其代入 p，并两边乘以 $(x+1)^3$，得到新的三次方程

$$(k^3-2k^2)x^3 + (k^3-6k^2+8)x^2 + (k^3-4k^2+12k-8)x + (k^3-8k^2+20k-16) = 0 \quad (7.32)$$

其系数是关于 k 的三次式。通过计算 方程 (7.32) 中 x 的各个系数的根，可以验证当 $k \geq 6$ 时所有系数均为正。因此，方程 (7.32)不可能有正 x 的根，这就产生了矛盾。因此，$\lambda_{\{k-1,k\}}(\mathcal{D}_N^*, \cdot)$ 在 p^* 处取得最大值。最后，可以验证 $\lambda_{\{k-1,k\}}(\mathcal{D}_N^*, p^*)\gamma_{\{k-1,k\},k}(\mu(\mathcal{D}_N^*)) = \frac{k}{2}\alpha'_{k-1}$，如所求。 □

引理 *7.29* 的证明。 定义 $p^* = \frac{1}{2} + \frac{1}{2}\frac{1}{(k-1)^{\alpha}}$ 按照 引理 7.24 的证明，并使用

下界 $\gamma_{\{k-1,k\},\,k}(\mu(\mathcal{D}_N)) \le \sum_{i=0}^{k} \binom{i}{k-1} \mathcal{D}_N\langle i\rangle$，只需证明

$$\frac{k}{2}\alpha'_{k-1} \le \inf_{\mathcal{D}_N\in\Delta_k} \frac{\sum_{i=0}^{k}(1-p^*)^{k-i-1}(p^*)^{i-1}((k-i)(p^*)^2+p^*(1-p^*)+i(1-p^*)^2)\,\mathcal{D}_N\langle i\rangle}{\sum_{i=0}^{k}\binom{i}{k-1}\mathcal{D}_N\langle i\rangle}$$

根据命题 7.18，接下来只需证明，对于每个 $i\in[k]\cup\{0\}$,

$$\frac{k}{2}\alpha'_{k-1}\frac{i}{k-1} \le (1-p^*)^{k-i-1}(p^*)^{i-1}((k-i)(p^*)^2+p^*(1-p^*)+i(1-p^*)^2).$$

我们再次注意到 $\alpha'_{k-1}=(1-p^*)^{k/2-1}(p^*)^{k/2-1}$，定义 $r=\frac{p^*}{1-p^*}=\frac{k}{k-2}$，并约去 $(1-p^*)^{k-1}$，从而将我们所需的不等式化简为

$$\frac{1}{2}r^{i-\frac{k}{2}-1}\cdot\frac{k-2}{k-1}\left(i+r+(k-i)r^2\right)\ge i. \tag{7.33}$$

对每个 $i\in[k]\cup\{0\}$。同样，我们不失一般性地假设 $k\ge 6$；基础情形 $i=k/2-1$，$k/2$ 可直接验证，接下来用归纳法证明。若方程 (7.33)对 i成立，且我们要证明它对 $i+1$成立，只需交叉相乘，并转而证明不等式

$$r(i+1+r+(k-(i+1))r^2)i \ge (i+1)(i+r+(k-i)r^2),$$

化简后得到

$$(k-2i)(k-1)(k^2-4i-4)\le 0,$$

当且仅当 $k/2\le i\le(k^2-4)/4$ (并且对于所有 $k\ge 6$，$(k^2-4)/4\ge k$) 时该式成立。另一方向（即 $i\le k/2-1$ 且向下归纳）类似。 □

观察 7.34. 对于 Th_4^3，最优的 $\mathcal{D}_N^*=(0,0,\frac{4}{5},\frac{1}{5},0)$确实与 $\mathcal{D}_Y^*=(\frac{4}{15},0,0,\frac{11}{15},0)$ 构成一个填充单向配对（由 $\mathcal{D}_0=(0,0,0,1,0)$、$\tau=\frac{1}{5}$、$\mathcal{D}'_N=(0,0,1,0,0)$ 和 $\mathcal{D}'_Y=(\frac{4}{15},0,0,\frac{8}{15},0)$ 给出），因此我们可以排除在 $o(\sqrt{n})$空间内对 $\overline{\text{Max-BCSP}}(Th_4^3)$ 进行流式计算 $(\frac{4}{9}+\epsilon)$-近似。

7.5.3 $f_{\{(k+1)/2\},k}$ FOR (SMALL) ODD k

在本小节中，我们证明奇数$k\in\{3,\dots,51\}$时$f_{\{(k+1)/2\},k}$ 的草图近似性界。定义$\mathcal{D}_{0,k}\in\Delta_k$ 为$\mathcal{D}_{0,k}\langle 0\rangle=\frac{k-1}{2k}$ 和$\mathcal{D}_{0,k}\langle k\rangle=\frac{k+1}{2k}$。我们证明 —— ——

以下两个引理:

引理 7.35. 对于所有奇数 $k \geq 3$, $\alpha(f_{\{(k+1)/2\},k}) \leq \lambda_{\{(k+1)/2\}}(\mathcal{D}_{0,k}, p'_k)$，其中 p'_k 定义为 $\frac{3k-k^2+\sqrt{4k+k^2-2k^3+k^4}}{4k}$。

引理 7.36. 对于所有奇数 $k \in \{3,\dots,51\}$，以下结论成立。对于所有 $p \in [0,1]$，表达式 $\lambda_{\{(k+1)/2\}}(\cdot,p)\,\gamma_{\{(k+1)/2\},k}(\mu(\cdot))$ 在 $\mathcal{D}_{0,k}$ 处取最小值。

我们首先写出 $\lambda_{\{(k+1)/2\}}$ 的显式公式。引理 7.21 给出

$$\lambda_{\{(k+1)/2\}}(\mathcal{D},p) = \sum_{i=0}^{k}\left(\sum_{j=\max\{0,i-(k-1)/2\}}^{\min\{i,(k+1)/2\}}\binom{i}{j}\binom{k}{(k+1)/2-j}(1-p)^{(k+1)/2+i-2j}p^{(k-1)/2-i+2j}\right)\mathcal{D}\langle i\rangle.$$

对于 $i \leq (k-1)/2$，对 j 的求和从 0 到 i；对于 $i \geq (k+1)/2$，则从$i-(k-1)/2$ 到 $(k+1)/2$。因此，代入 $\mathcal{D}_{0,k}$，得到:

$$\lambda_{\{(k+1)/2\}}(\mathcal{D}_{0,k},p) = \binom{k}{(k+1)/2}\left(\frac{k-1}{2k}(1-p)^{(k+1)/2}p^{(k-1)/2} + \frac{k+1}{2k}(1-p)^{(k-1)/2}p^{(k+1)/2}\right). \tag{7.37}$$

根据引理 7.12 和 7.22，$\gamma_{\{(k+1)/2\},k}(\mu(\mathcal{D}_{0,k})) = \gamma_{\{(k+1)/2\},k}(\frac{1}{k}) = 1$。因此，引理 7.35和 7.36 共同推出以下定理:

定理 7.38。对于奇数 $k \in \{3,\dots,51\}$,

$$\alpha(f_{\{(k+1)/2\},k}) = \binom{k}{(k+1)/2}\left(\frac{k-1}{2k}(1-p'_k)^{(k+1)/2}(p'_k)^{(k-1)/2} + \frac{k+1}{2k}(1-p'_k)^{(k-1)/2}(p'_k)^{(k+1)/2}\right),$$

其中 $p'_k = \frac{3k-k^2+\sqrt{4k+k^2-2k^3+k^4}}{4k}$如 引理 7.35所述。

回顾一下，$\rho(f_{(k+1)/2,k}) = \binom{k}{k+1\ ()/2}2^{-k}$。尽管目前我们尚未得到关于$\alpha(f_{\{(k+1)/2\},k})$对于较大的奇数 k的下界，但引理 7.35 给出的上界足以证明定理 7.6，也就是说，可以验证

$$\lim_{k\ \text{odd}\to\infty}\frac{\binom{k}{(k+1)/2}\left(\frac{k-1}{2k}(1-p'_k)^{(k+1)/2}(p'_k)^{(k-1)/2} + \frac{k+1}{2k}(1-p'_k)^{(k-1)/2}(p'_k)^{(k+1)/2}\right)}{\rho(f_{\{(k+1)/2\},k})} = 1.$$

我们指出，对于 $f_{\{(k+1)/2\},k}$，我们的下界（引理 7.36）比我们对 kAND (引理 7.24) 和Th_k^{k-1} (引理 7.29）所能证明的结果更强，因为无论 p为何，该不等式都成立。这对我们很有利，因为 p^* 引理 7.35 给出的最优值 相当复杂。† 接下来要证明引理 7.35和7.36。

引理 *7.35* 的证明引理 *7.35*。 对 p 求方程 (7.37)的导数

$$\frac{d}{dp}\left[\lambda_{\{(k+1)/2\}}(\mathcal{D}_{0,k},p)\right] = -\frac{1}{4k}\binom{k}{(k+1)/2}(pq)^{(k-3)/2}(4kp^2+(2k^2-6k)p+(-k^2+2k-1)),$$

其中 $q=1-p$。因此， $\lambda_{\{(k+1)/2\}}(\mathcal{D}_{0,\ k},\ \cdot)$ 的临界点为 $p=0$、1、p'_k，以及 $\frac{3k-k^2-\sqrt{4k+k^2-2k^3+k^4}}{4k}$。对于所有 $k\geq 0$，最后这个值均非正（因为 $(3k-k^2)^2-(4k+k^2-2k^3+k^4) = -4k(k-1)^2$）。 □

我们的下界证明（引理 7.36）与此前的下界证明（即引理 7.24 和引理 7.29）略有不同，具体如下。对于 $i\in[k]\cup\{0\}$，令 $\mathcal{D}_i\in\Delta_k$ 由 $\mathcal{D}_i\langle i\rangle = 1$定义。对于 kAND（引理 7.24），我们利用了这样一个事实： $\lambda_{\{k\}}(\cdot,p^*)\ \gamma_{\{k\},k}(\mu(\cdot))$ 是线性函数之比，因此根据命题 7.18，只需验证 $\mathcal{D}_0,\ldots,\mathcal{D}_k$ 处的下界。对于 Th_k^{k-1}（引理 7.29）， $\lambda_{\{k-1,k\}}(\cdot,p^*)\ \gamma_{\{k-1,k\},k}(\mu(\cdot))$ 不是线性函数之比，因为分母 $\gamma_{\{k-1,k\},k}(\mu(\mathcal{D})) = \min\{\sum_{i=0}^{k}\ {}_{k-1}^{\ i}\ \mathcal{D}\langle i\rangle, 1\}$ 在 Δ_k 上不是线性的。不过，我们通过用线性函数 $\gamma'(\mathcal{D}) = \sum_{i=0}^{k}\ {}_{k-1}^{\ i}\ \mathcal{D}\langle i\rangle$ 给分母取上界，再调用命题 7.18（同样是为了说明只需验证 $\mathcal{D}_0,\ldots,\mathcal{D}_k$ 处的下界），完成了证明。

