arXiv:2512.19515v1 [cs.CC] 22 Dec 2025

即使在较小深度下，否定也很强大

Bruno Cavalar * Th´eo Bor´em Fabris† Partha Mukhopadhyay‡
Srikanth Srinivasan§ Amir Yehudayoff¶

2025年12月23日

摘要

我们研究布尔设置和代数设置中否定的力量，并证明了以下结果。

1. 我们构造了一族含有 n 个变量的多项式，其中所有单项式的系数均为正数，使得 P_n 可以由一个多项式规模的深度三电路计算，但任何计算它的单调电路规模都至少为 $2^{\Omega(n)}$。这是单调与非单调算术计算之间可能达到的最强分离结果，改进了此前所有结果，包括 Valiant（1980）的开创性工作，以及 Chattopadhyay、Datta 和 Mukhopadhyay（2021）最近的研究。随后，我们将这一结果进一步推广，从而证明常数次数多项式具有强单调分离性，解决了 Shpilka 和 Yehudayoff（2010）综述中提出的一个开放问题。

2. 转向布尔情形后，我们可以为特定布尔函数证明超多项式的单调布尔电路下界，这意味着某些单调多项式的所有幂都无法由多项式规模的单调算术电路计算。这在算术情形下带来了一种新型的单调与非单调分离。

3. 随后，我们定义了一类具有线性代数性质的问题，它们与张成程序相似，并证明了这些问题的单调布尔电路下界。特别是，这为均匀分布（非单调）$\mathbf{NC}^2$ 中的函数给出了目前已知最强的单调下界。我们的构造还导出了一个显式拟阵，该拟阵定义了一个难以计算的单调函数，从而解决了 Jukna 和 Seiwert（2020）提出的一个开放问题；该问题涉及贪心算法与纯动态规划算法相对能力的比较。

我们的单调算术复杂度和布尔电路下界基于已知技术，例如将单调算术复杂度归约为多划分通信复杂度，以及用于证明单调布尔电路下界的近似方法；但为了利用低深度电路获得高效上界，我们克服了若干新的挑战。

*牛津大学计算机科学系，英国。获英国工程与自然科学研究委员会项目 EP/Z534158/1“计算复杂性综合研究方法：结构、自指与下界”资助。电子邮箱：bruno.cavalar@cs.ox.ac.uk

†哥本哈根大学计算机科学系，丹麦。获欧洲研究委员会（ERC）资助，资助协议编号为 101125652（ALBA）。电子邮箱：thfa@di.ku.dk

‡印度金奈数学研究所。电子邮件：partham@cmi.ac.in§丹麦哥本哈根大学计算机科学系。获欧洲研究委员会（ERC）根据编号为101125652（ALBA）的资助协议资助。电子邮件：srsr@di.ku.dk

¶哥本哈根大学计算机科学系，以及以色列理工学院。获丹麦国家研究基金会主席项目资助。电子邮件：amir.yehudayoff@gmail.com

目录

1 引言 1
1.1 背景与结果 .1
1.2 挑战与证明思路 .3
1.3 开放问题 .7
1.4 致谢 .8

2 算术分离 9
2.1 图生成的多项式及其 $\Sigma\Pi\Sigma$ 上界.9
2.2 单调算术复杂度与通信复杂度.11
2.3 多分区通信复杂度下界.12
2.4 单调算术电路下界.15

3 单调布尔电路下界的一个判据 16

4 布尔分离 20
4.1 非单调低深度电路上界 .20
4.2 通过良性编码得到的单调布尔电路下界 .20
4.3 良性编码的显式构造 .26

5 混合分离 29
5.1 非单调低深度电路上界 .29
5.2 性质良好的 $\mathbb{R}$-矩阵 .29
5.3 利用性质良好的矩阵得到单调布尔电路下界 .34

1 引言

1.1 背景与结果

算术模型之间的分离。在论文《一次否定具有指数级威力》中，Valiant [Val80] 证明，VP 中存在 n 元单调多项式，要求单调算术电路的规模至少为 $2^{\Omega(n^{1/2})}$，并且 VP 中的每项计算都可以通过一个否定门完成。Chattopadhyay、Datta 和 Mukhopadhyay [CDM21]最近将上界加强到了深度三电路（也称为 $\Sigma\Pi\Sigma$ 电路）；他们证明，对于一个可由多项式规模的 $\Sigma\Pi\Sigma$ 电路计算的单调多项式，其单调电路复杂度有一个 $2^{\tilde{\Omega}(n^{1/4})}$ 下界。另一项近期工作表明，在常数度扩展图上定义、含有 n 个变量的生成树多项式，其单调算术电路复杂度为 $2^{\Omega(n)}$ [CDGM22]。然而，生成树多项式目前已知的最佳非单调上界是一个多项式规模的代数分支程序（ABP） [W70] ，通过行列式计算得到 [Csa76, Ber84]。我们的第一个主要结果是对这些结果的加强。

定理 m 1.1. 存在一个 n 元多项式 $P = P_n$ ，满足以下条件：

1. P 可由一个大小为 $O(n^3)$ 的 $\Sigma\Pi\Sigma$ 电路计算。
2. 任何计算 P 的单调算术电路，其大小至少为 $2^{\Omega(n)}$。

定理 P_n中的多项式族 $_{n\geq 1}$ 可以由一致电路序列计算。也就是说，存在一台图灵机，它以 n作为输入，运行时间为多项式时间（n），并输出一个计算 P_n的电路。多项式 P_n 由一个具有 G个顶点的扩展图 $n/2$描述，其形式为

$$P_n(x) = \sum_{a\in\{0,1\}^{n/2}} \left(\sum_{\{u,v\}\in E(G)} a_u a_v - 1 \right)^2 \prod_{i=1}^{n/2} x_{i,a_i}. \tag{1}$$

下面我们将证明，存在一个规模较小的 $\Sigma\Pi\Sigma$ 电路来计算 P_n。利用 G 是扩展图这一事实，我们证明 P_n 的单调电路复杂度很高。这基于一个从单调算术电路下界到通信复杂度问题的归约。近年来有若干结果利用了单调电路下界与通信复杂度之间的联系， [RY11、HY13、Sri20、CDM21、CDGM22、CGM22]。

综上，这在代数设置中实现了单调计算与非单调计算之间可能达到的最强分离。单个否定门对两个单调深度三电路执行减法；即使与一般的单调电路相比，它也具有指数级的强大能力。

填充论证使我们能够推导出常次数多项式的单调算术电路与非单调算术电路之间的新分离结果。这使我们能够解决 Shpilka 和 Yehudayoff 的综述中提出的开放问题 9 [SY10]。在这项工作之前，对于常次数多项式，已知的分离结果仅存在于单调算术电路与一般算术公式 [HY09]之间。

定理 1.2。 对于每个常数 $k \in \mathbb{N}$ 和 $n \in \mathbb{N}$，都存在一个 n 元多项式 $P = P_{n,\,k}$ 其总次数为 k ，满足以下条件：

1. P 可以由大小为 $O(n(\log n)^2)$ 的 $\Sigma\Pi\Sigma$ 电路计算。
2. 任何计算 P 的单调算术电路，其规模至少为 $(n/k)^{\Omega(k)}$.

这种填充论证之所以可行，仅仅是因为我们在定理 ***1.1*** 中证明了一个强指数级 [CDM21]下界（强化了 P_n ），也因为我们对上文定义的多项式 [CDGM22] 给出的上界非常简单（目前尚不清楚如何从 [CDGM22] 的强指数级下界得到这种分离）。

算术模型与布尔模型之间的分离。研究单调算术复杂度的主要挑战之一，是证明存在显式单调多项式P，使得对每个单调多项式 Q， $P\cdot Q$ 的单调复杂度 [HY21]都很高。我们的所有证明技巧似乎都无法解决这个问题。我们朝着解决这一问题迈出了一步。我们找到了一个显式单调多项式 P，使得 P 具有规模较小的非单调算术电路，但 P 的每个幂次的单调复杂度都很高。据我们所知，这是首个此类分离。

我们通过与布尔电路下界的联系来实现这一点。对于每个 n 元单调多项式 P（定义在 $\mathbb{R}$ 上），我们可以通过如下对应关系定义一个单调布尔函数 f_P: $\{0,1\}^n \to \{0,1\}$

$$f_P(x) = 1 \iff P(x) > 0.$$

我们的第一个观察是， P 的单调电路可以导出 f_P. 的单调电路

观察 1.3。如果 P 可以由规模为 s 的单调算术电路计算，那么 f_P 可以由规模为 s 的单调布尔电路计算。

概要。将 $+$ 门替换为 $\vee$ 门，并将 $\times$ 门替换为 $\wedge$门，即可得到计算 s 的布尔电路。■

一个优点是， f_P 不仅对应于 P，还对应于 P的所有幂。因此， f_P 的单调下界可以导出 P 所有幂的单调下界。第二个重要优点是，我们知道如何证明单调布尔复杂度的下界。Razborov [Raz85] 以及之后的许多研究 [AB87、Tar88、HR00、CKR22、CGR$^+$25] 发展了用于证明布尔单调电路复杂度下界的近似方法。特别是，已知的完美二分图匹配函数下界已经意味着，永久多项式的任意幂对于单调算术电路都是超多项式难的 [Raz85] （甚至是指数级难的 [CGR$^+$25]）。

我们可以将此结果推广，以证明分离性。为此，我们还需要给 P或 f_P的非单调电路复杂度给出上界。通过线性代数和行列式来证明算术电路上界，是一个核心工具 [Csa76，Val79，Ber84，MV97]。综合起来，我们得到以下强分离性结果。

定理 1.4。存在一个实数域上的单调 n 元多项式 $P = P_n$，满足以下性质：

1. P 可以由一个 算术电路计算，其规模关于 n 为多项式，深度为 $O((\log n)^2)$。
2. 任何计算与 P 对应的布尔函数 f_P 的单调布尔电路，其规模至少为 $n^{\Omega((\log n)^{1/2})}$。

因此，任何计算 P 的幂的单调算术电路，其规模也必定是超多项式级别。

布尔模型之间的分离性。将我们的构造稍作调整，使其适用于域 $\mathbb{F}_2$ ，也能在布尔情形下改进单调电路与非单调电路之间的分离性。我们稍作迂回，以便更好地说明背景。[AB87、Tar88]的结果表明，存在一个属于 P 的单调函数，需要规模为 $2^{n^{1/6-o(1)}}$的单调电路。基于这些结果，de Rezende 和 Vinyals [dRV25]最近证明，存在一个属于 P 的单调函数，需要规模为 $2^{n^{1/3-o(1)}}$的单调电路。最近，Cavalar 等人 [CGR+25] 改进了 Razborov 的结果，并证明二分图的匹配函数（可由 RNC [Lov79] 计算，也可由准 NC [FGT19]计算），以及另一个可由 L 计算的显式单调函数，都需要规模为 $2^{n^{1/6-o(1)}}$的单调电路。更早的工作 [GKRS18、GGKS20]也展示了一个属于 NC 的显式函数，它需要规模为 $2^{n^{\varepsilon}}$的单调电路，其中 $\varepsilon > 0$ 是一个未明确指定的常数。

在本文中，我们得到了以下定理，为一个属于**NC** 的函数证明了最强的定量下界（除 $o(1)$ 项外，该下界也达到了已知的属于**P**的函数的最佳下界）。

定理 1.5。 对于任意充分大的 $n \in \mathbb{N}$，存在一个单调布尔函数 $f\colon \{0,1\}^n \to \{0,1\}$ ，满足以下性质：

1. f 可由一个规模关于 n 为多项式、深度为 $O(\log n)^2$,的均匀布尔电路计算，即 f 属于均匀分布 $\mathbf{NC}^2$
2. 任何计算 f 的单调布尔电路，其规模至少为 $2^{n^{1/3-o(1)}}$。

函数 f （定理 1.5中的函数）具有另一项重要性质。由于任意单调函数都由其极小项所确定，因此比较极小项的“复杂度”与该函数的单调复杂度颇有意义。具体而言，Jukna 和 Seiwert [JS20] 研究了极小项为拟阵基的单调函数。他们的研究动机是比较贪心算法与纯动态规划算法的能力。按照他们的术语，函数 f （定理 1.5 中的函数）给出了一个明确的问题实例：贪心算法可以精确地解决该问题，而使用纯动态规划近似求解该问题的代价很高。他们通过计数论证证明了这类问题的存在，但我们给出了此类函数的首个显式例子，解决了他们研究中的一个开放问题（见 [JS20，问题 1]）。近年来，虽然也有其他关于通过线性代数定义的单调布尔函数的下界结果 [GKRS18、CGR+25]，但这些结果似乎无法为上述基于拟阵的函数导出下界。

1.2 挑战与证明思路

算术下界。为了证明定理 1.1，我们沿用了 Hrubeˇs 和 Yehudayoff [HY13] 在非交换情形下的一个思路，[1] 而这一思路又受到通信复杂度方面结果的启发 [Raz92, FMP+15]。设 $P(x_1,0,x_1,1,\ldots,x_n,0,x_n,1)$ 是一个（集合多线性）多项式，使得 P 中的每个单项式都具有 $x_{1,a_1}\cdots x_{n,a_n}$ 的形式，其中 $a \in \{0,1\}^n$.。已知 [Nis91]，如果 P 有一个大小为 s 的“简单”[2] 单调非交换电路，那么我们可以

[1]在这个模型中，变量不可交换。[2]这一模型的专业名称是代数分支程序（ABP）。对于一般电路，也可以给出类似但更复杂的分解。

写出

$$P = \sum_{i=1}^{s} Q_i \cdot R_i$$

其中每个 Q_i 依赖于变量的前半部分（$x_{j,\ b}$ 对于 $j \in [n/2]$），而 R_i 依赖于后半部分，并且所有多项式都是单调的。这类似于通信复杂度中的情形：我们可以用一个规模较小的双边通信协议来计算函数f：$\{0,1\}^{n/2} \times \{0,1\}^{n/2} \to \{0,1\}$ 从而将 f分解为少量布尔（因此非负的）矩形。[HY13] 的工作展示了如何利用这种联系得到非单调与单调分离。分离实例的灵感来自唯一不相交函数。该函数通过内积有一个简单的代数描述，由此得到一个非单调上界；而下界则运用了 Razborov 关于这一问题通信复杂度下界的思想 [Raz92] 。

我们的设置是标准的交换设置，这意味着我们得到与上述类似的分解，只不过每个 Q_i 依赖于变量的一半（但具体是哪一半未知）（更准确地说，对于某个 $j \in S_i$，有 $|S_i| = n/2$）x_{jb} 。此时，类比对象不再是标准通信复杂度模型，而是多分区通信复杂度模型；在该模型中，分解里的每个矩形都可以使用不同的输入划分。此前的研究已考察过这一模型及其变体，包括 [ˇD HJ04、Hay11、HY16]。尤其是 [Hay11、Juk15、HY16] 的工作发现了一种技术：通过使用扩展图定义困难函数（针对标准通信模型）的变体，将标准通信复杂度中的某些结构化下界“提升”到多分区设置中。特别是，唯一不相交函数的下界适用于这种提升技术。式 (1) 中定义的多项式 P_n 是这个提升后的布尔函数的一个代数变体（类似于 [HY13] 的分离实例与唯一不相交函数之间的关系）。下界论证结合了唯一不相交函数的非确定性通信复杂度下界（这是 Razborov 的结果，但我们使用 [KW15]给出的一个版本）。为了提升下界，我们需要构造一个能够进行覆盖论证的困难分布。这个困难分布运用了一些来自 [Sri20]的思想。

为了得到常数次数多项式的分离（从而解决 [SY10] 中的未决问题），我们使用填充论证。变量 P_n 自然地分成 n 组，每组包含 2 个变量。我们将这些组收集到 k 个桶中，每个桶包含 n/k 组。现在，每组有 $2^{n/k}$ 个可能的单项式，我们定义一个新的多项式 Q_k，并将这些单项式视为变量。很容易看出，Q_k 至少与 P_n 一样难，因为 Q_k 的电路很容易通过将 Q_k 中的每个变量替换为对应的单项式，得到 P_n 的电路。不过，反过来就不那么显然了。尽管如此，由于我们针对 P_n 的深度为 3 的非单调电路非常简单，我们也能够修改这一构造，得到一个规模和深度都较小的 Q_k 非单调电路。

算术与布尔上界。 为证明定理1.4 和1.5，我们考虑与满秩向量集对应的多项式和布尔函数。设 M 是一个 $r \times n$ 域上的矩阵 $\mathbb{F}$。我们将同时考虑域为有限域的情形以及 $\mathbb{R}$。对于 $S \subseteq [n]$ 的列的任意子集 M，设 $M[S]$ 是 M 限制在 S中的列所得的限制。令f_M：$\{0,1\}^n \to \{0,1\}$ 是与 M相关联的单调布尔函数，定义为

$$f_M(x) = 1 \text{ iff the matrix } M[S] \text{ has full rank,}$$

其中 $S = \{i \in [n] : \ x_i = 1\}$ 是 M 的列集合， x 表示该集合满足的条件。等价地，函数f_M（x）当且仅当线性方程组 $y^{\mathsf{T}} M[S] = 0$有唯一解时取值为 1。该函数可由规模和深度为 $O(\log n)^2$ [ABO99、Mul87]的布尔电路计算。

Whe对于 $\mathbb{F} = \mathbb{R}$，我们还通过以下方式将一个 n 元多线性多项式 P_M 与 M 关联起来：

$$P_M(x) := \sum_{\substack{S \subseteq [n]: \\ |S| = r}} \det(M[S])^2 \cdot \prod_{i \in S} x_i. \tag{2}$$

对于 $x \in \{0,1\}^n$，可知 $P_M(x) > 0$ 当且仅当 $f_M(x) = 1$。柯西–比内公式使我们能够通过非单调电路（且深度为多对数级）高效计算 P_M。由此得到我们的算术非单调上界。

人们很容易想到，尝试用 [GKRS18、CGR+25]中所考虑的那类函数来推导我们的分离性。这些函数对应于判断某个线性方程组是否有解。具体而言，存在一个隐式矩阵 M，其定义在域 $\mathbb{F}$上，而输入字符串被解释为对 S 中 M各列的一个子集进行编码。若 $M[S]$ 张成一个固定的目标向量 $v \neq 0$，则该函数接受输入。然而，与和行列式多项式紧密相关的满秩性质不同，我们似乎无法将这种张成限制与一个可高效构造的多项式联系起来。此外，满秩向量集是一个向量空间（也因此是一个拟阵）的基，但对于张成 v的向量，情况并非如此。这对我们解决 [JS20]中的问题 1 至关重要。

最后，正如我们在开放问题一节中所讨论的，函数 f_M 可以通过一种鲜有研究的单调计算模型来计算，我们将其称为单调秩程序。这类程序是单调跨度程序的限制，而单调跨度程序是一种得到广泛研究的单调计算模型 [KW93、BGW99]，可计算 [GKRS18、CGR+25] 中的函数，并且等价于线性秘密共享方案 [Bei11]。单调秩程序可能远弱于单调跨度程序，就像单调依赖程序（单调跨度程序的另一种限制） [PS96]一样。如果确实如此，那么我们的工作就将针对单调跨度程序所证明的指数级单调电路下界 [GKRS18] 扩展到了更简单的计算模型。

单调布尔下界。现在我们讨论本文中的单调布尔电路下界。回顾上文，存在一个固定矩阵 $r \times n$ M，我们希望为布尔函数 f_M 证明一个下界： $\{0,1\}^n \to \{0,1\}$ 该函数判断给定的 M 的列的子集是否满秩。

为了证明这样的下界，我们采用 Razborov 的近似技术 [Raz85]，该技术多年来经过了多次改进 [AB87、Ros14、CKR22、CGR+25]。基于这些成果，我们将近似方法应用于单调布尔电路下界时的核心思想提炼出来，形成下面一个一般且简洁的陈述（定理 3.3）。粗略地说，该陈述指出，要证明布尔函数 f的单调电路下界，只需构造两个分布 $\mathcal{D}_0$ 和 $\mathcal{D}_1$，使它们分别支撑在 f 的 0 和 1 上，并满足两个条件：

- （ $\mathcal{D}_1$的扩散性）：在$\mathcal{D}_1$ 下，任意 w 个变量同时取值为 1 的概率至多为q^{-w} （其中 q 和 w 尽可能大）。

- （$\mathcal{D}_0$的鲁棒向日葵）：大小为 s^k 的任意 w-析取范式都包含一个子集，该子集相对于 $\mathcal{D}_0$是一个鲁棒向日葵。通俗地说，这是一组项，可以将其替换为单个项，而不会显著改变该析取范式在来自 $\mathcal{D}_0$.的输入上的表现。

由这两个条件得到的下界大约是 $(q/s)^w$.从高层次来看， $\mathcal{D}_1$ 的扩散性意味着它支撑在低重量的字符串上，而 $\mathcal{D}_0$ 的向日葵性质意味着它支撑在高重量的字符串上。根据 f的单调性，这些重量“恰恰与应有的相反”； f 中的 1 应该比 f中的 0 更靠后。

要将这一技巧用于 f_M，我们需要定义这些分布，而这些分布又取决于 M.的选择。最简洁的例子是 $\mathbb{F}_2$上的随机 $r \times n$矩阵，其中 $r \approx n^{\varepsilon}$。标准计算表明，这样的矩阵满足两个线性代数性质：

- P1： r 列的大多数子集都是线性无关的。~
- P0：所有基数为 $r' = \Omega(r)$的列子集都是线性无关的。

P1 使我们能够轻松得到汉明重量尽可能低的扩展 $\mathcal{D}_1$：只需随机选择一个大小为 r 的子集，并将这些位设为 1。这样得到的扩展分布的扩展参数为 $q \approx (n/r)$。

选择分布 $\mathcal{D}_0$ 稍微棘手一些：为了抽样得到大量线性相关的列，我们随机选取一个向量 $u \in \mathbb{F}_2^r$，并挑出所有与 u. 正交的列。这个分布具有均匀边缘分布（因此汉明重量相对较高），并且根据上面的性质 P0，它也是 r'-wise 独立的。后一性质使我们能够证明 $\mathcal{D}_0$ 的鲁棒向日葵性质：用均匀分布替换 $\mathcal{D}_0$，因为低宽度的析取范式无法区分这两种分布 [（Baz09,—Tal17] ），除非误差达到 $\exp(-\tilde{\Omega}(\sqrt{r'}))$。现在可以利用关于乘积分布的鲁棒向日葵引理的最新界 [（ALWZ21，BCW21，Rao25] ），用参数 $s \approx \sqrt{r'}$ 论证所需性质。优化参数后，选择 r 为 $r \approx n^{2/3}$，从而得到 $\exp(n^{1/3})$ 的下界 $\approx$。有趣的是，这是首次运用 Bazzi 定理证明单调电路下界。