对于 $f_{\{(k+1)/2\},\ k}$，我们证明只需在更大的（但仍然有限的）分布集合上验证下界。

引理 *7.36* 的证明。 回想 $\epsilon_{(k+1)/2,k} = \frac{1}{k}$，令 $\Delta_k^+ = \{\mathcal{D}\in\Delta_k\colon \mu(\mathcal{D})\leq\frac{1}{k}\}$ 和$\Delta_k^- = \{\mathcal{D}\in\Delta_k\colon \mu(\mathcal{D})\geq\frac{1}{k}\}$。注意到 $\Delta_k^+\cup\Delta_k^- = \Delta_k$，且限制在 Δ_k^+或 Δ_k^- 上时，$\gamma_{\{(k+1)/2\}\ k}\ \mu\cdot$. ,(( )) 是线性的，因此我们可以将 命题 7.18 应用于 $\lambda_{\{k-1,k\}}(\cdot,p^*)\gamma_{\{k-1,k\},k}(\mu())$。

†例如，对于 3AND，类似的陈述并不成立；我们得到的是 $\mathcal{D}_N^* = (0,\ 0,\ 1,\ 0)$，但在 $p=\frac{3}{4}$，

$$\frac{\lambda_{\{3\}}((0,\frac{1}{2},\frac{1}{2},0),\frac{3}{4})}{\gamma_{\{3\},3}(\mu(0,\frac{1}{2},\frac{1}{2},0))} = \frac{3}{16} \leq \frac{27}{128} = \frac{\lambda_{\{3\}}((0,0,1,0),\frac{3}{4})}{\gamma_{\{3\},3}(\mu(0,0,1,0))}.$$

令 $\mathcal{D}_{i,j} \in \Delta_k$，对于 $i < (k+1)/2, j > (k+1)/2$，定义为 $\mathcal{D}_{i,j}\langle i\rangle = \frac{2j-}{2}(k+1)(j-i)$ 和 $\mathcal{D}_{i,j}\langle j\rangle = \frac{-2i}{(k+1)2}(j-i)$。注意，对每个 i,j，$\mu(\mathcal{D}_{i,j}) = \frac{1}{k}$。我们声称 $\{\mathcal{D}_i\}_{i\le(k+1)/2} \cup \{\mathcal{D}_{i,j}\}$ 是 Δ_k^+ 的极点，更准确地说，每个分布 $\mathcal{D} \in \Delta_k^+$ 都可以表示为这些分布的凸组合。事实上，这可以通过以下过程构造性地得到：给定一个分布 $\mathcal{D}$，对于每个 $\mathcal{D}\langle i\rangle$，当 $i < (k+1)/2$ 时，从中减去相应的量（并加到对应的 $\mathcal{D}_i$ 的系数上），直到（重新归一化后的）分布的边缘分布为 $\frac{1}{k}$；然后从满足 $i < (k+1)/2$且 $j > (k+1)/2$ 的成对 $\mathcal{D}\langle i\rangle, \mathcal{D}\langle j\rangle$ 中减去相应的量，并将其加到适当的 $\mathcal{D}_{i,j}$ 的系数上，直到 $\mathcal{D}$ 消失（即，对所有 $i \in [k] \cup \{0\}$，$\mathcal{D}\langle i\rangle$ 为零）。类似地，每个分布 $\mathcal{D} \in \Delta_k^-$ 都可以表示为分布 $\{\mathcal{D}_i\}_{i\ge(k+1)/2} \cup \{\mathcal{D}_{i,j}\}$的凸组合。因此，根据命题 7.18，只需验证

$$\frac{\lambda_{\{(k+1)/2\}}(\mathcal{D}, p)}{\gamma_{\{(k+1)/2\},k}(\mu(\mathcal{D}))} \ge \frac{\lambda_{\{(k+1)/2\}}(\mathcal{D}_N^*, p)}{\gamma_{\{(k+1)/2\},k}(\mu(\mathcal{D}_N^*))}$$

对每个 $\mathcal{D} \in \{\mathcal{D}_i\} \cup \{\mathcal{D}_{i,j}\}$。将 p 视为变量，对于每个奇数 $k \in \{3, \ldots, 51\}$，我们生成一组 $O(k^2)$ 次多项式不等式，涉及 p，并使用 Mathematica 对其进行验证。

□

7.5.4 Other symmetric predicates

在下方的 表 7.1 中，我们列出了另外四个对称布尔谓词（除 kAND、Th_k^{k-1} 和 $f_{\{(k+1)/2\},k}$ 外），其草图近似性已通过“极大极小方法”在解析上得到确定。这些值是通过 Mathematica 代码中的两个子程序计算得出的：`estimateAlpha` ——它针对给定的支撑集，对使 α 最小的情形进行数值或符号估计；以及 `testMinMax` ——它根据特定的 $\mathcal{D}_N$ 计算该 $\mathcal{D}_N$ 的 p^*，并通过在 p^* 处计算 λ_S，以解析方式检验下界是否足以证明 $\mathcal{D}_N$ 是最小值。

我们指出，表 7.1 中的两个情形（以及 kAND），最优 $\mathcal{D}_N$ 是有理数，且支撑集位于两个坐标上。然而，在表 7.1中的另外两个情形里，最优 $\mathcal{D}_N$ 涉及三次方程的根。

在§7.5.3中，我们证明了由 $\mathcal{D}_N^*\langle 0\rangle = \frac{k-1}{2k}$ 和 $\mathcal{D}_N^*\langle k\rangle = \frac{k+1}{2k}$ 定义的 $\mathcal{D}_N^*$ 对于$f_{\{(k+1)/2\},k}$ 在 $k \in \{3, \ldots, 51\}$为奇数时是最优的。利用相同的 $\mathcal{D}_N^*$，我们还能够解决 11

S	k	α	$\mathcal{D}_N^*$
$\{2,3\}$	3	$\frac{1}{2}+\frac{\sqrt{3}}{18}\approx 0.5962$	$(0, \frac{1}{2}, 0, \frac{1}{2})$
$\{4,5\}$	5	8根$_{\mathbb{R}}(P_1)\approx 0.2831$	$(0, 0, 1-\text{root}_{\mathbb{R}}(P_2), \text{root}_{\mathbb{R}}(P_2), 0, 0)$
$\{4\}$	5	8$\text{root}_{\mathbb{R}}(P_3)\approx 0.2394$	$(0, 0, 1-\text{root}_{\mathbb{R}}(P_4), \text{root}_{\mathbb{R}}(P_4), 0, 0)$
$\{3,4,5\}$	5	$\frac{1}{2}+\frac{3\sqrt{5}}{125}\approx 0.5537$	$(0, \frac{1}{2}, 0, 0, \frac{1}{2}, 0)$

表 7.1： 使用"极大极小方法"解析计算出精确 α 值的对称谓词。对于具有唯一正实根的多项式 P： $\mathbb{R}\to\mathbb{R}$，令 $\text{root}_{\mathbb{R}}(p)$ 表示该根，并定义多项式 $P_1(z)=-72+4890z-108999z^2+800000z^3$， $P_2(z)=-908+5021z-9001z^2+5158z^3$，$P_3(z)=-60+5745z-183426z^2+1953125z^3$ $P_4(z)=-344+1770z-3102z^2+1811z^3$ ( ) , ( ) 。(值得注意的是，在 $f_{\{4\},5}$ 和 $f_{\{4,5\},5}$ 的计算中，我们必须以数值方式（高精度）而非解析方式检验根的相等性)。

其他情形，其中 S"接近于" $\{(k+1)/2\}$；例如， $S=\{5,6\}$， $\{5,6,7\}$， $\{5,7\}$ 对于 $k=9$。（我们省略了 α 和 $\mathcal{D}_N$ 的值，因为它们是利用次数最高为 8 的多项式的根定义的。）

在前面提到的所有情形中，"$\mathcal{D}_N^*$ 的支撑大小为 2"这一条件很有帮助，因为它使关于 $\mathcal{D}_N^*$ 的优化问题实质上变成单变量问题；然而，我们通过分析确认，在另外两种情形（ $S=\{3\}$， $k=4$ 和 $S=\{3,5\}$， $k=5$）中，"对支撑大小为 2 的分布使用极大极小方法"不足以得到 α的紧确界（参见 Mathematica 代码中的 `testDistsWithSupportSize2` ）。不过，对支撑于两个层级的 $\mathcal{D}_N$ 使用极大极小方法，仍能得到关于 α的较好（但不紧确）界。对于 $S=\{3\}$， $k=4$，使用 $\mathcal{D}_N=(\frac{1}{4},0,0,0,\frac{3}{4})$，我们得到界 $\alpha(f_{\{3\},4})\in[0.3209,0.3295]$（差值为 2。67%）。对于 $S=\{3,5\}$， $k=5$，使用 $\mathcal{D}_N=(\frac{1}{4},0,0,0,\frac{3}{4},0)$，我们得到 $\alpha(f_{\{3,5\},5})\in[0.3416,0.3635]$ （差值为 6。42%）。

最后，我们还分析了这样一些情形：数值解非常接近紧确界，但由于它们很可能涉及高次数多项式的根，我们无法得到解析解。例如，在情形 $S=\{4,5,6\},k=6$ 中，令 $\mathcal{D}_N=(0,0,0,0.930013,0,0,0.0699$ 给出 $\alpha(f_{\{4,5,6\},6})\in[0.44409972,0.44409973]$，仅相差 0.000003%。（我们在此猜想 $\alpha=\frac{4}{9}$。）对于 $S=\{6,7,8\}$， $k=8$，使用 $\mathcal{D}_N=(0,\ 0,\ 0,\ 0,\ 0.699501,\ 0.300499)$，我们得到界 $\alpha(f_{\{6,7,8\},8})\in[0.20848,0.20854]$ （差值为 0.02%）。‡

‡有趣的是，在后一种情形下，尝试沿用 $f_{\{7,8\}}$,8 和 $f_{\{8\}}$,8 的模式时，使用 $\mathcal{D}_N=(0, 0, 0, 0, 9\ 13, 4\ 13, 0, 0, 0)$ 得到的上下界相差 2.12%（其中在 §7.5.2 和 §7.5.1 中，我们分别令 $\mathcal{D}_N^*=(0, 0, 0, 0, 16\ 25, 9\ 25, 0, 0, 0)$ 和 $(0, 0, 0, 0, 25\ 41, 16\ 41, 0, 0, 0)$）。

设 $f_{S,k} = \mathrm{Th}_k^t$ 为一个阈值谓词（因此 $S = \{t, \dots, k\}$）。本节的主要目标是证明定理 7.7，该定理给出了一种用于 Max-BCSP(Th_k^t) 的简单的基于"偏差"的草图算法。按照 §4.1 中对 Max-2AND 实例中变量偏差的定义，给定一个 Max-BCSP(Th_k^t) 的实例 Ψ，对于 $i \in [n]$，令 $\mathrm{bias}_\Psi(i)$ 表示变量 x_i 正向出现的子句的总权重减去其负向出现的子句的总权重；也就是说，如果 Ψ 由子句 $(\mathbf{b}(\ell), \mathbf{j}(\ell)\ w(\ell))^{\ell \in [m]}$ 组成，那么

$$\mathrm{bias}_\Psi(i) \stackrel{\text{def}}{=} \sum_{\ell \in [m]:\ j(\ell)_t = i} (-1)^{b(\ell)_t} w_\ell,$$

和偏差$_\Psi$ $\stackrel{\text{定义}}{=} \frac{1}{kW_\Psi} \sum_{i=1}^n |$偏差$_\Psi(i)|$。偏差$_\Psi$ 可通过 1-范数草图算法进行测量（即 定理 2.2 由 [Ind06; KNW10],亦用于 [GVV17; CGV20; CGSV21a]）：