我们注意到，Bazzi 定理是我们的下界中唯一的额外开销；否则，我们本可以达到已知最佳的、针对一个 **NP** 函数（$\approx \exp(n^{1/2})$ [CKR22]）的单调电路下界。尽管如此，通过 Bazzi 定理将问题归约到鲁棒向日葵引理，比通过匹配向日葵的“块状”族进行归约更有效；后者来自 [CGR+25], 给出了一个针对 **NC** 函数的更高阶下界（他们的下界为 $\approx \exp(n^{1/6})$ 。另一方面，他们的上界更好（该函数属于 **L**），因此这些结果很难说孰优孰劣。

为了获得具有上述性质的显式矩阵，我们采用具有足够大距离和对偶距离的二元线性码构造。将性质 P0 和 P1 转换为编码理论的表述后，我们可以通过证明该码的对偶距离至少为 r'来得到 P0，并通过证明其距离足够大来得到 P1。

最后，为了证明算术模型与布尔模型之间的分离，我们需要论证上述下界适用于一个实矩阵 M。一种自然的策略是重复上述论证，例如考虑每列都是独立符号向量 $v \in \{-1, 1\}^r$的随机矩阵 $\mathcal{D}_0$ 。然而，这会导致一个问题：无法像上面那样定义分布 [LO43，Erd45],，因为按此方式采样得到的点不太可能具有较大的汉明重量（根据标准的反集中论证，两个随机符号向量正交的概率很小），因此 $\mathcal{D}_0$ 其边缘分布很小。

我们需要有很多实向量，使得它们的许多子集都线性相关。如何做到这一点？主要思路是选择一个稀疏矩阵。我们对每一列进行采样，使其成为 M 一个

汉明重量较低的随机布尔向量。这样就得到一个分布 $\mathcal{D}_0$ 它具有更高的边缘分布，并满足有界独立性的一种较弱形式。遗憾的是，我们无法将这种较弱形式与最强的鲁棒向日葵引理结合起来使用。不过，我们可以将它与经典向日葵引理搭配使用 [ER60] 从而证明一个超多项式下界 `类似于 Razborov [Raz85]（而不是指数下界）。

汉明球与子空间。在证明 $\mathcal{D}_1$的扩展性时，我们证明了一个关于子空间与布尔立方体交模式的技术性结果，我们认为该结果本身也很有趣。设 $\mathbb{F}$ 是任意一个域，且 V 是 $\mathbb{F}^n$ 的一个维数为d的子空间。一个标准事实是 $|V \cap \{0,1\}^n| \leq 2^d$(例如参见 [AY24]）。我们将这一界从完整的汉明立方体推广到半径为 s的汉明球。我们证明， s 中汉明重量至多为 V 的布尔立方体点的数量至多为 $\binom{d}{\leq s}$. 很容易看出，这些界在由以下向量生成的向量空间 V d 中都是紧的：标准基向量。

1.3 开放问题

单调秩程序的威力。大小为 k 、定义在域$\mathbb{F}$ 上的单调张成程序，是一个 $\mathbb{F}$矩阵 A，包含 k 行，并为每一行标记一个来自$\{x_1, \ldots, x_n\}$的输入变量。若由 $x \in \{0,1\}^n$ 满足的变量所标记的行构成的集合 A_x所张成的空间包含向量 x，则该张成程序接受二进制串 $e_1 = (1, 0, \ldots\ldots, 0)$（通过适当的换基，也可以选取任意其他向量）。存在一个线性规模的单调张成程序，可以计算 [GKRS18、CGR+25]中的函数。利用标准技巧，也不难用单调张成程序计算 f_M。

有趣的是，函数 f_M 也可以通过一种看似更简单的单调模型来计算，我们将其称为 单调秩程序。与单调张成程序一样，单调秩程序是一个矩阵 A，其行带有标记。区别在于，当且仅当 x 的 A_x 满秩时，单调秩程序才接受输入。线性秘密共享方案领域也研究过这类模型 [NNP04]，并将其称为“非冗余”，因为对于任何最小接受的 A_x，其中都不存在依赖关系 x。

一种相关模型称为单调依赖程序，当且仅当 x 的 A_x 线性相关时才接受输入。这已被证明比单调张成程序弱指数级 [PS96]。单调秩程序是否弱于单调张成程序，仍是一个未解决的问题。

平面图上匹配的单调复杂度。 要证明计算复杂性上的分离，需要分两步。我们有两个计算类 A和 B，并需要找出一个问题 P，它属于 B 但不属于 A。在我们的语境中， A 是单调类，而 B 是非单调类。我们使用了通信复杂度中的技术 [Raz92、KW15] 以及近似方法 [Raz85]，以证明针对 A的下界。为了证明 P 属于 B，我们使用了带否定的深度 3 电路的威力，或者线性代数的威力。

证明分离性还有另一条不同的路径。在他的工作中， [Val80], Valiant 利用了这样一个事实：平面图中的完美匹配数量由 Pfaffian 给出 [Kas67] 因此，我们可以将其归约为计算行列式多项式。同样，上界来自线性代数。Valiant 证明了，对于某些平面图，Pfaffian 可以由多项式规模的非单调算术电路计算；更准确地说，可以由代数分支程序计算

其规模为多项式。但我们感兴趣的是分离布尔单调电路和算术非单调电路。我们知道上界成立，但尚不清楚对于平面图，使用单调布尔电路判定完美匹配问题是否困难。

常数深度分离。 定理 1.1 表明，存在一个可由深度为 3 的算术电路计算、但需要最大单调算术复杂度的多项式，从而改进了此前此类分离性结果 [CDM21]。在布尔情形中，一系列研究 [AG87、Oko82、RW92、GS92、BGW99、COS17、GKRS18、CO23、CGR+25] 直接或间接地研究了常深度电路与单调电路的相对能力。最近的研究发现，存在一个可由常深度电路计算、但需要超多项式规模单调电路的单调函数 [CGR+25]。一个尚未解决的问题是，是否存在某种常深度电路模型（实际上，甚至是 $O(\log n)$ 深度电路）可计算的单调函数，却需要指数规模的单调电路。是否存在一个矩阵 M 使得 f_M 能够展现这种分离性?

从代数分离的角度来看，这类问题也很有趣。是否存在一个多项式 P，它可由常数深度甚至对数深度算术电路计算，并且 f_P 需要超多项式规模、甚至指数规模的单调布尔电路？鉴于近期已有若干非平凡算法通过常数深度算术电路实现，这似乎是可能的 [AW24]。

其他问题。关于我们用于获得这些结果的技术，还有一些更具体的问题：

- 我们能否将第2 节中的下界提高到 $\Omega\left(\binom{n}{k}\right)$，对于一个 n元常数次数多项式 k而言?

- 我们能否使第5 节（定理1.4）中的界达到指数级？这需要为仅弱独立（按照引理5.11的定义）的分布证明一个更好的鲁棒向日葵引理。一种方法是证明我们的分布能够欺骗低宽度析取范式。值得注意的是，近期研究已揭示了哪些类型的分布能够欺骗析取范式方面的限制 [AGG+25]。

- 我们能否将第 M_n 5节中的矩阵随机选择显式化？在第4节中，我们的构造使用了具有较大距离和对偶距离的二元线性码的显式构造。

- 第5 节中的下界是否也适用于每一列（在 M_n中）仅为 $O(1)$-稀疏的情形?

1.4 致谢

PM、TBF 和 SS 在*2025* 年代数复杂性理论研讨会（*WACT*）期间于波鸿开始合作，并感谢本次研讨会的组织者热情接待。SS 还要感谢 Rohit Gurjar 和 Roshan Raj 指引他关注利用柯西-比内公式得到的、与拟阵相关的多项式恒等式；感谢 Radu Curticapean 与他讨论子图多项式；感谢 Duri Janett 提供与提升定理相关的参考资料；并感谢 Susanna de Rezende 对 [dRV25]给予澄清。BC 感谢英国工程与自然科学研究委员会项目 EP/Z534158/1“计算复杂性综合研究方法：结构、自指与下界”提供的支持。

论文结构。本文其余部分安排如下。定理1.1 和定理1.2 的证明见第2节。第3 节介绍了我们证明布尔单调电路下界所需的框架。定理1.4和定理1.5 的证明分别见第4节和第5 节。

2 算术分离

本节的目标是证明单调与非单调代数电路之间存在强分离性。

2.1 图的多项式及其 $\Sigma\Pi\Sigma$ 上界

令 G 为一个顶点集为 $[n]$的图。用 $E(G)$表示 G的边集，并令 $e(G) := |E(G)|$。令X为变量集 $2n$ 变量 $X := \{x_{1,0}, x_{1,1}, \ldots, x_{n,0}, x_{n,1}\}$。令 P_G为如下定义的非负多项式：

$$P_G := \sum_{a\in\{0,1\}^n} \left(\sum_{\{u,v\}\in E(G)} a_u a_v - 1 \right)^2 \prod_{i=1}^{n} x_{i,a_i}.$$

对于 的每个除数 k n $Q_{k\,G}$ k $k2^{n/k}$ $\{x_{i,a} \mid i \in$，令,为关于变量 、定义 $[k], a \in \{0,1\}^{n/k}\}$ 如下的 次多项式：

$$Q_{k,G} := \sum_{a\in\{0,1\}^n} \left(\sum_{\{u,v\}\in E(G)} a_u a_v - 1 \right)^2 \prod_{i=1}^{k} x_{i,(a_{(i-1)n/k+1},\ldots,a_{in/k})}.$$

注意，$P_G = Q_{n,G}$。反过来，通过应用代换

$$x_{i,a} \leftarrow \prod_{j\in[n/k]} x_{(i-1)n/k+j,a_j} \tag{3}$$

对于多项式 $Q_{k,\ G}$，我们得到多项式 P_G。我们首先证明多项式 $Q_{k,\ G}$的一些上界。

引理 2.1。对于上述所有 G， k ，多项式 $Q := Q_{k,\ G}$ 具有一个大小为 $O(e(G)^2 k 2^{n/k})$ 的 $\Sigma\Pi\Sigma$ 公式。

证明。对于每个 $p \in \mathbb{N}$，令

$$Q_p := \sum_{a\in\{0,1\}^n} \left(\sum_{\{u,v\}\in E(G)} a_u a_v \right)^p \prod_{i=1}^{k} x_{i,(a_{(i-1)n/k+1},\ldots,a_{in/k})}.$$

我们可以将 Q 写成

$$\begin{aligned} Q &= \sum_{a\in\{0,1\}^n} \left(\left(\sum_{\{u,v\}\in E(G)} a_u a_v \right)^2 - 2 \left(\sum_{\{u,v\}\in E(G)} a_u a_v \right) + 1 \right) \prod_{i=1}^{k} x_{i,(a_{(i-1)n/k+1},\ldots,a_{in/k})} \\ &= Q_2 - 2Q_1 + Q_0. \end{aligned}$$

首先,

$$Q_0 = \prod_{i=1}^{k} \left(\sum_{a \in \{0,1\}^{n/k}} x_{i,a} \right).$$

其次,

$$\begin{aligned} Q_1 &= \sum_{\{u,v\} \in E(G)} \sum_{a \in \{0,1\}^n} a_u a_v \prod_{i=1}^{k} x_{i,(a_{(i-1)n/k+1}, \ldots, a_{in/k})} \\ &= \sum_{\{u,v\} \in E(G)} Q_{1,uv} \end{aligned}$$

其中

$$Q_{1,uv} := \sum_{a \in \{0,1\}^n} a_u a_v \prod_{i=1}^{k} x_{i,(a_{(i-1)n/k+1}, \ldots, a_{in/k})}.$$

对于每个 $u \in [n]$, 令 $(i_u,\ j_u) \in [k] \times [n/k]$ 为满足以下条件的唯一一对

$$u = (i_u - 1)n/k + j_u.$$

如果 $i_u \neq i_v$, 则

$$\begin{aligned} Q_{1,uv} = &\left(\sum_{a \in \{0,1\}^{n/k}} a_{j_u} x_{i_u,a} \right) \cdot \left(\sum_{a \in \{0,1\}^{n/k}} a_{j_v} x_{i_v,a} \right) \\ &\cdot \prod_{i \in [k] \setminus \{i_u, i_v\}} \left(\sum_{a \in \{0,1\}^{n/k}} x_{i,a} \right). \end{aligned}$$

如果 $i_u = i_v$, 则

$$Q_{1,uv} = \left(\sum_{a \in \{0,1\}^{n/k}} a_{j_u} a_{j_v} x_{i_u,a} \right) \cdot \prod_{i \in [k] \setminus \{i_u\}} \left(\sum_{a \in \{0,1\}^{n/k}} x_{i,a} \right).$$

第三,

$$Q_2 = \sum_{\{u,v\},\{r,s\} \in E(G)} Q_{2,uv,rs}$$

其中

$$Q_{2,uv,rs} := \sum_{a \in \{0,1\}^n} a_u a_v a_r a_s \prod_{i=1}^{k} x_{i,(a_{(i-1)n/k+1}, \ldots, a_{in/k})}.$$

与上述$Q_{1,uv}$ 情形类似，我们可以使用大小为 $O(k2^k)$的 $\Pi\Sigma$ 单调公式来计算$Q_{2,uv,rs}$ 。■

推论 2.2。　　对于所有如上所述的 G ， 多项式 P_G 都有一个大小为 $O(e(G)^2 n)$的 $\Sigma\Pi\Sigma$ 公式。

证明。 根据引理2.1 可得 k 等于 n。 ■

2.2 单调算术复杂度与通信复杂度

我们的单调算术电路下界基于通信复杂度。这种联系已在多项工作中得到运用 [RY11，Juk15，Sri20]。我们首先定义布尔函数的多划分矩形数，并证明（以求完整）它与多项式的单调算术复杂度之间的关系。

设 X 是一个有限集。若存在 X 的一个划分 $\{Y, Z\}$，使得

$$R = \{\, S \cup T \mid S \in \mathcal{Y}, T \in \mathcal{Z} \}$$

对于某个 $\mathcal{Y} \subseteq \mathcal{P}(Y)$ 和 $\mathcal{Z} \subseteq \mathcal{P}(Z)$ 成立，则称 $Y(\mathcal{Z} \subseteq \mathcal{P})$ 是一个矩形。若 $|Y|,\ |Z| \in [1/3, 2/3) \cdot |X|$，则称矩形是平衡的。对于每个 $a \in \{0,1\}^n$，令

$$\mathrm{supp}(a) := \{\, i \in [n] \mid a_i = 1 \}$$

对于 $S \subseteq \{0,1\}^n$，令

$$\mathrm{supp}(S) := \{\, \mathrm{supp}(a) \mid a \in S \} \subseteq \mathcal{P}([n]).$$

f 的多划分矩形数$\mathrm{mprn}(f)$：$\{0,1\}^n \to \{0,1\}$ 是满足以下条件的最小数 r：存在一个由关于 $[n]$ 的平衡矩形组成的族 $\{R_i\}_{i \in [r]}$，使得

$$\mathrm{supp}(f^{-1}(1)) = \bigcup_{i \in [r]} R_i.$$

算术复杂度与矩形数之间的联系如下所述。设 $X := \{x_1, \ldots, x_m\}$，并设 $\mathcal{X} := \{X_1, \ldots, X_n\}$ 是将 X 划分为 n 个部分的一个划分。若多项式 P 的每个单项式对于每个 $i \in [n]$ 都恰好含有 X_i 中的一个元素，则称该多项式为 $\mathcal{X}$-集合多线性的。若多项式对 $(g,\ h)$ 关于 $\mathcal{X}$ 是一个单调对，则存在 X 的一个划分 $\{Y, Z\}$，使得 $\mathcal{X}$ 是 $\{Y, Z\}$ 的细化，并且 $g \in \mathbb{R}[Y]$ 和 $h \in \mathbb{R}[Z]$ 以及 g 和 h 是单调多项式。若非负对 $(g,\ h)$ 满足 $|\mathcal{X}_Y|$，$|\mathcal{X}_Z| \in [1/3, 2/3) \cdot |\mathcal{X}|$，且对于每个 $W \subseteq X$，则称其为平衡的。

$$\mathcal{X}_W := \{\, B \in \mathcal{X} \mid B \subseteq W \}.$$

换句话说，$\mathcal{X}$ 中每个 Y，Z 的部分数量是平衡的。

下面的结构引理已在 [RY11] 中针对一般的（不一定是集合多线性的）单调电路得到证明，并在 [Yeh19] 中针对有序多项式得到证明。下面针对集合多线性情形的证明基本相同。

引理 2.3。如果 P 是一个由大小为 s 的单调电路计算的单调 $\mathcal{X}$-集合多线性多项式，那么存在一个平衡单调对 $\{(g_i,\ h_i)\}_{i \in [s]}$ 的族，使得

$$P = \sum_{i \in [s]} g_i h_i,$$

并且每个乘积 $g_i h_i$ 只包含来自 P的单项式。

证明略述。简而言之，该证明利用了这样一个事实：计算集合多线性多项式的单调电路在语法上是集合多线性的；然后，通过对边数进行归纳，并找出一个计算平衡对的乘积门，即可得到该引理。■

现在，令 X 为 $2n$ 变量的集合 $X := \{x_{1,0}, x_{1,1}, \ldots, x_{n,0}, x_{n,1}\}$，并令 $\mathcal{X} := \{X_1, \ldots, X_n\}$ 为其划分，其中 $X_i := \{x_{i,0}, x_{i,1}\}$。对于任意 $\mathcal{X}$-集合多线性单项式 $m := \prod_{i=1}^{n} x_{i,\ a_i}$，令

$$\mathcal{A}(m) := \{\, i \in [n] \mid a_i = 1\}.$$

对于一个 $\mathcal{X}$-集合多线性多项式 P，令

$$\mathcal{A}(P) := \{\, \mathcal{A}(m) \mid m \in \mathrm{supp}(P)\} \subseteq \mathcal{P}([n]).$$

引理 2.4. 设 $f\colon \{0,1\}^n \to \{0,1\}$，并设 P 是一个单调的 $\mathcal{X}$-集合多线性多项式。若 $\mathrm{supp}(f^{-1}(1)) = \mathcal{A}(P)$，则

$$\mathrm{S}^{+}(P) \geq \mathrm{mprn}(f).$$

证明。设 C 是一个大小为 s、计算 P 的单调电路。根据引理 2.3，我们知道存在一个由平衡单调对构成的族 $\{(g_i,\ h_i)\}_{i\in[s]}$，使得

$$P = \sum_{i\in[s]} g_i h_i.$$

对 P 的这种分解意味着其支撑集有如下分解

$$\mathrm{supp}(P) = \bigcup_{i\in[s]} \{\, m_1 m_2 \mid m_1 \in \mathrm{supp}(g_i), m_2 \in \mathrm{supp}(h_i)\}.$$

因此，我们得到如下分解

$$\mathcal{A}(P) = \bigcup_{i\in[s]} \{\, \mathcal{A}(m_1) \cup \mathcal{A}(m_2) \mid m_1 \in \mathrm{supp}(g_i), m_2 \in \mathrm{supp}(h_i)\},$$

根据假设，这意味着

$$\mathrm{supp}(f^{-1}(1)) = \bigcup_{i\in[s]} \{\, \mathcal{A}(m_1) \cup \mathcal{A}(m_2) \mid m_1 \in \mathrm{supp}(g_i), m_2 \in \mathrm{supp}(h_i)\}.$$

最后一个观察是，对于任意平衡单调对（$g,\ h$），集合

$$R := \{\, \mathcal{A}(m_1) \cup \mathcal{A}(m_2) \mid m_1 \in \mathrm{supp}(g), m_2 \in \mathrm{supp}(h)\}$$

是 $[n]$的一个平衡矩形。结合上述分解，即可完成引理的证明。

■

2.3 多划分通信复杂度下界

在本节中，我们证明多划分通信复杂度下界，进而推出单调电路下界。我们所考虑的问题定义在一个图 G上，其顶点集为 $[n]$。对于 G的顶点的一个子集 U，我们将 G 在U上的诱导子图记为 $G[U]$。记 $f_G\colon \{0,1\}^n \to \{0,1\}$ 为如下定义的函数：

$$f_G(a) = 1 \iff e(G[\mathrm{supp}(a)]) \neq 1.$$

注意，多项式 P_G 的支集与 $f_G^{-1}(1)$ 相同。

只要 G 是一个扩展图，我们的下界就成立，因为这是 [Sri20], 中的引理 9 所要求的，我们将其重述为引理 2.7。具体而言， [Sri20] 所采用的扩展图定义是： G 是一个 d-正则图，其邻接矩阵的第二大特征值至多为 $d^{0.75}$。我们的主要引理如下。

引理 2.5。 若 G 是一个顶点集为 $[n]$的扩展图，则

$$\mathrm{mprn}(f_G) \geq 2^{\Omega(n)}.$$

下界的主要组成部分是以下类似通信复杂度下界的引理。它可以从通信复杂度的角度推导自 Kaibel 和 Weltge 的一项结果 [KW15]; 参见 Roughgarden 的讲义 [Rou15]中的引理 5.10。

引理 2.6。 对于 $\ell \in \mathbb{N}$，我们定义 2ℓ元异于 *1* 的不相交函数$\mathrm{DISJ}_\ell^{\neq 1}$ 如下：

$$\mathrm{DISJ}_\ell^{\neq 1}(b_1 \ldots, b_\ell, c_1, \ldots, c_\ell) = 1 \Leftrightarrow |\mathrm{supp}((b_1, \ldots, b_\ell)) \cap \mathrm{supp}((c_1, \ldots, c_\ell))| \neq 1.$$

令 $\ell \in [n]$ 和 $g := \mathrm{DISJ}_\ell^{\neq 1}$ 。对于每个 $i \in [\ell]$，从集合 $\{(0, 0), (1, 0), (0, 1)\}$ 中独立且均匀随机地选取一个元素 $(b_i, b_{\ell+i})$，并令 $b := (b_1, \ldots, b_{2\ell})$ 为相应的、定义在 2ℓ 个变量上的随机赋值。若 R 是一个划分为 $\{\{1, \ldots, \ell\}, \{\ell+1, \ldots, 2\ell\}\}$ 的 $[2\ell]$ 矩形，且满足 $R \subseteq \mathrm{supp}(g^{-1}(1))$，则

$$\Pr_b[b \in R] < 2^{-\ell/2}.$$

证明。 正如笔记中引理 5.10 的证明所示 [Rou15] 适用于任何唯一不相交性 1-矩形，因此，由于任何异于 1 的不相交函数 1-矩形也都是唯一不相交性 1-矩形，便可得出本引理。 ■