推论 7.39。对于每个谓词 $f: \mathbb{Z}_2^k \to \{0,1\}$ 以及每个 $\epsilon > 0$，都存在一个$O(\log n/\epsilon^2)$-空间随机化草图算法，用于解决以下问题：输入为 *Max-BCSP* 的一个实例 Ψ (Th_k^t)（以约束数据流的形式给出），目标是将偏差$_\Psi$ 估计到不超过 $1 \pm \epsilon$的乘法因子范围内。

证明。按如下方式调用 定理 2.2中的 1-范数草图算法：对于每个输入约束 $(\mathbf{b}, \mathbf{j}\ \ell)$，其权重为 w，将更新 $(j_1, wb_1) \dots, (j_k, wb_k)$ 插入数据流中（并进行适当归一化）。

□

现在回顾$\beta_{S,k}(\mu)$ 和 $\gamma_{S,k}(\mu)$ 在 方程 (7.15)中的定义。我们的简单算法最大布尔约束满足问题(Th_k^t 依赖于以下两个引理，我们将在下文证明它们：

引理 7.40。$val_\Psi \le \gamma_{S,k}($偏差$_\Psi)$。

引理 7.41。$val_\Psi \ge \beta_{S,k}($偏差$_\Psi)$。

总之，这两个引理意味着，输出 $\alpha(\mathrm{Th}_k^t) \cdot \gamma_{S,k}($偏差$_\Psi)$ 可得到 Max-BCSP(Th_k^t) 的 $\alpha(\mathrm{Th}_k^t)$-近似，因为 $\alpha(\mathrm{Th}_k^t) = \inf_{\mu \in [-1,1]} \beta_{S,k}(\mu)\ \gamma_{S,k}(\mu)$（方程 (7.15)）。我们可以将其实现为一个小空间草图算法（在近似比中损失任意小的加性常数 $\epsilon > 0$），因为根据引理 7.22，$\gamma_{S,k}(\cdot)$ 是分段线性的：

定理 7.7 的证明。为了获得 val_Ψ 的 $(\alpha-\epsilon)$-近似，令 $\delta>0$ 足够小，使得 $\frac{1-\delta}{1+\delta}\alpha(\mathsf{Th}_k^t) \geq \alpha(\mathsf{Th}_k^t) - \epsilon$。我们声称，将偏差$_\Psi$（使用推论 7.39）估计到乘法 δ 因子以内，并输出 $\widehat{v} = \alpha(\mathsf{Th}_k^t)\gamma_{S,k}(\frac{b}{1+\delta})$，就足够了。注意，根据引理 7.22，$\gamma_{S,k}$ 是单调的，因为 Th_k^t 是阈值函数。

事实上，假设 $\widehat{b} \in [(1-\delta)\text{偏差}_\Psi, (1+\delta)\text{偏差}_\Psi]$；那么 $\frac{\widehat{b}}{1+\delta} \in [\frac{1-\delta}{1+\delta}\text{偏差}_\Psi, \text{偏差}_\Psi]$。现在我们观察到

$$\begin{aligned}
\gamma_{S,k}\left(\frac{\widehat{b}}{1+\delta}\right) &\geq \gamma_{S,k}\left(\frac{1-\delta}{1+\delta}\mathsf{bias}_\Psi\right) && \text{(monotonicity of } \gamma_{S,k}) \\
&= \min\left\{\frac{1+\frac{1-\delta}{1+\delta}\mathsf{bias}_\Psi}{1+\epsilon_{s,k}}, 1\right\} && \text{(Lemma 7.22)} \\
&\geq \frac{1-\delta}{1+\delta}\min\left\{\frac{1+\mathsf{bias}_\Psi}{1+\epsilon_{s,k}}, 1\right\} && (\delta>0) \\
&= \frac{1-\delta}{1+\delta}\gamma_{S,k}(\mathsf{bias}_\Psi). && \text{(Lemma 7.22)}
\end{aligned}$$

由此我们得出

$$\begin{aligned}
(\alpha(\mathsf{Th}_k^t)-\epsilon)\mathsf{val}_\Psi &\leq (\alpha(\mathsf{Th}_k^t)-\epsilon)\gamma_{S,k}(\mathsf{bias}_\Psi) && \text{(Lemma 7.40)} \\
&\leq \alpha(\mathsf{Th}_k^t)\cdot\frac{1-\delta}{1+\delta}\gamma_{S,k}(\mathsf{bias}_\Psi) && \text{(assumption on } \delta) \\
&\leq \widehat{v} && \text{(our observation)} \\
&\leq \alpha(\mathsf{Th}_k^t)\gamma_{S,k}(\mathsf{bias}_\Psi) && \text{(monotonicity of } \gamma_{S,k}) \\
&\leq \beta_{S,k}(\mathsf{bias}_\Psi) && \text{(Eq. (7.15))} \\
&\leq \mathsf{val}_\Psi, && \text{(Lemma 7.41)}
\end{aligned}$$

如所需。 □

7.6.1 Proving the lemmas

为证明引理 7.40 和7.41，我们将Max-2AND 的模板分布定义从§4.1.2 推广到所有 Max-BCSP(f) 问题。对于谓词 $f\colon \overline{\mathbb{Z}}_2^k \to \{0,1\}$、一个定义在 Ψ 个Max-BCSP(f) 实例（包含 n 个变量），以及一个赋值$\mathbf{x} \in \mathbb{Z}_2^n$，令 $\mathcal{D}_\Psi^{\mathbf{x}} \in \Delta(\mathbb{Z}_2^k)$

表示以下模板分布：若 Ψ 的约束为 $(\mathbf{b}(\ell),\mathbf{j}(\ell)\ w(\ell))^{\ell\in[m]}$，我们以概率 $^{w_{(\ell)}}/_{W_\Psi}$ 对 ℓ 进行采样，并输出 $\mathbf{b}(\ell)\ +\mathbf{x}|_{\mathbf{j}(\ell)}$。也就是说，$\mathcal{D}^{\mathbf{x}}_{\Psi}(\mathbf{a})$ 是满足以下条件的约束 ℓ 的分数权重：代入赋值 $\mathbf{x}$，并按照$\mathbf{b}(\ell)$ 取反后，结果为$\mathbf{a}$。注意，$\mathcal{D}^{\mathbf{x}}_{\Psi}$ 不一定是对称的；不过，我们仍可以定义标量“边缘分布” $\mu_S(\mathcal{D}) \overset{\text{def}}{=} \mu(\mathrm{Sym}(\mathcal{D}))$。$\mathcal{D}^{\mathbf{x}}_{\Psi}$ 的重要性质总结如下命题所示：

命题 7.42。设 Ψ 是最大布尔约束满足问题(Th^t_k)的一个实例。则：

i. 对于任意 $p\in[0,1]$ 和 $x\in\mathbb{Z}_2^n$，$\mathbb{E}_{\mathbf{a}\sim\mathcal{B}_p^n}[val_\Psi(a+x)]=\lambda_S(\mathcal{D}^{\mathbf{x}}_{\Psi},p)$。 *ii.* 对于每个 $x\in\mathbb{Z}_2^n$，$\mu_S(\mathcal{D}^{\mathbf{x}}_{\Psi})=\frac{1}{kW_\Psi}\sum_{i=1}^n(-1)^{x_i+1}$偏差$_\Psi(i)\le$ 偏差$_\Psi$。 *iii.* 如果对于每个 i，偏差$_\Psi(i)>0\implies x_i=1$ 且偏差$_\Psi(i)<0\implies x_i=0$，则 $\mu_S(\mathcal{D}^{\mathbf{x}}_{\Psi})=$偏差$_\Psi$。

证明。Omitted（由定义和期望的线性性直接得出）。 □

现在，我们已经具备证明这些引理的条件：

Proof 的 引理 7.40. 令 $\mathbf{x}\in\mathbb{Z}_2^n$ 表示 Ψ的最优赋值。则

$$\begin{aligned}
\mathsf{val}_\Psi &= \mathsf{val}_\Psi(\mathbf{x}) && \text{(def. of } \mathbf{x})\\
&= \lambda_S(\mathcal{D}^{\mathbf{x}}_{\Psi},1) && \text{(第 i 项的命题 7.42与 } p=1)\\
&= \gamma_S(\mathcal{D}^{\mathbf{x}}_{\Psi}) && \text{(Eq. (5.1))}\\
&\le \gamma_{S,k}(\mu_{\mathsf{S}}(\mathcal{D}^{\mathbf{x}}_{\Psi})) && \text{(Eq. (7.14) and Proposition 7.10)}\\
&\le \gamma_{S,k}(\mathsf{bias}(\Psi)) && \text{(第 ii 项的命题 7.42以及 } \gamma_S \text{ 的单调性, } k)
\end{aligned}$$

如所愿。 □

引理 *7.41* 的证明。令$\mathbf{x}\in\mathbb{Z}_2^n$ 表示如下赋值：x_i 当 偏差$_\Psi(i)\ge 0$ 时赋值为 1，否则赋值为 0。现在

$$\mathsf{val}_\Psi \ge \sup_{p\in[0,1]}\left(\mathop{\mathbb{E}}_{\mathbf{a}\sim\mathcal{B}_p^n}[\mathsf{val}_\Psi(\mathbf{a}+\mathbf{x})]\right) \qquad \text{(概率方法)}$$

$$
\begin{aligned}
&= \sup_{p\in[0,1]} \left(\lambda_S(\mathcal{D}_\Psi^{\mathbf{x}}, p)\right) && \text{(Item i of Proposition 7.42)}\\
&\geq \beta_S(\mathcal{D}_\Psi^{\mathbf{x}}) && \text{(Eq. (5.1))}\\
&\geq \beta_{S,k}(\mu_{\mathsf{S}}(\mathcal{D}_\Psi^{\mathbf{x}})) && \text{(Eq. (7.14) and Proposition 7.10)}\\
&= \beta_{S,k}(\mathsf{bias}(\Psi)) && \text{(Item iii of Proposition 7.42)}
\end{aligned}
$$

如所需。 □

7.6.2 The classical algorithm

最后，我们陈述 引理 7.40 的另一个推论——一种简单的随机化、 $O(n$时间和空间流式算法，用于输出近似最优赋值，适用于极大极小方法成立的情形。

定理 7.43。 设 Th_k^t 是一个阈值谓词，且 $p^* \in [0,1]$ 满足极大极小方法成立，即

$$
\alpha(Th_k^t) = \inf_{\mathcal{D}_N \in \Delta_k} \left(\frac{\lambda_S(\mathcal{D}_N, p^*)}{\gamma_{S,k}(\mu(\mathcal{D}_N))} \right).
$$

那么，对于输入 Ψ，以下算法输出的赋值的期望值至少为 $\alpha(Th_k^t) \cdot val_\Psi$：若 $bias_\Psi(i) \geq 0$，则将每个变量赋值为1；否则赋值为0；随后以概率 p^* 独立翻转每个变量的赋值。

定理 *7.43* 的证明。设 p^* 如定理陈述所述，并按$\mathbf{x}$ 的证明中所述定义引理 7.41。我们输出赋值$\mathbf{x} + \mathbf{a}$，对$\mathbf{a} \sim \mathcal{B}_{p^*}^n$，目标是证明其期望值至少为 $\alpha(\mathsf{Th}_k^t)\mathsf{val}_\Psi$。

将极大极小方法应用于 $\mathsf{Sym}(\mathcal{D}_\Psi^{\mathbf{x}})$，并利用命题 7.10，我们得到：

$$
\lambda_S(\mathcal{D}_\Psi^{\mathbf{x}}, p^*) \geq \alpha(\mathsf{Th}_k^t)\gamma_{S,k}(\mu_{\mathsf{S}}(\mathcal{D}_\Psi^{\mathbf{x}})). \tag{7.44}
$$

因此，我们预期的输出值为

$$
\begin{aligned}
\mathop{\mathbb{E}}_{\mathbf{a}\sim\mathcal{B}_{p^*}} [\mathsf{val}_\Psi(\mathbf{x}+\mathbf{a})] &= \lambda_S(\mathcal{D}_\Psi^{\mathbf{x}}, p^*) && \text{(Item i of Proposition 7.42)}\\
&\geq \alpha(\mathsf{Th}_k^t)\gamma_{S,k}(\mu_{\mathsf{S}}(\mathcal{D}_\Psi^{\mathbf{x}})) && \text{(Eq. (7.44))}\\
&= \alpha(\mathsf{Th}_k^t)\gamma_{S,k}(\mathsf{bias}_\Psi) && \text{(Item iii of Proposition 7.42)}
\end{aligned}
$$

$$\geq \alpha(\mathsf{Th}_k^t)\mathsf{val}_\Psi, \qquad \text{(Lemma 7.40)}$$

如所愿。 □

7.7 [CGSV21A] is incomplete: Streaming lower bounds for Max-3AND?