接下来，我们需要在 $f_G^{-1}(1)$ 上定义一个“困难分布”，使得包含在 $f_G^{-1}(1)$ 中的所有平衡 1-矩形的测度都很小。虽然函数 f_G 与异于 1 的不相交函数有些相似，但这并不能直接由上面的引理推出，因为我们事先并不知道需要处理的划分。

考虑以下算法，它在 [Sri20], 中定义，用于从 G中抽取一个随机匹配：对于 $m \in [n]$ 作为给定输入，

1. 令 $M \leftarrow \varnothing$。
2. 对于 $i = 1, 2, \ldots, m$，执行以下操作：
   (a) 从 G 中移除所有与 M 中任意顶点的距离至多为 2 的顶点。令 G_i 为所得图。(b) 从 $E(G_i)$ 中均匀随机选取一条边 e_i ，并将其添加到 M。
3. 输出 M。

现在给定一个匹配的 M，我们使用以下过程来定义一个随机输入 $a \in \{0,1\}^n$ tof_G:

1. 对于每个 $u \in [n] \setminus V(M)$，设定 $a_u = 0$。

2. 对于每个 $\{u, v\} \in M$，从 $\{(0,\ 0)、(1,\ 0)、(0,\ 1)\}$ 中独立且均匀地随机选择一个元素 $(a_u,\ a_v)$。

注意，$e(G[\mathrm{supp}(a)]) = 0$ 根据我们对 a 的选择，这意味着上述过程在 $f_G^{-1}(1)$ 上定义了一个概率分布。因此，引理 2.5 立即可由以下断言推出：对于每个平衡矩形 $R \subseteq f_G^{-1}(1)$，

$$\Pr_a[\mathrm{supp}(a) \in R] \leq 2^{-\Omega(n)}.$$

因此，只需证明这个不等式。

随机输入 a 的有用性质依赖于随机匹配 M 的以下性质；这些性质已在 [Sri20] 的引理 9 中陈述。

引理 2.7。如果 G 是一个扩展图，其顶点集为 $[n]$，那么存在一个常数 $\alpha > 0$，使得对于$m := \lceil \alpha n \rceil$，并且对于使用 m 作为输入、通过上述算法采样得到的随机匹配 M，以下结论成立：

1. M 是一个基数为 m的诱导匹配。

2. 对于 $[n]$的每个平衡划分 $\{A, B\}$，

$$\Pr_M[|M \cap E_G(A, B)| \leq \gamma m] \leq \exp(-\gamma m),$$

对于某个绝对常数 $\gamma > 0$。

设 $\{A, B\}$ 是一个有效划分，它证明了 R 是一个基数为 $[n]$的平衡矩形。根据引理 2.7，我们知道 M 是一个基数为 G 的诱导匹配，并且，以至少 $1 - 2^{-\Omega(n)}$的概率，有

$$|M \cap E_G(A, B)| \geq \gamma m =: s'.$$

对于一个固定的诱导匹配

$$E := \{\{u_1, v_1\}, \ldots, \{u_s, v_s\}\} \subseteq E(G)$$

对于每个 $i \in [s]$，当 $s \geq s'$ 和 $u_i \in A$ 和 $v_i \in B$ 时，我们以随机匹配 M 满足以下条件为条件

$$M \cap E_G(A, B) = E.$$

现在我们可以定义以下随机变量：对于每个 $i \in [s]$，令

$$b_i := a_{u_i} \text{ and } b_{s+i} := a_{v_i},$$

其中 $a \in \{0, 1\}^n$ 是与 M 关联的随机赋值。令

$$b := (b_1, \ldots, b_{2s})$$

是根据上述定义得到的随机 $2s$ 变量布尔赋值。根据赋值 a 的定义，我们得到每一对 $(b_i,\ b_{s+i})$ 都是独立且均匀地选取的，

从集合 $\{(0,\ 0),\ (1,\ 0),\ (0,\ 1)\}$ 中随机选取。令 g 为 $2s$ 元异于 1 的不相交函数。我们观察到

$$f_G(a) = 1 \iff g(b) = 1$$

对于上述赋值 a 和 b 。另请注意， b是对 g 的一个随机赋值，满足引理 2.6的假设，并且 $\mathrm{supp}(a) \in R$ 蕴含 $\mathrm{supp}(b) \in R_E$，其中

$$R_E := \{\, S \cup T \mid S \subseteq \{1,\dots,s\}, T \subseteq \{s+1,\dots,2s\}, (\{\, u_i \mid i \in S\} \cup \{\, v_{i-s} \mid i \in T\}) \in R\}.$$

由于 R是一个划分为 $\{A, B\}$ 的矩形，且我们有 $\{\, u_i \mid i \in S\} \subseteq A$和 $\{\, v_{i-s} \mid i \in T\} \subseteq B$，因此 R_E是一个划分为 $\{\{1,\dots,s\},\{s+1,\dots,2s\}\}$的 $[2s]$ 矩形。此外，我们有$R_E \subseteq \mathrm{supp}(g^{-1}(1))$，因为任意 $S \cup T \in R_E$ 都满足

$$\{\, u_i \mid i \in S\} \cup \{\, v_{i-s} \mid i \in T\} \in R \subseteq \mathrm{supp}(f^{-1}(1)),$$

这意味着 $g(1_S,\ 1_T) = 1$，其中我们将 S和 T分别视为对应的示性向量。

因此， R_E 是一个满足引理 2.6假设的矩形，因此我们可以应用该引理得到

$$\Pr_a[b \in R_E] \le 2^{-\Omega(s)} = 2^{-\Omega(n)},$$

这意味着

$$\begin{aligned}\Pr_{M,a}[a \in R \mid M \cap E_G(A,B) = E] &\le \Pr_{M,a}[b \in R_E \mid M \cap E_G(A,B) = E] \\ &= \Pr_a[b \in R_E] \le 2^{-\Omega(n)}.\end{aligned}$$

因此，我们得到

$$\begin{aligned}\Pr_{M,a}[a \in R] &= \Pr_{M,a}[a \in R, |M \cap E_G(A,B)| < s'] \\ &\quad + \sum_{E \subseteq E(G): |E| \ge s'} \Pr_{M,a}[a \in R \mid M \cap E_G(A,B) = E] \cdot \Pr_M[M \cap E_G(A,B) = E] \\ &\le 2^{-\Omega(n)}.\end{aligned}$$

2.4 单调算术电路下界

现在来证明我们的单调算术电路下界。

推论 2.8 (定理 1.1)。 若 G 是一个 n顶点扩展图，则 $\mathsf{S}^+(P_G) \ge 2^{\Omega(n)}$。

证明。 我们有

$$\begin{aligned}\mathcal{A}(P_G) &= \left\{ \mathcal{A}\left(\prod_{i=1}^n x_{i,a_i}\right) \,\middle|\, a \in \{0,1\}^n, \sum_{\{u,v\} \in E(G)} a_u a_v \ne 1 \right\} \\ &= \{\, \mathrm{supp}(a) \mid a \in \{0,1\}^n, e(G[\mathrm{supp}(a)]) \ne 1\} \\ &= \mathrm{supp}(f_G^{-1}(1)),\end{aligned}$$

因此，根据引理 2.4 和 2.5，我们得到

$$\mathrm{S}^{+}(P_G) \geq \mathrm{mprn}(f_G) \geq 2^{\Omega(n)}.$$

■

推论 2.9（定理 1.2）。设 $k \in \mathbb{N}$ 且 $n \in \mathbb{N}$。设 G 是一个具有 nk 个顶点的图。如果 G 是一个扩展图，那么

$$\mathrm{S}^{+}(Q_{k,G}) \geq (m/k)^{\Omega(k)},$$

其中 $m := k2^n$ 是次数为 k 的多项式 $Q_{k,\ G}$中的变量数。

证明。通过代换（公式 3），我们可以将任意一个规模为 s 、计算$Q_{k,\ G}$ 的单调电路转换为一个规模为 $s + O(mn)$ 的单调电路，该电路计算 P_G。因此，根据推论 2.8，我们有 $2^{\Omega(nk)} \leq s + O(mn)$，所以

$$s \geq 2^{\Omega(nk)} = (2^n)^{\Omega(k)} = (m/k)^{\Omega(k)}.$$

因此，我们得到

$$\mathrm{S}^{+}(Q_{k,G}) \geq (m/k)^{\Omega(k)}.$$ ■

3 单调布尔电路下界的一个判据

这里的目标是描述一种判据，用于证明函数 $f\colon \{0,1\}^n \to \{0,1\}$ 的单调布尔电路下界。该判据基于存在满足某些性质的分布 $\mathcal{D}_0$和 $\mathcal{D}_1$，它们定义在 $\{0,1\}^n$ 上。我们先介绍两个重要的定义。

定义 3.1（向日葵）。对于 $S \subseteq [n]$，令 t_S 表示函数

$$t_S(x) := \bigwedge_{i \in S} x_i$$

其中约定 $t_\varnothing \equiv 1$。

如果 $|\mathcal{S}| \geq 2$ 且，那么集合族 $\mathcal{S} \subseteq \mathcal{P}([n])$ 称为一个 $(\mathcal{D}, \varepsilon)$-向日葵

$$\Pr_{x \sim \mathcal{D}} \left[\exists S \in \mathcal{S} : t_{S \setminus K}(x) = 1\right] > 1 - \varepsilon, \tag{4}$$

其中 $K := \bigcap_{S \in \mathcal{S}} S$。如果对于每个 $S \in \mathcal{S}$，都有 $|S| = \ell$，则称族 $\mathcal{S}$ 是 ℓ-均匀分布的。令 $r(\mathcal{D}, \ell, \varepsilon)$ 为最小整数 r，使得每个大小至少为 r^ℓ 的 ℓ-均匀分布集合族都包含一个 $(\mathcal{D}, \varepsilon)$-向日葵（如果不存在这样的 r，则 ∞）。◀

定义 3.2（扩展）。对于整数 t 和 $q > 0$，若分布 $\mathcal{D}$ 在 $\{0,1\}^n$ 上满足：对于每个满足 $|A| \leq t$ 的 $A \subseteq [n]$，

$$\Pr_{x \sim \mathcal{D}}[t_A(x) = 1] \leq q^{-|A|}.$$

◀

我们证明，函数 f 的单调电路下界：$\{0,1\}^n \to \{0,1\}$ 可直接由接受输入的分布 $\mathcal{D}_1$ 的扩展性界，以及拒绝输入的分布 $\mathcal{D}_0$ 的向日葵界推出。

定理 3.3（下界判据）。设 $n \in \mathbb{N}$，且 $f\colon \{0,1\}^n \to \{0,1\}$ 是一个单调函数。设 $t \in \mathbb{N}$ 和 $q \in$（0，1）。设 $\mathcal{D}_0$，$\mathcal{D}_1$ 是定义在 $\{0,1\}^n$ 上的分布，使得 $\mathcal{D}_1$ 是 t-重q-扩展的，并且

$$\alpha := \min\left\{ \Pr_{x\sim\mathcal{D}_0}[f(x)=0],\ \Pr_{x\sim\mathcal{D}_1}[f(x)=1] \right\}.$$

令 $w \in \mathbb{N}$ 满足 $w \le t/2$，并定义

$$r_w := \max_{\ell\in[2w]} r(\mathcal{D}_0, \ell, \alpha n^{-3w}).$$

若 $8r_w \le q \le r_w n$，则任何计算 f 的布尔单调电路，其规模至少为

$$\left(\frac{c\alpha q}{r_w}\right)^w$$

其中 c 是一个普适正常数。

我们使用 Razborov 的近似方法证明定理 3.3 [Raz85]，，将近期研究中“定制向日葵”的方法加以推广 [CKR22、BM25、CGR+25]，该方法最初见于 [Ros14]。此前，[Cav20、BM25]中已出现过一些向日葵判据。我们对该方法的介绍与 [CGR+25]类似，不同之处在于我们考虑任意分布。以下是主要引理。

引理 3.4. 设 $n \in \mathbb{N}$，且 $f\colon \{0,1\}^n \to \{0,1\}$ 是一个单调函数。设 $t \in \mathbb{N}$ 和 $q \in$ 属于 (0，1)。设 $\mathcal{D}_0$，$\mathcal{D}_1$ 是定义在 $\{0,1\}^n$ 上的分布，满足 $\mathcal{D}_1$ 是 t-wise q-扩展，且对每个 $i \in \{0,1\}$，supp($\mathcal{D}_i$) $\subseteq f^{-1}(i)$。设 $w \in \mathbb{N}$ 满足 $w \le t/2$，并定义

$$r_w := \max_{\ell\in[2w]} r(\mathcal{D}_0, \ell, n^{-3w}).$$

如果 $8r_w \le q \le r_w n$，那么计算 f 的任何布尔单调电路的规模至少为

$$\left(\frac{cq}{r_w}\right)^w$$

其中，c 是一个普适正常数。

在证明主要引理之前，让我们先利用它来证明定理 3.3。

定理 *3.3* 的证明。对于每个 $b \in \{0,1\}$，我们有 $\Pr_{x\sim\mathcal{D}_b}[f(x)=b] \ge \alpha > 0$。令 $\mathcal{D}_b^*$为在事件 $\mathcal{D}_b$ 条件下的分布 $f(x)=b$。首先，分布 $\mathcal{D}_1^*$ 是 t-wise (αq)-扩展的，因为对于每个 $A \in \binom{[n]}{\le t}$，

$$\Pr_{x\sim\mathcal{D}_1^*}[t_A(x)=1] \le \frac{1}{\alpha}\cdot \Pr_{x\sim\mathcal{D}_1}[t_A(x)=1] \le (\alpha q)^{-|A|}.$$

其次，每个 ($\mathcal{D}_0$，$\alpha\varepsilon$)-向日葵 $\mathcal{S}$ 都是一个 ($\mathcal{D}_0^*$，ε)-向日葵，因为

$$\Pr_{x\sim\mathcal{D}_0^*}\left[\forall S\in\mathcal{S}\ \ t_{S\setminus K}(x)=0\right] \le \frac{1}{\alpha}\cdot \Pr_{x\sim\mathcal{D}_0}\left[\forall S\in\mathcal{S}\ \ t_{S\setminus K}(x)=0\right] < \frac{\varepsilon\alpha}{\alpha} = \varepsilon,$$

因此 $r(\mathcal{D}_0^*,\ \ell,\ \varepsilon) \le r(\mathcal{D}_0,\ \ell,\ \alpha\varepsilon)$。结论现在由引理3.4得出。 ■

在本节余下部分，我们证明引理3.4。设 $\mathcal{D}_0$，$\mathcal{D}_1$，q，t，w，ℓ 满足该引理的假设。我们将 $\mathcal{D}$ 记作分布

$$\mathcal{D} := (\mathcal{D}_0 + \mathcal{D}_1)/2.$$

我们的目标是用一个单调析取范式公式来近似给定的单调电路

$$F_{\mathcal{S}} \coloneqq \bigvee_{S \in \mathcal{S}} t_S$$

对于满足某些性质的给定集合族 $\mathcal{S} \subseteq \mathcal{P}([n])$。

我们称 $F_{\mathcal{S}}$ 为 r-小，如果对于每个 $\ell \in [n]$,

$$|\mathcal{S} \cap \binom{[n]}{\ell}| \leq r^{\ell}.$$

我们称 $F_{\mathcal{S}}$ 具有宽度 w，如果对于每个 $S \in \mathcal{S}$，$|S| \leq w$。最后，如果 $F_{\mathcal{S}}$ 既是 r-小的，又具有宽度 w，则称其为 (w, r)-析取范式。近似方法接下来分以下两步进行。

命题 3.5。存在一个普适常数 $c \in (0,1)$，使得如果一个大小至多为 $(cq/r_w)^w$ 的单调电路计算 f，那么就存在一个 (w, r_w)-析取范式 F，使得

$$\Pr_{x \sim \mathcal{D}}[F(x) = f(x)] \geq 0.9.$$

命题 3.6。对于每个 $\delta \in (0, 1/2)$ 以及每个 $(w, \delta q)$-析取范式 F，我们有

$$\Pr_{x \sim \mathcal{D}}[F(x) = f(x)] \leq 1/2 + 2\delta.$$

在证明这两个论断之前，我们先证明主要引理。

引理 *3.4* 的证明。证明使用了上述两个论断。当 $r_w = \infty$ 时，定理显然成立，因此假设 $r_w < \infty$。假设（反证） f 可以由一个大小为 $\leq (cq/2r_w)^w$ 的单调电路计算，其中 $c > 0$ 是论断 3.5中的常数。由于根据假设 $8r_w \leq q$，论断 3.5 意味着存在一个 $(w, q/8)$-析取范式，使得

$$\Pr_{x \sim \mathcal{D}}[F(x) = f(x)] \geq 0.9,$$

这与论断3.6相矛盾。 ■

命题 3.6 的证明。设 $F \coloneqq F_S$ 是一个 $(w, \delta q)$-析取范式。如果 $F \equiv \mathbb{1}$（即 $\varnothing \in \mathcal{S}$），根据 $\mathcal{D}$ 的定义以及对于每个 $b \in \{0,1\}$，$\mathcal{D}_b$ 的支撑集包含于 $f^{-1}(b)$ 这一事实，该命题显然成立。否则，注意到 $F(x)$ 成立，当且仅当存在 $S \in \mathcal{S}$ 使得 $t_S(x)$ 成立。由于 F 是 δq-小的，宽度为 w，且 $\mathcal{D}_1$ 是 t-wise q-扩展的，并且 $w \leq t/2$，我们有

$$\Pr_{x \sim \mathcal{D}_1}[F(x) = 1] \leq \sum_{k \in [w]} \sum_{S \in \mathcal{S} \cap \binom{[n]}{k}} \Pr_{x \sim \mathcal{D}_1}[t_S(x) = 1] \leq \sum_{k \in [w]} (\delta q)^k q^{-k} \leq 2\delta.$$ ■

命题的证明 3.5。为方便起见，令 $r := r_w$ 并令 $\varepsilon := n^{-3w}$。令 C 为一个大小至多为 $(cq/r)^w$、计算 f 的单调电路，其中 $c > 0$ 待定。我们将从输入门开始，逐门归纳构造一个 (w, r)-析取范式来表示 C，直至到达输出门。每个输入变量本身已经是一个 (w, r)-析取范式。直接组合归纳构造出的 (w, r)-析取范式时，项数可能会增加，进而可能不再满足 r-小这一条件。为了保持析取范式的小规模，我们通过以下步骤近似直接组合的结果。接下来的命题总结了所得析取范式的性质。

算法 1 摘取过程 $\mathsf{pluck}(\mathcal{S})$

1: **当** $\exists \ell \in [2w]$: $|\mathcal{S} \cap \binom{[n]}{\ell}| > r^\ell$ **时**2: 令 $\mathcal{S}' \subseteq \mathcal{S} \cap \binom{[n]}{\ell}$ 为一个 $(\mathcal{D}_0, \varepsilon)$-向日葵，其核为 K3: 令 $\mathcal{S} \leftarrow \{K\} \cup \{S \in \mathcal{S} : K \not\subseteq S\}$4: **结束循环**

注意，由于 r的选取，算法第 2 行总是可行的。

断言 **3.7.** 若 $F_{\mathcal{S}}$ 的宽度为 $2w$，则 $F_{\mathsf{pluck}(\mathcal{S})}$ 是一个具有 $F_{\mathsf{pluck}(\mathcal{S})} \geq F_{\mathcal{S}}$ 个成员的 $(2w, r)$-析取范式 d

$$\Pr_{x \sim \mathcal{D}_0}[F_{\mathsf{pluck}(\mathcal{S})}(x) > F_{\mathcal{S}}(x)] \leq n^{-w}.$$

证明。由于核 K 包含于 $\mathcal{S}'$ 和 $|\mathcal{S}'| > 1$中的所有集合，因此在第 3 行，$\mathcal{S} \cap \binom{[n]}{\ell}$ 的大小必然会减小，最终我们会得到一个 r-小族。因此，由于 $\mathcal{S}$ 的宽度为 $2w$，算法至多经过 $\sum_{i=0}^{2w} \binom{n}{i} \leq n^{2w}$ 次迭代便会结束。由此可知，$F_{\mathsf{pluck}(\mathcal{S})}$ 是一个 $(2w, r)$-析取范式。

由于核属于向日葵中的所有集合，我们得到 $F_{\mathsf{pluck}(\mathcal{S})} \geq F_{\mathcal{S}}$。接下来需要界定第 3 行中 $\mathcal{D}_0$ 上产生的误差。只有当 $t_K(x) = 1$ 且对所有 $S \in \mathcal{S}$，都有 $t_S(x) = 0$ 时，才会产生这种误差。因此，单次迭代（摘取向日葵）产生的误差可界定为

$$\Pr_{x \sim \mathcal{D}_0}[F_{\mathsf{pluck}(\mathcal{S})}(x) > F_{\mathcal{S}}(x)] \leq \Pr_{x \sim \mathcal{D}_0}[\forall S \in \mathcal{S},\ t_{S \setminus K}(x) = 0] \leq \Pr_{x \sim \mathcal{D}_0}[\forall S \in \mathcal{S}',\ t_{S \setminus K}(x) = 0] < \varepsilon,$$

因为 $\mathcal{S}'$ 是一个 $(\mathcal{D}_0, \varepsilon)$-向日葵。迭代次数至多为 n^{2w}，且 $\varepsilon = n^{-3w}$，因此总误差至多为 n^{-w}。■

如上所述，每个输入门本身就是一个 (w, r)-析取范式。按照电路顺序逐个考察电路中的门，我们将归纳地为电路中的每个门构造一个 (w, r)-析取范式。设 g 是一个形如 $g := g_1 \circ g_2$ 的门，其运算为二元运算 $\circ \in \{\vee, \wedge\}$。假设我们已归纳地为 g_1 和 g_2 分别构造了两个 (w, r)-析取范式 $F_{\mathcal{S}}$ 和 $F_{\mathcal{T}}$。我们将构造一个析取范式 F_g，使得

$$E_{1,g} := \Pr_{x \sim \mathcal{D}_1}[F_g(x) < (F_{\mathcal{S}} \circ F_{\mathcal{T}})(x)] \leq (2r/q)^w \tag{5}$$

and

$$E_{0,g} := \Pr_{x \sim \mathcal{D}_0}[F_g(x) > (F_{\mathcal{S}} \circ F_{\mathcal{T}})(x)] \leq (2r/q)^w. \tag{6}$$