在本节中，我们证明 定理 7.19。我们先给出几个引理。

引理 7.45。 对于 $\mathcal{D} \in \Delta_3$，表达式

$$\frac{\lambda_{\{3\}}(\mathcal{D}, \frac{1}{3}\mathcal{D}\langle 1\rangle + \frac{2}{3}\langle 2\rangle + \mathcal{D}\langle 3\rangle)}{\gamma_{\{3\},3}(\mu(\mathcal{D}))}$$

唯一地在 $\mathcal{D} = (0,\ 0,\ 1,\ 0)$ 处取得最小值，其值为 $2\,9$。

证明。 令 $p = \frac{1}{3}\mathcal{D}\langle 1\rangle + \frac{2}{3}\mathcal{D}\langle 2\rangle + \mathcal{D}\langle 3\rangle$ 且 $q = 1 - p$，由 引理 7.12、7.21和 7.22可将该表达式展开为

$$\frac{\mathcal{D}\langle 0\rangle\, p^3 + \mathcal{D}\langle 1\rangle\, p^2(1-p) + \mathcal{D}\langle 3\rangle\, p(1-p)^2 + \mathcal{D}\langle 3\rangle\, (1-p)^3}{\frac{1}{2}(1 - \mathcal{D}\langle 0\rangle - \frac{1}{3}\mathcal{D}\langle 1\rangle + \frac{1}{3}\mathcal{D}\langle 2\rangle + \mathcal{D}\langle 3\rangle)}.$$

该表达式的最小值及其唯一性已在 Mathematica 代码中通过解析方法得到验证。

□

引理 7.46。 设 X 是一个紧致拓扑空间，$Y \subseteq X$ 是一个闭子空间，Z 是一个拓扑空间，且 $f\colon\ X \to Z$ 是一个连续映射。设 $x^* \in X$、$z^* \in Z$ 满足 $f^{-1}(z^*) = \{x^*\}$。设 $\{x_i\}_{i\in\mathbb{N}}$ 是 Y 中的点序列，且 $\{f(x_i)\}_{i\in\mathbb{N}}$ 收敛到 z^*。那么 $x^* \in Y$。

证明。 由 X的紧致性，存在一个子序列 $\{x_{j_i}\}_{i\in\mathbb{N}}$，它收敛到极限 $\widetilde{x}$。由闭包，$\widetilde{x} \in Y$。由连续性，$f(\widetilde{x}) = z^*$，因此 $\widetilde{x} = x^*$。 □

最后，我们有：

定理 7.19 的证明。由引理 7.45，$\beta_{\{3\}}(\mathcal{D}_N)\ \gamma_{\{3\}},3(\mu(\mathcal{D}_N))$ 在 $\mathcal{D}_N^* = (0, 0, 1, 0)$ 处取得唯一最小值。由引理 7.12 可得 $\mu(\mathcal{D}_N^*) = \frac{1}{3}$；并且从下文引理 7.22 的证明中可直接看出，$\gamma_{\{3\}}(\mathcal{D}_Y)$ 满足 $\mu(\mathcal{D}_Y) = \frac{1}{3}$时，其唯一最小值由 $\mathcal{D}_Y^* = (\frac{1}{3}, 0, 0, \frac{2}{3})$ 取得。 – –

最后，我们利用拓扑性质排除存在无限序列的填充单边对、使其比率任意接近$_{2\ 9}$的可能性。将分布 $\mathcal{D} \in \Delta_3$ 视为向量 $(\mathcal{D}\langle\theta\rangle, \mathcal{D}\langle 1\rangle, \mathcal{D}\langle 2\rangle, \mathcal{D}\langle 3\rangle) \in \mathbb{R}^4$。令 $D \subset \mathbb{R}^4$ 表示这类分布的集合。令 $M \subset D \times D \subset \mathbb{R}^8$ 表示边缘分布匹配的分布对所构成的子集，令 $M' \subset M$ 表示具有均匀边缘分布的分布对所构成的子集，而 $P \subset M$ 表示填充单边对的子集。 D、 M、 M'和 P 都是紧致的（相对于欧几里得拓扑）；事实上， D、 M和 M'有界，且由有限个线性等式和严格不等式定义；再令 $M' \subset M$ 表示边缘分布为均匀分布的分布对所构成的子集，则 P 是紧致集合 $[0,1] \times D \times M' \subset \mathbb{R}^{13}$ 在连续映射 $\tau \times \mathcal{D}_0 \times (\mathcal{D}'_Y, \mathcal{D}'_N) \mapsto (\tau\mathcal{D}_0 + (1-\tau)\mathcal{D}'_Y, \tau\mathcal{D}_0 + (1-\tau)\mathcal{D}'_N)$ 下的像。因此， P是闭集。

现在，函数

$$\alpha : M \to \mathbb{R} \cup \{\infty\} : (\mathcal{D}_N, \mathcal{D}_Y) \mapsto \frac{\beta_{\{3\}}(\mathcal{D}_N)}{\gamma_{\{3\}}(\mathcal{D}_Y)}$$

是连续的，因为连续函数之比仍然连续，而 $\beta_{\{3\}}$ 是连续函数在紧区间上的单变量上确界（即 λ_S），通常在其余变量上连续。因此，若存在一列填充单向配对 $\{(\mathcal{D}_N^{(i)}, \mathcal{D}_Y^{(i)}) \in P\}_{i\in\mathbb{N}}$使得 $\alpha(\mathcal{D}_N^{(i)}, \mathcal{D}_Y^{(i)})$ 收敛到$_{2\ 9}$当 $i \to \infty$时，由于M是紧致的且 P是闭的，引理 7.45 和 7.46 推出 $(\mathcal{D}_N^*, \mathcal{D}_Y^*) \in P$，矛盾。 –

□

8

结论与未来方向

Open directions for further progress abound以期理解流式设置下约束满足问题的可近似性。在本章中，我们汇总了若干此类问题。

8.1 Unique games-hardness vs. streaming hardness

我们首先具体阐述一个由 Chou 等人 [CGSV21a],提出的问题：

> “[我们的知识中] 存在一些奇怪的空白。例如，人们自然会猜想，（有条件的）多项式时间设置下的不可近似性，也应当会导致流式设置下的（无条件）不可近似性。但我们没有正式的定理来证明这一点。”

也就是说，问题如下：如果 (β, γ)-最大约束满足问题$(\mathcal{F})$ 根据 Raghavendra 的二分定理 [Rag08], 在经典意义下是 UG 困难的，那么它是否也必然难以由 $\sqrt{n}$-空间流式算法解决?¯一个有趣的特殊情形是，Raghavendra 的二分定理 [Rag08] 表明最大约束满足问题$(\mathcal{F})$ 具有近似抗性(在

唯一博弈猜想下）。它是否也必然具有流式近似抗性，符合 [CGSV21a;CGSV21b]的结论？具体而言， [CGSV21a] 研究了 Potechin [Pot19] 构造的一个平衡线性阈值谓词 f_{Pot} : $\mathbb{Z}_2^k \to \{0,1\}$ 使得最大布尔约束满足问题(f_{Pot}) 根据 [Rag08]是 UG 近似抗性的；他们指出，由于 f_{Pot} 是平衡线性阈值函数，因此无法支持单变量独立性（参见例 5.6），所以需要新的工具来证明最大布尔约束满足问题(f_{Pot}) 的流式近似抗性。

这里，我们给出这个开放问题的一个显式表述。对于一个分布 $\mathcal{D} \in \Delta(\mathbb{Z}_2^k)$，令 $\boldsymbol{\mu}^{(2)}(\mathcal{D}) \in [-1,1]^{k\times k}$ 表示 $\mathcal{D}$的二阶边缘分布矩阵，该对称矩阵的元素为 $\mu^{(2)}(\mathcal{D})_{i,\,j} = \mathbb{E}_{\mathbf{b}\sim\mathcal{D}}[(-1)^{b_i+b_j}]$ 其中 $i,\ j \in [k]$。现在 [Pot19]以如下方式表述了 [Rag08] 的近似抗性判据：

定义 8.1。布尔谓词 $f\colon \mathbb{Z}_2^k \to \{0,1\}$ 支持一个标准半定规划的完美整数间隙实例，如果存在 $\mathcal{D}_N \in \Delta(\mathbb{Z}_2^k)$ 和 $\mathcal{D}_{Y,\,\mathbf{b}} \in \Delta(\mathbb{Z}_2^k)$ 对每个$\mathbf{b} \in \mathit{supp}(\mathcal{D}_N)$ 都满足：

i. 对所有 $\mathbf{a} \in \mathbb{Z}_2^k$，$\mathit{val}_{\Psi(\mathcal{D}_N)}(\mathbf{a}) = \rho(f)$。

ii. 对所有 $\mathbf{b} \in \mathit{supp}(\mathcal{D}_N)$，$\mathit{val}_{\Psi(\mathcal{D}_{Y,\mathbf{b}})}(\mathbf{b}) = 1$。

iii. 对所有 $\mathbf{b}$、$\mathbf{b}' \in \mathit{supp}(\mathcal{D}_N)$，$\boldsymbol{\mu}(\mathcal{D}_{Y,\mathbf{b}}) = \boldsymbol{\mu}(\mathcal{D}_{Y,\mathbf{b}'})$ 以及 $\boldsymbol{\mu}^{(2)}(\mathcal{D}_{Y,\mathbf{b}}) = \boldsymbol{\mu}^{(2)}(\mathcal{D}_{Y,\mathbf{b}'})$。

与 [CGSV21a] 流式计算的二分定理（定理 5.2）相比，注意到 定义 8.1 中的第 i 项 is 更强 于条件 $\beta_f(\mathcal{D}_N) = \rho(f)$，因为$\Psi(\mathcal{D}_N)$ 的值在每一个赋值下都有界，而不只是随机对称赋值。另一方面，不存在单一的 **是** 分布 $\mathcal{D}_Y$；相反，我们有一个集合，其中包含**是**分布，它们具有相同的一阶边缘分布和二阶边缘分布。