若 $\circ = \vee$，我们通过令 $F_g := F_{\mathsf{pluck}(\mathcal{S} \cup \mathcal{T})}$ 来近似 $F_{\mathcal{S}} \vee F_{\mathcal{T}}$。注意，根据断言 3.7，我们有 $F_{\mathsf{pluck}(\mathcal{S} \cup \mathcal{T})}$ 是一个 (w, r)-析取范式，并且

$$F_{\mathsf{pluck}(\mathcal{S} \cup \mathcal{T})} \geq F_{\mathcal{S} \cup \mathcal{T}} = F_{\mathcal{S}} \vee F_{\mathcal{T}}.$$

因此，在 $\mathcal{D}_1$ 上进行摘取不会引入误差，这意味着 (5)。此外，根据断言 $n^{-w} \leq (2r/q)^w$ 在 $\mathcal{D}_0$ 上进行摘取至多产生误差3.7 以及 $q \leq rn$，这意味着 (6)。

如果 $\circ = \wedge$，我们通过先取 g 来进行近似

$$\mathcal{F} := \mathsf{pluck}\left(\{S \cup T : S \in \mathcal{S}, T \in \mathcal{T}\}\right).$$

根据断言 3.7，$F_{\mathcal{F}}$ 是 r-小的，因为对于每个 $S \in \mathcal{S}$，$|S \cup T| \leq 2w$，$T \in \mathcal{T}$。与 $\vee$ 情形一样，这不会在 $\mathcal{D}_1$ 上产生误差，而在 $\mathcal{D}_0$ 上的误差至多为 $n^{-w} \leq (2r/q)^w$。现在，我们通过从 $\mathcal{F}$ 中移除所有宽度大于 w 的集合来定义 F_g。由于 $F_g \leq F_{\mathcal{F}}$，这一移除不会在 $\mathcal{D}_0$ 上产生误差。由于 $\mathcal{F}$ 是 r- 小的，$\mathcal{D}_1$ 的 q- 扩散性意味着

$$\Pr_{x \sim \mathcal{D}_1}[F_g(x) > F_{\mathcal{F}}(x)] \leq \sum_{\ell=w+1}^{2w} \sum_{S \in \mathcal{F} \cap \binom{[n]}{\ell}} \Pr_{x \sim \mathcal{D}_1}[t_S(x) = 1] \leq \sum_{\ell=w+1}^{t} r^\ell q^{-\ell} \leq (2r/q)^w,$$

其中我们用到了 $q \geq 2r$。由此我们证明了（5）和（6）。

最后，令 F 为输出门的（w，r）-析取范式。根据并集界和方程（5），

$$\Pr_{x \sim \mathcal{D}_1}[C(x) > F(x)] \leq \sum_g E_{1,g} \leq (cq/r)^w (2r/q)^w \leq (2c)^w \leq 0.1,$$

对于 $c = 0.05$。对于 $\Pr_{x \sim \mathcal{D}_0}[C(x) < F(x)]$，也有类似的界。因此

$$\Pr_{x \sim \mathcal{D}}[F(x) \neq f(x)] = \frac{1}{2} \Pr_{x \sim \mathcal{D}_1}[C(x) > F(x)] + \frac{1}{2} \Pr_{x \sim \mathcal{D}_0}[C(x) < F(x)] \leq 0.1. \qquad \blacksquare$$

4 布尔分离

回顾一下，给定一个矩阵 M，其具有 n 行和 m列，定义在域 $\mathbb{F}$上，布尔函数f_M：$\{0,1\}^m \to \{0,1\}$ 当且仅当输入 $S \subseteq [m]$ 满足 $M[S]$ 具有满秩时才接受该输入。在本节中，我们只考虑 $\mathbb{F} := \mathbb{F}_2$ 以证明定理1.5。

4.1 非单调低深度电路上界

我们先证明定理1.2的上界部分。

引理 4.1（上界）。对于任意矩阵 $M \in \mathbb{F}^{n \times m}$，函数 f_M 可由一个大小为 poly(m)、深度为 $O(\log m)^2$ 的布尔电路计算。

证明。对于一个输入 1_S，其对应于集合 $S \subseteq [m]$的指示向量，我们需要计算矩阵 $M[S]$的秩。已知该秩可由一个大小为 poly(m)、深度为 $O(\log m)^2$ [ABO99，Mul87]的布尔电路计算。$\blacksquare$

4.2 基于良态编码的单调布尔电路下界

我们先来定义一种特殊的线性二元码，它们将在第4.3节中明确构造。我们只会使用这些码的抽象性质来定义概率分布，以便应用定理3.3，并为计算与这些码相关函数的单调电路证明下界。

定义 4.2. 对于 $M \in \mathbb{F}^{n\times m}$，我们将 M 的（线性）码 $\mathcal{C}_M$ 定义为

$$\mathcal{C}_M := \{\, M^\top w \mid w \in \mathbb{F}^n \} \subseteq \mathbb{F}^m,$$

并将 M 的对偶码 $\mathcal{D}_M$ 定义为

$$\mathcal{D}_M := \{\, w \in \mathbb{F}^m \mid Mw = 0 \} \subseteq \mathbb{F}^m.$$

我们称码 $\mathcal{C} \subseteq \mathbb{F}^m$ 为线性码，如果存在一个秩为 n 的矩阵 $G \in \mathbb{F}^{n\times m}$，称为 $\mathcal{C}$的生成矩阵，使得

$$\mathcal{C} = \mathcal{C}_G.$$

对于任意线性码 $\mathcal{C} \subseteq \mathbb{F}^m$，如果一个秩为 $m-n$ 的矩阵 $H \in \mathbb{F}^{(m-n)\times n}$ 满足以下条件，我们称其为 $\mathcal{C}$ 的校验矩阵：

$$\mathcal{C} = \mathcal{D}_H,$$

并且在这种情况下，我们将 $\mathcal{C}$ 的对偶码 $\mathcal{C}^*$ 定义为

$$\mathcal{C}^* := \mathcal{C}_H,$$

它与校验矩阵 H的选择无关。我们将线性码 $\mathcal{C} \subseteq \mathbb{F}^m$ 的距离 定义为

$$d(\mathcal{C}) := \min_{x\in\mathcal{C}, x\neq 0} |\{\, i \in [m] \mid x_i \neq 0\}|,$$

并将其对偶距离 定义为 $d^*(\mathcal{C}) := d(\mathcal{C}^*)$。对于每个 d，$t \in \mathbb{R}_{\geq 0}$，如果$d(\mathcal{C}) > d$ 且 $d^*(\mathcal{C}) > t$，我们称 $\mathcal{C}$ 是 $(d,\ t)$-良态 。◀

本节的主要定理如下。

定理 4.3。设 $n \in \mathbb{N}$，且 $m := m(n) \in \mathbb{N}$，以及 $d := d(n) \in \mathbb{N}$，并且 $t := t(n) \in \mathbb{N}$。设$\mathcal{C} \subseteq \mathbb{F}^m$ 是任意一个（$d,\ t$）-良态线性码，其生成矩阵为 $M \in \mathbb{F}^{n\times m}$。如果 $2n < d$，那么 f_M 的单调复杂度至少为

$$\Omega\left(\frac{d}{n\sqrt{t}}\right)^{\sqrt{t}/(b\log m)},$$

其中，$b \in \mathbb{R}$ 是一个足够大的正常数。

在 4.3 节中，我们将使用该定理

$$m \approx n^{3/2}\log n,\ \text{and}\ d \approx m-n,\ \text{and}\ t \approx n.$$

本节的其余部分将用于证明该定理。以下我们假设 $\mathcal{C}$ 和 M 满足定理中的假设。对于每个$i \in [m]$，记 $M_i \in \mathbb{F}^n$ 为 M 的第 i列。我们首先证明一些与 M的子矩阵的秩相关的性质。其中一些是编码理论中的标准事实，但为完整起见，我们在此给出证明。

引理 4.4（第 1 章的定理 10，出自 [MS77]）。对于每个 $S \subseteq [m]$ 满足 $|S| \leq t$ 的情况，M 中由 S 索引的列线性无关。

证明。设 S 是 $[m]$ 的一个子集，使得 M 中由 S 索引的列线性相关。那么存在一个非零向量 $v \in \mathbb{F}^m$，使得 $\mathrm{supp}(v) \subseteq S$，并且

$$\sum_{i \in [m]} v_i M_i = 0.$$

因此，$Mv = 0$，且 $v \in \mathcal{D}_M$。注意到 $\mathcal{D}_M = \mathcal{C}^*$，因为对于任意满足 $\mathcal{C} = \mathcal{D}_H$ 的矩阵 $H \in \mathbb{F}^{(m-n)\times m}$，我们有

$$\mathcal{C}^* = \mathcal{C}_H \text{ and } HM^\top = 0.$$

根据 $\mathcal{C}^*$ 的距离定义，以及 $\mathcal{C}$ 是 (d,t)-良态的这一事实，我们得到

$$|S| \geq |\mathrm{supp}(v)| \geq d^*(\mathcal{C}) > t.$$ ■

引理 4.5. 对于任意维数为 $D < n$ 的子空间 $V \subseteq \mathbb{F}^n$，以及作为 M 的均匀随机列的 u，我们有

$$\Pr_u [u \in V] \leq 1 - d/m =: \Delta.$$

证明. 由于 V 的维数为 $D \leq n-1$，存在一个非零向量 $c \in \mathbb{F}^n$，使得对于每个 $v \in V$，都有 $v^\top c = 0$。令 $C \subseteq [m]$ 为 M 中属于 V 的那些列组成的集合，并令

$$w := M^\top c \in \mathcal{C}_M = \mathcal{C}.$$

注意，对于每个 $i \in C$，都有 $w_i = M_i^\top c = 0$。因此，根据 $\mathcal{C}$ 的距离定义，以及 $\mathcal{C}$ 是 (d,t)-良态的这一事实，我们得到

$$m - |C| \geq |\mathrm{supp}(w)| \geq d(\mathcal{C}) > d.$$

因此，

$$\Pr_u [u \in V] \leq \frac{|C|}{m} \leq 1 - \frac{d}{m}.$$ ■

引理 4.6. 对于任意 $N := N(m) \in \mathbb{N}$ 满足 $N \leq m$ 的情形，以及从 $\binom{[m]}{N}$ 中均匀随机抽取的随机集合 S，我们有

$$\Pr_S [M[S] \text{ is not full rank}] \leq 2^n \Delta^N.$$

证明. 令 $\mathrm{span}(S) := \mathrm{span}(\{ M_i \mid i \in S \})$，其中 M_i 是由 $i \in [m]$ 索引的 M 的列。注意，$M[S]$ 的秩至多为 $n-1$，当且仅当存在一个维数为 $n-1$ 的子空间 $V \subseteq \mathbb{F}^n$，使得 $\mathrm{span}(S) \subseteq V$。因此，

$$\begin{aligned} \Pr_S [M[S] \text{不满秩}] &\leq \Pr_S [\exists V \subseteq \mathbb{F}_2^n \text{使得 } \dim(V) = n-1 \text{ 且 } \mathrm{span}(S) \subseteq V] \\ &\leq \sum_{V \subseteq \mathbb{F}_2^n, \dim(V) = n-1} \Pr_S [S \subseteq V]. \end{aligned}$$

根据命题 Stanley 第 1.7.2 节中 [Sta97], 的数量 $n-1$ 维子空间 $\mathbb{F}^n$ 是

$$\frac{(2^n - 1)(2^n - 2) \cdots (2^n - 2^{n-2})}{(2^{n-1} - 1)(2^{n-1} - 2) \cdots (2^{n-1} - 2^{n-2})} \leq 2^n - 1.$$