例 *8.2. Guruswami*、*Levin*、*Sudan* 和 *Trevisan* *[GLST98]* 研究了谓词f_{GLST}：$\mathbb{Z}_2^4 \to \{0,1\}$，其定义为 $f_{\mathrm{GLST}}(b_1,b_2,b_3,b_4) = 1 + b_2 + b_1b_3 + (1-b_1)b_4$。正如 *Potechin* *[Pot19]* 所指出的，f_{GLST} 支持一个完美整数间隙实例。事实上，取$\mathcal{D}_N = \mathcal{U}_{\{(0,0,0,0),(0,1,0,0)\}}$, $\mathcal{D}_{Y,(0,0,0,0)} = \mathcal{U}_{\{(0,0,0,1),(0,1,1,0),(1,0,1,0),(1,1,0,1)\}}$，以及 $\mathcal{D}_{Y,(0,1,0,0)} = \mathcal{U}_{\{(1,0,0,1),(0,1,0,1),(0,0,1,0),(1,1,1,0)\}}$；特别是，$\boldsymbol{\mu}(\mathcal{D}_{Y,(0,0,0,0)}) = \boldsymbol{\mu}(\mathcal{D}_{Y,(0,1,0,0)}) = \mathbf{0}$ 和 $\boldsymbol{\mu}^{(2)}(\mathcal{D}_{Y,(0,0,0,0)})$ 以及 $\boldsymbol{\mu}^{(2)}(\mathcal{D}_{Y,(0,1,0,0)})$ 除 *(3, 4)/(4, 3)* 位置上的元素外都恒为零，这些元素为-1。我们注意到，f_{GLST} 也支持单变量独立性，例如，它支持单变量独立的 $\mathcal{D} = \mathcal{U}_{\{(0,1,0,0),(1,0,1,1)\}}$。

开放问题 1. 证明：如果 $f\colon \mathbb{Z}_2^k \to \{0,1\}$ 支持标准半定规划的一个完美整数间隙实例，那么 *Max-BCSP*(f) 在 $\sqrt{n}$空间内具有流式近似抗性；也就是说，对于每个 $\epsilon > 0$，任何以$(\rho(f) + \epsilon)$近似比近似 *Max-BCSP*(f) 的流式算法，至少需要$\Omega(\sqrt{n})$ 空间。

关于开放问题 1 的一个有趣之处在于，f 的完美整数性间隙假设似乎并未指明应使用哪种特定的**是** 分布来证明流式下界。

8.2 Random-ordering and linear-space streaming

回顾我们在§3.4 中的讨论：[KKS15] 和 [KK19] 分别证明了针对 $\sqrt{n}$空间的数据流随机排序下界和线性空间对抗顺序下界，所针对的问题是最大割。如§5.2, [CGS+22] 随后将线性空间下界推广到了所谓的“宽”谓词族。然而，据我们所知，并无证据表明这两个下界不能推广到所有符合以下条件的谓词族：它们是 $\sqrt{n}$空间、对抗顺序下具有流式近似抗性的，而这符合 [CGSV21b], 的定义；也就是说，所有“弱支撑单变量独立性”的谓词族（见上文 §5.1.2 末尾）。沿着这一方向，一个雄心勃勃的目标是证明针对能够同时使用线性空间和随机输入顺序的算法的下界：

开放问题 2。 证明：如果 $\mathcal{F}$ 是一个弱支撑单变量独立性的谓词族，那么对于任意 $\epsilon > 0$，使用随机顺序流式算法对最大约束满足问题$(\mathcal{F})$ 进行$(\rho(\mathcal{F}) + \epsilon)$近似需要$\Omega(n)$ 空间。

我们认为 开放问题 2很可能成立，但需要进行深入得多的组合分析，其要求甚至超过了 [KK19中的分析； CGS+22]。

另一方面，对于不具备这些单变量独立性性质的族，情况似乎要复杂得多。即使在最简单的情形——最大有向割——我们也在 §4.3.1 中讨论过，我们针对 $\sqrt{n}$-空间对抗排序流式计算构造的困难实例，在 $O(\log n)$-空间随机排序流式计算以及 $o(n)$-空间对抗排序流式计算中都会失效。事实上，据我们所知，这些设置下关于 最大有向割的唯一下界来自最大割的平凡归约，它只能说明 $(\frac{1}{2}+\epsilon)$-近似的困难性。因此，我们猜想，[CKP+21; CGS+21]的思想

用于区分困难实例的方法，可以从 [CGV20] 推广到这些设置下针对 最大有向割的一般近似算法：

开放问题 **3.** 证明：对于每个 $\epsilon > 0$，最大有向割都可以通过以下算法实现 $(\frac{1}{2} - \epsilon)$ 近似：

i. $O(\operatorname{polylog} n)$ 空间的随机顺序流式算法。

ii. $o(n)$ 空间的对抗顺序流式算法。

8.3 Streaming (vs. sketching) lower bounds

在我们的合作研究中 [BHP+22]，我们证明了 [CGSV21a] 的流式下界，尤其是填充单向配对判据（定理 5.4），无法排除那些在 $\sqrt{n}$ 空间内超越最佳草图近似的流式近似算法。也就是说，虽然$\sqrt{n}$空间草图算法无法以$\frac{2}{9} + \epsilon$近似 最大有向割 对每个 $\epsilon > 0$成立，但 [CGSV21a] 中的技术无法将此结论加强到适用于所有流式算法（定理 7.19）。不过，正如我们在 观察 7.20, [CGSV21a] 中所述，$\sqrt{n}$空间流式算法确实无法以 ≈ 0.2362近似最大有向割。因此，我们认为以下猜想颇为可信：

开放问题 4. 证明对于每个 $\epsilon > 0$，对 *Max-3AND* 进行$(\frac{2}{9} + \epsilon)$近似的流式算法至少需要$\Omega(\sqrt{n})$ 空间。

然而，我们目前尚未发现任何可用于证明开放问题 4的候选通信博弈。

关于 $\sqrt{n}$-空间流式计算，另一个可能的方向是尝试将其扩展到$k = 2$，$q > 2$这一情形。（[CGSV21a，命题 212] 表明，在 $k = q = 2$的情形下，边缘分布匹配的分布总是填充单边对。）事实上，我们在 $q = 3$，$k = 2$的情形下构造了以下示例：

例 8.3。 我们将构造两个分布 $\mathcal{D}_Y$，$\mathcal{D}_N \in \Delta(\mathbb{Z}_3^2)$ 分别对应于 $k = 2$，$q = 3$ 情形中的分布（如 *§5.1.2* 末尾所述）。令

$$\mathcal{D}_Y = \left\{ (0,1) \ w.p. \ \frac{1}{4}, (1,1) \ w.p. \ \frac{1}{4}, (2,2) \ w.p. \ \frac{1}{2} \right\}$$

and

$$\mathcal{D}_N = \left\{ (0,2)\ w.p.\ \frac{1}{4}, (1,2)\ w.p.\ \frac{1}{4}, (2,1)\ w.p.\ \frac{1}{2} \right\}.$$

那么， $\mathcal{D}_Y$和 $\mathcal{D}_N$的第一坐标边缘分布分别为： $\{0$ 以 $_{14}$ 的概率，1 以 $_{14}$ 的概率，2 以 $\frac{1}{2}\}$ 的概率；第二坐标边缘分布为： $\{1$ 以 $_{12}$ 的概率，2 以 $\frac{1}{2}\}$ 的概率。因此，它们的边缘分布相匹配，但并非均匀分布；此外， $\mathcal{D}_Y$ 和 $\mathcal{D}_N$ 的支撑集不相交，因此它们不是填充单向配对。

8.4 Multi-pass lower bounds

Assadi 和 N 的近期多遍环计数下界 [AN21] 大致表明，对于每个固定的 $\epsilon > 0$ 和 $p \in \mathbb{N}$, $(1-3\epsilon, 1-2\epsilon)$-最大割 需要 $\Omega(n^{1-O(p\epsilon)})$ 空间用于p-遍流式算法（见他们论文中的 §5.3）。

开放问题 5。 证明对于每个 $\epsilon > 0$ 和 $p \in \mathbb{N}$，都存在 $\delta > 0$，使得任何p-遍数据流算法若能$(\frac{1}{2}+\epsilon)$近似最大割，则需要$\Omega(n^{\delta})$ 空间。（更进一步，证明需要$\Omega(n)$ 空间，并且适用于随机排序设置！）

这种界限无法通过对周期计数的归约 `依照 [AKSY20;AN21], 得出，这类归约具有以下一般结构：**是** 实例和**否** 实例都是由顶点互不相交的周期和路径组成的并集；在这些周期中，**是** 实例中的偶周期更多，而**否** 实例中的奇周期更多。**否** 实例的值低于**是**实例，因为每个割在每个奇周期中至少有一条边无法割开。然而，由于奇周期的长度至少为 3，**否** 实例的值至少为 $_{2\ 3}$，因此不能用于证明近似抗性。

相反，如果这确实可行，我们预计开放问题 5 将通过 sBPD 游戏的一个变体得到解决（见定义 3.4）：该游戏有 p “轮”，每位 Bob_t 都能在每轮重新看到自己的输入（每轮结束时，Bob_T 向 Bob_1发送一条消息）。请注意，这种“p轮、 T玩家”的 sBPD 游戏不同于有pT 位玩家的（标准）sBPD；例如，在第 1 轮中，Bob_1 可以存储其输入的某种“哈希”，然后在第 2 轮验证该哈希。因此，与单轮 sBPD 不同，Bob_1在第 2 轮的输入并非与之前的输入“独立”。因此，我们必须在这样的设定中，按照 [KK19] 的思路进行 sBPD 困难性分析 `：从第 2 轮开始，输入 $(M_t, \mathsf{z}(t))$

每位 Bob_t的输入都是从一种“典型”但并非均匀分布的分布中抽取的。在这种设定下证明困难性，似乎远远超出了当前的下界技术所能做到的范围。



术语表

Notations

k	约束满足问题/超图的元数
i	变量索引 ($\in [n]$)
ℓ	边索引 ($\in [m]$)
m	约束/超边数量
n	变量/顶点数量
q	字母表大小（$\in [m]$）
T	玩家数/子实例数
$[k]$	自然数 $\{1, \ldots, q\}$
$\mathbb{Z}_q$	模 q 的整数群
f	谓词（$\mathbb{Z}_q^k \to \{0,1\}$）
$\mathcal{F}$	谓词族
α	约束/超边密度（关于 n）
$\mathbf{b}$	CSP 谓词标签/否定模式
$\mathbf{e}$	超边的顶点索引（$\in [n]^k$）
$\mathbf{j}$	约束的变量索引（$\in [n]^k$）
$\mathbf{x}$	CSP 赋值（$\in \mathbb{Z}_q^n$）
$\mathbf{x}\|_{\mathbf{j}}$	将 $\mathbf{x}$ 投影到坐标 $\mathbf{j}$ （$\in \mathbb{Z}_q^k$）
$\mathcal{U}_S$	均匀分布
$\mathcal{M}_{k,\ \alpha}(n)$	$\mathcal{U}$ 关于 k-超匹配
$\mathcal{G}_{k,\ \alpha}(n)$	$\mathcal{U}$ 关于 k-超图
$\mathcal{B}_p$	伯努利分布-p 分布（$= 0$ 概率为 p，否则为 1）
M	顶点-超边邻接矩阵
$M_{\text{折叠}}$	M的折叠版本
$\widehat{f}$(秒)	f的傅里叶系数
$\mathbb{1}_S$	S的示性函数
supp	向量/函数/分布的支撑集
$\mathfrak{S}_k$	$[k]$上的排列集合

Abbreviations

CSP	约束满足问题
C2S	通信到流式（归约）
SDP	半定规划
UGC	唯一博弈猜想

Communication games

BPD	布尔划分检测
sBPD	顺序布尔划分检测
siBPD	隐式 sBPD
RMD	随机掩码检测
sRMD	顺序 RMD
siRSD	序列隐式随机化偏移检测

参考文献

[ABM12] Per Austrin、Siavosh Benabbas 和 Avner Magen。“关于二次阈值约束满足问题”。载于：离散数学与理论计算机科学 14.2（2012 年 11 月）。会议版本发表于 LATIN 2010，第 205–228 页。[AKSY20] Sepehr Assadi、Gillat Kol、Raghuvansh R. Saxena 和 Huacheng Yu。“用于环计数、最大割、匹配大小及其他问题的多遍图流下界”。载于：2020 年 IEEE 第 61 届计算机科学基础年会。FOCS 2020（线上，2020年11月16日至19日）。2020年11月，第 354–364 页。DOI：10.1109/FOCS46700.2020.00041。[ALM+98] Sanjeev Arora、Carsten Lund、Rajeev Motwani、Madhu Sudan 和 Mario Szegedy。“证明验证与近似问题的困难性”。载于：ACM 学报 45.3（1998 年 5 月 1 日）。会议版本发表于 FOCS 1992，第 501–555 页。ISSN：0004-5411。DOI：10.1145/278298.278306。[AM09] Per Austrin 和 Elchanan Mossel。“基于两两独立性的抗近似谓词”。载于：计算复杂性 18.2（2009 年 6 月 1 日）。会议版本发表于 CCC 2008，第 249–271 页。DOI：10.1007/s00037-009-0272-6。[AMS99] Noga Alon、Yossi Matias 和 Mario Szegedy。“近似频率矩的空间复杂度”。载于：计算机与系统科学杂志 58.1（1999 年 2 月 1 日）。会议版本发表于 STOC 1996，第 137–147 页。DOI：10.1006/jcss.1997.1545。[AMW15] Per Austrin、Rajsekar Manokaran 和 Cenny Wenner。“近似排序约束满足问题的 NP 困难性”。载于：计算理论 11（2015 年）。会议版本发表于 APPROX 2013，第 257–283 页。DOI：10.4086/toc.2015.v011a010。[AN21] Sepehr Assadi 和 Vishvajeet N. “通过流式异或引理得到的参数估计与性质测试图流下界”。载于：第 53 届 ACM SIGACT 计算理论年会论文集。STOC 2021（线上，2021 年 6 月 21–25 日）。计算机协会，2021 年 6 月 15 日，第 612–625 页。DOI：10.1145/3406325.3451110。[AOW15] Sarah R. Allen、Ryan O’Donnell 和 David Witmer。“如何反驳随机约束满足问题”。载于：2015 年 IEEE 第 56 届计算机科学基础年会。FOCS 2015。2015 年 10 月。DOI：10.1109/FOCS.2015.48。

[AS98] Sanjeev Arora 和 Shmuel Safra。《证明的概率性检验：NP 的一种新刻画》。载于：ACM 学报 45.1（1998年1月1日）。会议版本发表于 FOCS 1992，第70–122页。 DOI: 10.1145/273865.273901。[Aus07] Per Austrin。《平衡最大 2-SAT 也许并非最难问题》。载于：第39届 ACM 计算理论研讨会论文集。STOC 2007（美国加利福尼亚州圣迭戈，2007年6月11日至13日）。计算机协会，2007年6月11日，第189–197页。 DOI：10.1145/1250790.1250818。[Aus10] Per Austrin。《任意 2-CSP 的紧确不可近似性》。载于：SIAM计算杂志 39.6（2010年1月）。会议版本发表于 FOCS 2007，第2430–2463页。DOI：10.1137/070711670。[BC17] Suman K. Bera 和 Amit Chakrabarti。《进一步收紧图流中三角形及其他子结构计数的空间界》。载于：第34届计算机科学理论方面研讨会。STACS 2017（德国汉诺威，2017年3月8日至11日）。Heribert Vollmer 和 Brigitte Vall´ee 编。第66卷。LIPIcs。德国达格施图尔：Schloss Dagstuhl — Leibniz-Zentrum f¨ur Informatik，2017，11:1–11:14。DOI: 10.4230/LIPIcs.STACS.2017.11。[BCK+18] Vladimir Braverman、Stephen Chestnut、Robert Krauthgamer、Yi Li、David Woodruff 和 Lin Yang。《数据流中的矩阵范数：更快的多遍算法与行序》。载于：第35届国际机器学习会议论文集。ICLR 2018（加拿大不列颠哥伦比亚省温哥华，2018年4月30日至5月3日）。第80卷。PMLR。2018年7月3日，第649–658页。[BGJR88] Francisco Barahona、Martin Gr¨otschel、Michael J¨unger 和 Gerhard Reinelt。《组合优化在统计物理与电路布局设计中的应用》。载于：《运筹学》36.3（1988），第493–513页。 DOI：10.1287/opre. 36.3.493。[BHP+22] Joanna Boyland、Michael Hwang、Tarun Prasad、Noah Singer 和 Santhoshini Velusamy。《对（某些）对称布尔约束满足问题的草图近似：闭式比率与简单算法》。2022年2月。arXiv：2112.06319 [cs.DS]。[BK19] Amey Bhangale 和 Subhash Khot。《通过损失一半将 UG 困难性转化为 NP 困难性》。载于：第34届计算复杂性会议。CCC 2019（美国新泽西州新不伦瑞克，2019年8月18日至20日）。第137卷。LIPIcs。Schloss Dagstuhl — Leibniz-Zentrum f¨ur Informatik，2019。 DOI: 10.4230/LIPIcs.CCC.2019.3。[BKKS20] Vladimir Braverman、Robert Krauthgamer、Aditya Krishnan 和 Roi Sinoff。《矩阵流中的 Schatten 范数：稀疏性万岁，维数再见》。载于：第37届国际机器学习会议论文集。ICLR 2020（2020年4月26日至5月1日）。第119卷。PMLR。2020年11月21日，第1100–1110页。

[BKPS98] Paul Beame、Richard Karp、Toniann Pitassi 和 Michael Saks。《随机 k-CNF 公式不可满足性证明的复杂性》。载于：第30届 ACM 计算理论研讨会论文集。STOC 1998（美国得克萨斯州达拉斯，1998年5月24日至26日）。1998年5月23日，第561–571页。 DOI: 10.1145/276698. 276870。[BM16] Boaz Barak 和 Ankur Moitra。《通过平方和层级进行含噪张量补全》。载于：第29届学习理论会议论文集。COLT 2016（美国纽约州纽约市，2016年6月23日至26日）。第49卷。PMLR。2016年，第417–445页。[BR21] Arindam Biswas 和 Venkatesh Raman。《最大 r-SAT 的次线性空间近似算法》。载于：计算与组合数学。COCOON 2021（台湾台南，2021年10月24日至26日）。第13025卷。LNCS。施普林格，Cham，2021年，第124–136页。[Bul17] Andrei A. Bulatov。《非一致约束满足问题的二分定理》。载于：2017年 IEEE 第58届计算机科学基础研讨会。FOCS 2017（美国加利福尼亚州伯克利，2017年10月15日至17日）。2017年10月，第319–330页。 DOI: 10.1109/FOCS.2017. 37。[BV04] Stephen Boyd 和 Lieven Vandenberghe。《凸优化》。第1版。剑桥大学出版社，2004年3月。727页。 DOI: 10.1017/CBO9780511804441。[CGL07] Amin Coja-Oghlan、Andreas Goerdt 和 Andr´e Lanka。《随机 k-SAT 的强反驳启发式方法》。载于：组合数学、概率与计算 16.1（2007年1月）。会议版本发表于 APPROX 2004，第5–28页。 DOI: 10 . 1017 / S096354830600784X。[CGMV20] Amit Chakrabarti、Prantar Ghosh、Andrew McGregor 和 Sofya Vorotnikova。《有向图流中的顶点排序问题》。载于：第31届 ACM-SIAM离散算法研讨会论文集。SODA 2020（美国犹他州盐湖城，2020年1月5日至9日）。工业与应用数学学会，2020年1月，第1786–1802页。 DOI: 10.5555/3381089.3381198。[CGS+21] Chi-Ning Chou、Alexander Golovnev、Madhu Sudan、Ameya Velingker 和 Santhoshini Velusamy。电子邮件。个人通信。2021年。[CGS+22] Chi-Ning Chou、Alexander Golovnev、Madhu Sudan、Ameya Velingker 和 Santhoshini Velusamy。《近似约束满足问题的线性空间流式下界》。载于：第54届 ACM 计算理论研讨会论文集。STOC 2022（意大利罗马，2022年6月20日至24日）。即将发表。2022年。[CGSV21a] Chi-Ning Chou、Alexander Golovnev、Madhu Sudan 和 Santhoshini Velusamy。《利用线性草图实现所有布尔约束满足问题的可近似性》。2021年2月24日。arXiv: 2102.12351v7 [cs.CC]。

[CGSV21b] Chi-Ning Chou、Alexander Golovnev、Madhu Sudan 和 Santhoshini Velusamy。《使用线性草图对所有有限约束满足问题进行可近似性研究》。载于：第62届 IEEE 计算机科学基础年会论文集。FOCS 2021（美国科罗拉多州丹佛，2022年2月7日至10日）。IEEE计算机学会，2021年。 DOI：10.1109/ FOCS52979.2021.00117。[CGV20] Chi-Ning Chou、Alexander Golovnev 和 Santhoshini Velusamy。《所有布尔最大2-CSP和最大kSAT的最优流式近似》。载于：2020 年 IEEE 第 61 届计算机科学基础年会。FOCS 2020（线上，2020年11月16日至19日）。IEEE计算机学会，2020年11月，第330–341页。 DOI：10.1109/FOCS46700.2020.00039。[Cha20] Amit Chakrabarti。《数据流算法》。讲义（草稿）。讲义（草稿）。2020年7月2日。 URL：https://www.cs.dartmouth.edu/~ac/Teach/CS35-Spring20/Notes/lecnotes.pdf。[CHIS12] Mahdi Cheraghchi、Johan H˚astad、Marcus Isaksson 和 Ola Svensson。《线性阈值谓词的近似》。载于：ACM计算理论汇刊 4.1（2012年3月1日）。会议版本发表于 APPROX 2010，2:1–2:31。 DOI：10.1145/2141938.2141940。[CKP+21] Lijie Chen、Gillat Kol、Dmitry Paramonov、Raghuvansh Saxena、Zhao Song 和 Huacheng Yu。电子邮件。2021年3月16日。[CKS01] Nadia Creignou、Sanjeev Khanna 和 Madhu Sudan。《布尔约束满足问题的复杂性分类》。离散数学与应用。工业与应用数学学会，2001年。 DOI：10 . 1137/ 1 . 9780898718546。[CMM09] Moses Charikar、Konstantin Makarychev 和 Yury Makarychev。《最大约束满足问题的近似最优算法》。载于：ACM算法汇刊 5.3（2009年7月）。会议版本发表于 SODA 2007，第1–14页。DOI：10.1145/1541885.1541893。[CS98] Benny Chor 和 Madhu Sudan。《介于关系的几何方法》。载于：SIAM离散数学期刊 11.4（1998年）。会议版本发表于算法，ESA 1995，第511–523页。 DOI：10.1137/S0895480195296221。[EH08] Lars Engebretsen 和 Jonas Holmerin。《用于 NP 的 PCP 中更高效的查询，以及最大约束满足问题近似困难性的改进》。载于：随机结构与算法 33.4（2008年12月）。会议版本发表于 STACS 2005，第497–514页。DOI：10.1002/rsa.20226。[Fei02] Uriel Feige。《平均情形复杂性与近似复杂性之间的关系》。载于：第34届ACM计算理论年会论文集。STOC 2002。美国纽约州纽约市：计算机协会，2002年5月19日，第534–543页。 DOI：10.1145/509907.509985。

[Fei98] Uriel Feige。《集合覆盖近似的 $\ln n$ 阈值》。载于：ACM 学报 45.4（1998年7月）。会议版本发表于 STOC 1996，第634–652页。 DOI：10.1145/285055.285059。[FG95] Uriel Feige 和 Michel X. Goemans。《双证明者证明系统值的近似及其在 MAX 2SAT 和 MAX DICUT 中的应用》。载于：第3届以色列计算理论与系统研讨会论文集。ISTCS 2003（1995年1月4日至6日）。IEEE计算机学会，1995年，第182–189页。 DOI：10.1109/ISTCS.1995.377033。[FGK05] Joel Friedman、Andreas Goerdt 和 Michael Krivelevich。《高效识别更多不可满足的随机 k-SAT实例》。载于：SIAM计算杂志 35.2（2005年1月）。会议版本发表于 STACS 2001，第408–430页。 DOI：10.1137/S009753970444096X。[FK98] Uriel Feige 和 Joe Kilian。《零知识与色数》。载于：计算机与系统科学杂志 57.2（1998年10月1日）。会议版本发表于 CCC 1996，第187–199页。 DOI：10.1006/jcss.1998.1587。 URL：https://www.sciencedirect.com/science/article/pii/S0022000098915872。[FO07] Uriel Feige 和 Eran Ofek。《大型随机3CNF公式中易于反驳的子公式》。载于：计算理论 3（2007年2月9日），第25–43页。 DOI：10.4086/ toc.2007.v003a002。[FV98] Tom´as Feder 和 Moshe Y. Vardi。《单调单子 SNP 与约束满足的计算结构：通过 Datalog 和群论进行研究》。载于：SIAM计算杂志 28.1（1998年1月），第57–104页。 DOI：10. 1137/S0097539794266766。[GHM+11] Venkatesan Guruswami、Johan H˚astad、Rajsekar Manokaran、Prasad Raghavendra 和 Moses Charikar。《击败随机排序很难：每个排序约束满足问题都具有近似抗性》。载于：SIAM计算杂志 40.3（2011年）。会议版本发表于 FOCS 2008，第878–914页。 DOI：10.1137/090756144。[GKK+08] Dmitry Gavinsky、Julia Kempe、Iordanis Kerenidis、Ran Raz 和 Ronald de Wolf。《单向量子通信复杂度的指数分离及其在密码学中的应用》。载于：SIAM计算杂志 38.5（2008年12月）。会议版本发表于 STOC 2007，第1695–1708页。 ISSN：0097-5397。 DOI：10.1137/ 070706550。[GKM22] Venkatesan Guruswami、Pravesh K. Kothari 和 Peter Manohar。《布尔约束满足问题反驳的算法与证书：“平滑情形不比随机情形更难”》。载于：第54届ACM年度计算理论研讨会论文集。STOC 2022（意大利罗马，2022年6月20日至24日）。2022年。

[GL17] Venkatesan Guruswami 和 Euiwoong Lee。《对称约束满足问题近似抗性的刻画》。载于：Theory of Computing 13.1（2017年6月13日）。会议版发表于 APPROX 2015，第 1–24 页。 DOI: 10.4086/toc.2017. v013a003.[GLST98] V. Guruswami、D. Lewin、M. Sudan 和 L. Trevisan。《用 3 查询 PCP 刻画 NP》。载于：第 39 届计算机科学基础研讨会年会论文集。FOCS 1998（美国加利福尼亚州帕洛阿尔托，1998年11月8–11日）。1998年11月，第 8–17 页。 DOI: 10.1109/SFCS.1998.743424.[GO16] Venkatesan Guruswami 和 Krzysztof Onak。《多遍图处理的超线性下界》。载于：Algorithmica 76.3（2016年3月）。会议版发表于 CCC 2013，第 654–683 页。 DOI: 10.1007/s00453-016-0138-7.[Gol11] Oded Goldreich。《三个 XOR 引理 —— 阐述》。载于：复杂性与密码学研究：随机性与计算交互杂论。Oded Goldreich 编。计算机科学讲义。柏林、海德堡：施普林格，2011年，第 248–272 页。 ISBN: 978-3-642-22670-0。 DOI: 10.1007/978- 3-642-22670-0_22.[GS21] Anupam Gupta 和 Sahil Singla。《随机顺序模型》。载于：超越算法的最坏情况分析。Tim Roughgarden 编。234-258：剑桥大学出版社，2021年1月14日。 ISBN: 978-1-108-49431-1。 URL: 10.1017/9781108637435. 015。[GT19] Venkatesan Guruswami 和 Runzhou Tao。《唯一博弈的流式计算困难性》。载于：近似、随机化与组合优化：算法与技术。APPROX 2019（美国马萨诸塞州剑桥，2019年9月20–22日）。Dimitris Achlioptas 和 L´aszl´o A. V´egh 编。第 145 卷。LIPIcs。Schloss Dagstuhl — Leibniz 信息学中心，2019年9月，5:1–5:12。 DOI: 10 .4230 / LIPIcs. APPROX-RANDOM.2019.5.[GVV17] Venkatesan Guruswami、Ameya Velingker 和 Santhoshini Velusamy。《近似最大 2-CSP 和最大无环子图的流式复杂性》。载于：近似、随机化与组合优化：算法与技术。APPROX 2017（美国加利福尼亚州伯克利，2017年8月16–18日）。Klaus Jansen、Jos´e D. P. Rolim、David Williamson 和 Santosh S. Vempala 编。第 81 卷。LIPIcs。Schloss Dagstuhl — Leibniz 信息学中心，2017年8月，8:1–8:19。DOI: 10.4230/LIPIcs.APPROX-RANDOM.2017.8.[GW95] Michel X. Goemans 和 David P. Williamson。《利用半定规划改进最大割和可满足性问题的近似算法》。载于：ACM 学报 42.6（1995年11月）。会议版发表于 STOC 1994，第 1115–1145 页。 ISSN: 0004-5411, 1557-735X。 DOI: 10.1145/227683.227684。

[H˚as01] Johan H˚astad。《一些最优不可近似性结果》。载于：ACM 学报 48.4（2001年），第 798–859 页。 DOI: 10.1145/502090.502098.[Has04] Gustav Hast。《利用随机限制近似最大 k 约束满足问题》。载于：近似、随机化与组合优化：算法与技术。APPROX 2004（美国马萨诸塞州剑桥，2004年8月22–24日）。Klaus Jansen、Sanjeev Khanna、Jos´e D. P. Rolim 和 Dana Ron 编。第 3122 卷。LNCS。施普林格，2004年，第 151–162 页。 DOI: 10.1007/978-3-540-27821-4_14.[Has05] Gustav Hast。《近似最大 k约束满足问题——以近乎线性因子超越随机赋值》。载于：自动机、语言与编程。ICALP 2005（2005年7月11–15日）。Lu´ís Caires、Giuseppe F. Italiano、Lu´ís Monteiro、Catuscia Palamidessi 和 Moti Yung 编。第 3580 卷。LNCS。施普林格，2005年，第 956–968 页。 DOI: 10.1007/11523468_77.[H˚as99] Johan H˚astad。《团在 $n^{1-\epsilon}$ 内难以近似》。载于：Acta Mathematica 182.1（1999年3月1日）。会议版发表于 FOCS 1996，第 105–142 页。 ISSN: 1871-2509。 DOI: 10.1007/BF02392825.[IMNO11] Piotr Indyk、Andrew McGregor、Ilan Newman 和 Krzysztof Onak。《数据流、性质测试及相关主题中的开放问题》。汇编自 IITK 海量数据集处理算法研讨会（2009年）和 Bertinoro 次线性算法研讨会（2011年）。2011年6月14日。 URL: https : // sublinear.info/files/bertinoro2011_kanpur2009.pdf.[Ind06] Piotr Indyk。《稳定分布、伪随机生成器、嵌入与数据流计算》。载于：ACM 学报 53.3（2006年5月）。会议版发表于 FOCS 2000，第 307–323 页。 DOI: 10.1145/1147954.1147955.[Kar72] Richard M. Karp。《组合问题之间的可约性》。载于：IBM 研究研讨会系列。R.E. Miller、J.W. Thatcher 和 J.D. Bohlinger 编。施普林格，1972年，第 85–103 页。 DOI: 10.1007/978-1-4684-2001-2_9.[Kho02] Subhash Khot。《唯一性双验证者单轮游戏的能力》。载于：第 34 届 ACM 计算理论研讨会论文集。STOC 2002（加拿大魁北克，2002年5月19–21日）。计算机协会，2002年5月，第 767–775 页。´: 10.1145/509907.510017. DOIKho[Subhash Khot。《关于唯一博弈猜想（特邀综述）》。载于：2010 年 IEEE 第 25 届计算复杂性年会论文集。CCC 2010（美国马萨诸塞州剑桥，2010年6月9–11日）。IEEE计算机学会，2010年6月9日，第 99–121 页。10] : 10.1109/CCC.2010.19. DOIKK[Dmitry Kogan 和 Robert Krauthgamer。《图与超图中的割草图化》。载于：第 6 届理论计算机科学创新年会论文集。ITCS 2015（以色列雷霍沃特，2015年1月11–13日）。计算机协会，2015年，第 367–376 页。15] : 10.1145/2688073.2688093。

[KK19] Michael Kapralov 和 Dmitry Krachun。《近似最大割的最优空间下界》。载于：第 51 届 ACM SIGACT计算理论研讨会论文集。STOC 2019（美国亚利桑那州菲尼克斯，2019 年 6 月 23–26 日）。计算机协会，2019 年 6 月，第 277–288 页。 DOI：10.1145/3313276.3316364。[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？》。载于：SIAM计算杂志 37.1（2007 年 5 月 14 日）。会议版本发表于 FOCS 2004。 DOI：10.1137/S0097539705447372。[KKP18] John Kallaugher、Michael Kapralov 和 Eric Price。《图与超图计数的草图复杂度》。载于：2018 IEEE 第 59 届计算机科学基础研讨会。FOCS 2018（法国巴黎，2018 年 10 月 7–9 日）。2018 年 10 月，第 556–567 页。 DOI：10.1109/FOCS.2018.00059。[KKS15] Michael Kapralov 、Sanjeev Khanna 和 Madhu Sudan。《近似最大割的流式下界》。载于：第 26 届 ACM-SIAM离散算法研讨会论文集。SODA 2015（美国加利福尼亚州圣迭戈，2015 年 1 月 4–6 日）。工业与应用数学学会，2015 年 1 月，第 1263–1282 页。 DOI：10.1137/1.9781611973730.84。[KKSV17] Michael Kapralov、Sanjeev Khanna、Madhu Sudan 和 Ameya Velingker。《对最大割的 ($1+\omega(1)$)-近似需要线性空间》。载于：第 28 届 ACM-SIAM离散算法研讨会论文集。SODA 2017（西班牙巴塞罗那，2017 年 1 月 16–19 日）。工业与应用数学学会，2017 年 1 月，第 1703–1722 页。 DOI：10.5555/3039686.3039798。[KMOW17] Pravesh K. Kothari、Ryuhei Mori、Ryan O'Donnell 和 David Witmer。《用于反驳任意约束满足问题的平方和下界》。载于：第 49 届 ACM SIGACT计算理论研讨会论文集。STOC 2017。即将发表。计算机协会，2017 年 6 月 19 日，第 132–145 页。 DOI：10. 1145/ 3055399.3055485。[KNW10] Daniel M. Kane、Jelani Nelson 和 David P. Woodruff。《关于草图化和流式计算小范数的精确空间复杂度》。载于：2010 年 ACM-SIAM离散算法研讨会论文集。SODA 2010（美国德克萨斯州奥斯汀，2010 年 1 月 17–19 日）。工业与应用数学学会，2010 年，第 1161–1178 页。 DOI：10.1137/1.9781611973075.93。[KO09] Subhash Khot 和 Ryan O'Donnell。《最大割增益的半定规划间隙与唯一博弈猜想困难性》。载于：Theory of Computing 5.4（2009 年 5 月 29 日）。会议版本发表于 STOC 2006，第 83–117 页。 DOI：10.4086/toc.2009.v005a004。

[KP20] John Kallaugher 和 Eric Price。《转向式流式计算与线性草图化之间的分离与等价性》。载于：第 52 届 ACM SIGACT计算理论研讨会论文集。STOC 2020（线上，2020 年 6 月 22–26 日）。美国纽约州纽约市：计算机协会，2020 年，第 1223–1236 页。 URL: http://doi.org/10.1145/3357713.3384278。[KR08] Subhash Khot 和 Oded Regev。《顶点覆盖可能难以近似到 $2-\epsilon$ 以内》。载于：Journal of Computer and System Sciences。Computational Complexity 2003 74.3（2008 年 5 月 1 日）。会议版本发表于 CCC 2003，第 335–349 页。DOI: 10.1016/j.jcss.2007.06.019。[KSTW01] Sanjeev Khanna、Madhu Sudan、Luca Trevisan 和 David P. Williamson。《约束满足问题的可近似性》。载于：SIAM计算杂志 30.6（2001 年 1 月 1 日）。会议版本发表于 STOC 1997 和 CCC 1997，第 1863–1920 页。 ISSN: 0097-5397。 DOI: 10.1137/S0097539799349948。 URL: https://epubs.siam.org/doi/10.1137/S0097539799349948（访问于 2021 年 10 月 29 日）。[LLZ02] Michael Lewin、Dror Livnat 和 Uri Zwick。《最大 2-SAT 与最大有向割问题的改进舍入技术》。载于：整数规划与组合优化。IPCO 2002。William J. Cook 和 Andreas S. Schulz 编。2002 年，第 67–82 页。 DOI: 10.1007/3-540-47867-1_6。[McG14] Andrew McGregor。《图流算法：综述》。载于：ACM SIGMOD Record 43.1（2014 年 5 月 13 日），第 9–20 页。 DOI: 10.1145/2627692.2627694。[MM01] Shiro Matuura 和 Tomomi Matsui。《最大有向割的 0.863-近似算法》。载于：近似、随机化与组合优化：算法与技术。APPROX 2001（美国加利福尼亚州伯克利，2001 年 8 月 18–20 日）。Michel Goemans、Klaus Jansen、Jos´e D. P. Rolim 和 Luca Trevisan 编。第 2129 卷。LNCS。柏林、海德堡：施普林格，2001 年，第 138–146 页。 DOI: 10 . 1007 / 3 - 540 - 44666-4_17。[MM17] Konstantin Makarychev 和 Yury Makarychev。《约束满足问题的近似算法》。载于：约束满足问题：复杂性与可近似性。Andrei Krokhin 和 Stanislav Zivny 编。第 7 卷。Dagstuhl Follow-Ups。德国达格施图尔：Schloss Dagstuhl — Leibniz-Zentrum f¨ur Informatik，2017 年，第 287–325 页。DOI: 10.4230/DFU.Vol7.15301.287。[Mut05] S. Muthukrishnan。《数据流：算法与应用》。第 1 卷。《理论计算机科学基础与趋势》2。Now Publishers, Inc.，2005 年 9 月 26 日。119 页。 DOI: 10.1561/0400000002。[New00] Alantha Newman。《最大无环子图的近似》。硕士论文。麻省理工学院，2000 年。[O'D14] Ryan O'Donnell。《布尔函数分析》。第 1 版。美国纽约州纽约市：剑桥大学出版社，2014 年 6 月 1 日。444 页。 ISBN: 978-1-107-03832-5。

[Opa79] Jaroslav Opatrny。《全序问题》。载于：《SIAM计算杂志》8.1（1979年2月），第111–114页。 DOI：10.1137/0208008。[Pot19] Aaron Potechin。《关于平衡线性阈值函数的近似抗性》。载于：第51届年度ACM SIGACT计算理论研讨会论文集。STOC 2019（美国亚利桑那州菲尼克斯，2019年6月23–26日）。计算机协会，2019年6月23日，第430–441页。 DOI：10.1145 / 3313276 . 3316374。[PS18] Pan Peng 和 Christian Sohler。《从随机顺序流中估计图参数》。载于：第29届年度ACM-SIAM离散算法研讨会论文集。SODA 2018（美国路易斯安那州新奥尔良，2018年1月7–10日）。工业与应用数学学会，2018年1月。 DOI：10 . 1137 / 1 . 9781611975031.157。[Rag08] Prasad Raghavendra。《每个约束满足问题的最优算法与不可近似性结果？》。载于：第40届年度ACM计算理论研讨会论文集。STOC 2008（加拿大不列颠哥伦比亚省维多利亚，2008年5月17–20日）。2008年，第245–254页。 DOI：10.1145/1374376.1374414。[RRS17] Prasad Raghavendra、Satish Rao 和 Tselil Schramm。《在谱阈值以下强力反驳随机约束满足问题》。载于：第49届年度ACM SIGACT计算理论研讨会论文集。STOC 2017（加拿大魁北克省蒙特利尔，2017年6月19–23日）。2017年6月19日，第121–131页。 DOI：10.1145/3055399.3055417。[Sch78] Thomas J. Schaefer。《可满足性问题的复杂性》。载于：第10届年度ACM计算理论研讨会论文集。STOC 1978（美国加利福尼亚州圣迭戈，1978年5月1–3日）。计算机协会，1978年5月1日，第216–226页。 DOI：10.1145/800133.804350。[SSV21] Noah Singer、Madhu Sudan 和 Santhoshini Velusamy。《每个排序约束满足问题的流式近似抗性》。载于：《近似、随机化与组合优化：算法与技术》。APPROX 2021（2021年8月16–18日）。Mary Wootters 和 Laura Sanit`a 编。第207卷。LIPIcs。Schloss Dagstuhl — 莱布尼茨信息学中心，2021年9月，17:1–17:19。 DOI：10.4230/LIPIcs. APPROX/RANDOM.2021.17。[ST00] Alex Samorodnitsky 和 Luca Trevisan。《具有最优摊销查询复杂度的NP类PCP刻画》。载于：第32届年度ACM计算理论研讨会论文集。STOC 2000（美国俄勒冈州波特兰，2000年5月21–23日）。美国俄勒冈州波特兰：计算机协会，2000年，第191–199页。 DOI：10.1145/335305.335329。[ST09] Alex Samorodnitsky 和 Luca Trevisan。《Gowers一致性、变量影响力与概率可检验证明》。载于：《SIAM计算杂志》39.1（2009年1月）。会议版本发表于STOC 2006，第323–360页。 DOI：10.1137/070681612。

[ST98] Madhu Sudan 和 Luca Trevisan。《具有低摊销查询复杂度的概率可检验证明》。载于：第39届计算机科学基础年度研讨会论文集。SFCS 1998（美国加利福尼亚州帕洛阿尔托，1998年11月8日至11日）。IEEE计算机学会，1998年，第18–27页。 DOI：10.1109/SFCS.1998.743425。[Tre04] Luca Trevisan。组合优化问题的不可近似性。2004年9月23日。arXiv：cs/0409043。[Tre12] Luca Trevisan。《关于 Khot 的唯一博弈猜想》。载于：美国数学学会通报 49.1（2012年1月），第91–111页。 DOI：10.1090/S0273-0979-2011-01361-1。[Tre98a] Luca Trevisan。《通过正线性规划实现并行近似算法》。载于：Algorithmica 21.1（1998年5月），第72–88页。 DOI：10.1007/PL00009209。[Tre98b] Luca Trevisan。《在概率可检验证明和线性测试中回收查询》。载于：第30届ACM计算理论研讨会论文集。STOC 1998（美国德克萨斯州达拉斯，1998年5月24日至26日）。计算机协会，1998年，第299–308页。 DOI：10.1145/276698.276769。[TSSW00] Luca Trevisan、Gregory B. Sorkin、Madhu Sudan 和 David P. Williamson。《构件、近似与线性规划》。载于：SIAM计算杂志 29.6（2000年1月1日）。会议版本发表于 FOCS 1996，第2074–2097页。 DOI：10.1137/S0097539797328847。[Yao77] Andrew Chi-Chih Yao。《概率计算：迈向统一的复杂度度量》。载于：第18届计算机科学基础年度研讨会论文集。SFCS 1977（美国罗得岛州普罗维登斯，1977年10月31日至11月2日）。IEEE计算机学会，1977年9月30日，第222–227页。 DOI：10.1109/SFCS.1977.24。[Zhu20] Dmitriy Zhuk。《CSP二分猜想的证明》。载于：ACM 学报 67.5（2020年8月26日）。会议版本发表于 FOCS 2017，30:1–30:78。 DOI：10.1145/3402029。[Zwi00] Uri Zwick。分析 Feige 和 Goemans 的最大 2-SAT 与最大有向割近似算法。2000年3月2日。 URL：https://www.cs.tau.ac.il/~zwick/papers/max2sat-maxdicut.ps.gz。[Zwi98] Uri Zwick。《至多涉及三个变量的约束满足问题的近似算法》。载于：第9届ACM-SIAM离散算法研讨会论文集。SODA 1998（美国加利福尼亚州旧金山，1998年1月25日至27日）。计算机协会，1998年，第201–210页。DOI：10.5555/314613.314701。



This thesis was typeset我们-ing LaTeX，最初由 Leslie Lamport 开发，并以 Donald Knuth 的 TEX 为基础。上面的插*Science Experiment 02*图由 Ben Schlitter 创作，并以 CC BY-NC-ND 3.0发布。一个可用于按照这种外观& 风格排版博士论文的模板已根据宽松的AGPL 许可证发布，可在线访问github.com/suchow/Dissertate，也可联系其主要作者 Jordan Suchow，邮箱地址为 suchow@post.harvard.edu。