对于任意一个（$n-1$）维子空间 V中的 $\mathbb{F}^n$，令 $C_V \subseteq [m]$ 为 M中包含于 V的列集合。根据引理 4.5，我们知道 $c := |C_V| \le \Delta m$，这意味着

$$\Pr_S[S \subseteq V] \le \Pr_S[S \subseteq C_V] = \frac{\binom{c}{N}}{\binom{m}{N}} \le \left(\frac{c}{m}\right)^N \le \Delta^N.$$

因此，

$$\Pr_S[M[S] \text{不是满秩的}] \le 2^n \Delta^N. \qquad \blacksquare$$

现在我们的目标是应用定理 3.3 来证明 f_M 的一个下界。因此，我们首先定义两个概率分布。直观地说，对于规模较小的单调布尔电路而言，这两个分布难以区分。

定义 4.7。我们通过对一个汉明重量为.....的 $a \in$ 进行均匀随机采样，来定义分布 $a \sim D_1$ $\{0,1\}^m$

$$N := n\lceil m/d \rceil. \tag{7}$$

我们通过均匀随机采样一个 $u \in \mathbb{F}_2^n$ 来定义分布 $a \sim D_0$；对于每个 $j \in [m]$，若 $\langle M[j]$，则令 a_j:= 1， $u\rangle = 0$ 否则令 a_j:= 0，其中内积是在 $\mathbb{F}_2$ 上计算的。◀

注意，根据 N 的选取以及假设 $2n \le d$，我们有 $N < m$ 一个 d

$$1 - 2^n(1-d/m)^N \ge 1 - 2^n e^{-Nd/m} \ge 1 - 2^n 2^{-n/\ln 2} \ge 1/2.$$

因此，根据引理 4.6，我们有

$$\Pr_{a\sim D_1}[f_M(a) = 1] \ge 1/2 =: \alpha.$$

此外，只要满足 $u \ne 0$，从 D_0 中采样的点 a 就是 f_M^{-1} (0) 的一个元素，因此

$$\Pr_{a\sim D_0}[f_M(a) = 0] = 1 - \frac{1}{2^n} \ge \alpha.$$

Sp的扩散性 D_1。要应用定理 3.3，我们需要证明 D_1 是“扩展的 ”.

引理 4.8（ D_1 的扩散性）。分布 D_1 是 N-wise（m/N）-扩展的 .

证明。设 T 是 $[m]$ 的任意子集，其大小为 $k \le N$。包含由 T 索引的列集合的 M 中的 N 大小列集合的数量为 $\binom{m-k}{N-k}$。因此，

$$\Pr_{a\sim D_1}\left[\bigwedge_{i\in T} a_i = 1\right] \le \frac{\binom{m-k}{N-k}}{\binom{m}{N}}.$$

化简上式可得

$$\Pr_{a\sim D_1}\left[\bigwedge_{i\in T} a_i = 1\right] \le \left(\frac{\prod_{i=0}^{k-1}(N-i)}{\prod_{i=0}^{k-1}(m-i)}\right) \le \left(\frac{N}{m}\right)^k,$$

利用以下事实： $\frac{N-i}{m-i} \le \frac{N}{m}$ 对于 $i \le k-1$。 $\blacksquare$

向日葵界 D_0。 第二步是证明（D_0， ε）-向日葵的向日葵界。我们首先证明 D_0 是 t-wise 独立的。

引理 4.9 （ D_0的独立性）。 分布 D_0 具有均匀边缘分布，且是 t-wise 独立的。

证明。 固定任意一个由 $[m]$组成的集合 $S := \{j_1, j_2, \ldots, j_t\}$。再固定一个向量

$$b := (b_1, b_2, \ldots, b_t) \in \mathbb{F}_2^t.$$

Then

$$\Pr_{a \sim D_0}[a\restriction_S = b] = \Pr_{u \in \mathbb{F}_2^n}[(\langle u, M[j_1]\rangle = b_1) \wedge \ldots \wedge (\langle u, M[j_t]\rangle = b_t)] = \Pr_{u \in \mathbb{F}_2^n}\left[u^\top M[S] = b\right].$$

利用秩-零化度定理，上述概率等于

$$\Pr_{u \in \mathbb{F}_2^n}\left[u^\top M[S] = b\right] = \frac{|\ker(M[S])|}{2^n} = \frac{1}{2^t},$$

其中，最后一个等号由以下事实得出： $M[S]$ 的秩为 t （引理 4.4）。由于 M 的列均非零（因为 $t > 0$），我们可以证明边缘分布是均匀的：对于每个 $\ell \in [t]$,

$$\Pr_{u \in \mathbb{F}_2^n}[\langle u, M[j_\ell]\rangle = 0] = \frac{1}{2}.$$ ■

我们证明中的另一个重要要素是 Bazzi 定理 [Baz09], , Tal 的研究进一步改进了该定理 [Tal17]。这表明，小型析取范式在k-wise 独立分布上的行为，与在真正的均匀分布上的行为几乎相同。

定理 4.10 （利用独立性欺骗析取范式：定理 7.1 [Tal17]） 。 设 F 是一个含有N项的析取范式，且 $\varepsilon \in (0,1)$。那么存在 $T \leq O(\log N \cdot \log(N/\varepsilon))$，使得对于任意一个$\mathcal{D}$ 满足 T-wise 独立且具有均匀边缘分布的分布，我们有

$$\left|\Pr_{a \sim \{0,1\}^n}[F(a) = 0] - \Pr_{a \sim \mathcal{D}}[F(a) = 0]\right| \leq \varepsilon.$$

最后，为了证明我们的向日葵引理，我们将 Bazzi 定理与近期获得的“鲁棒向日葵”的最优界结合起来（例如，参见 [Rao25，引理 2], [BCW21]） 。鲁棒向日葵是（均匀分布 ε）-向日葵，其中均匀分布 表示均匀分布。回顾定义 3.1 中“向日葵界” $r(\cdot, \cdot, \cdot)$。

引理 4.11 (鲁棒向日葵引理：引理 2 [Rao25])。对于每个 $k \in \mathbb{N}$ 和 $\varepsilon \leq 1/2$，我们有 r(均匀分布 k， ε) $= O(\log(k/\varepsilon))$。

现在我们可以为 D_0 证明一个向日葵引理。回顾一下， m 是函数 f_M 的输入比特数。

引理 4.12 （ t路独立分布的向日葵引理） 。 存在一个常数$b \geq 1$，使得对于 $w := \sqrt{t}/(b\log\ m)$ 以及每个 $k \leq 2w$，都有

$$r(D_0, k, m^{-4w}) = O(w \log m).$$

证明。令 $w := \sqrt{t}/(b\log\ m)$，其中常数 b 将在后面定义，并设 $\varepsilon := m^{-4w}$。我们将证明

$$r(D_0, k, \varepsilon) \le r(\mathsf{Uniform}, k, \varepsilon/2).$$

确实，假设 $\mathcal{S}$ 是一个核为 K 的 $\varepsilon/2$-鲁棒向日葵。令 $\mathcal{S}_K = \{ S \setminus K \mid S \in \mathcal{S}\}$。注意到 $F_{\mathcal{S}_K}$ 的宽度至多为 k，且至多包含 $\binom{m}{\le k} \le m^k$ 个项。

现在我们希望将定理4.10 应用于 $F_{\mathcal{S}_K}$，其中采用 t-wise independent distribution D_0 和近似参数 $\varepsilon/2$。定理 4.10 只有在以下条件成立时才能应用

$$t \ge D \log(|\mathcal{S}_K|) \log(|\mathcal{S}_K|/(\varepsilon/2)),$$

对于某个由定理 $D > 0$ 4.10 给出的常数 4.10。现在注意到

$$D \log(|\mathcal{S}_K|) \log(|\mathcal{S}_K|/(\varepsilon/2)) \le O(w^2 (\log m)^2) = \frac{1}{b^2} O(t) \le t$$

当 b 足够大时。因此，我们可以应用定理4.10 并得到

$$\begin{aligned}
\Pr_{x\sim D_0}[\exists S \in \mathcal{S} : t_{S\setminus K}(x) = 1] &= \Pr_{x\sim D_0}[F_{\mathcal{S}_K}(x) = 1] \\
&\ge \Pr_{x\sim\{0,1\}^n}[F_{\mathcal{S}_K}(x) = 1] - \varepsilon/2 \\
&= \Pr_{x\sim\{0,1\}^n}[\exists S \in \mathcal{S} : t_{S\setminus K}(x) = 1] - \varepsilon/2 \\
&> 1 - \varepsilon.
\end{aligned}$$

因此，集合 $\mathcal{S}$ 是一个（D_0，ε）-向日葵。通过观察到4.11，由引理 t

$$r(\mathsf{Uniform}, k, \varepsilon/2) \le O(\log(k/\varepsilon)) \le O(w \log m).$$ ■

总结。现在我们可以应用定理 3.3，从而完成证明。注意，分布D_1 和 D_0 在定义 4.7 中给出，且满足以下性质：

1. 对每个 $i \in \{0, 1\}$，我们都有 $\Pr_{x\sim D_i}[f_M(x) = i] \ge \alpha$；
2. D_1 是 N-wise（m/N）-扩展（引理 4.8）；
3. 对于 $w := \sqrt{t}/$（b对数 m），其中 b 是一个足够大的普适常数（引理 4.12），我们有 r（D_0，k，αm^{-3w}）$\le r$（D_0，k，m^{-4w}）$\le O$（w 对数 m），对每个 $k \le 2w$ 以及足够大的n。

因此，根据定理 3.3 以及 N（方程 7）的选取，我们得到 f_M 的单调复杂度至少为

$$\Omega\left(\frac{m}{Nw\log m}\right)^w \ge \Omega\left(\frac{d}{nw\log m}\right)^w = \Omega\left(\frac{d}{n\sqrt{t}}\right)^{\sqrt{t}/(b\log m)}.$$

这就完成了定理4.3的证明。

4.3 良态码的显式构造

现在我们构造一个显式的良态二进制码 $\mathcal{C}$ ，以便应用第4.2 节中的论证，证明计算均匀$\mathbf{NC}^2$中的布尔函数的单调电路具有指数下界。

引理 4.13. 令 $n, m, \ell \in \mathbb{N}$，并设 $\mathbb{F}_q$ 是一个满足 $q := 2^\ell$ 的有限域。设 $\mathcal{L} \subseteq \mathbb{F}_q^m$ 是由矩阵 $G \in \mathbb{F}_q^{n\times m}$ 生成的线性码。那么，存在一个由矩阵 $M \in \mathbb{F}_2^{r\times s}$ 生成的线性二元码 $\mathcal{C} \subseteq \mathbb{F}_2^s$，使得对于 $r := \ell n$ 和 $s := \ell m$，

$$d(\mathcal{L}) \le d(\mathcal{C}) \le \ell d(\mathcal{L}) \text{ and } d^*(\mathcal{L}) \le d^*(\mathcal{C}) \le \ell d^*(\mathcal{L}).$$

此外，如果 $\mathcal{L}$ 的生成矩阵 G 的每个元素都能在 poly(n, m, ℓ) 时间内计算出来，那么我们就能在 poly(n, m, ℓ) 时间内计算出 $\mathcal{C}$ 的生成矩阵 M 的所有元素。

证明。设 $\mathcal{B} := \{b_1, \ldots, b_\ell\}$ 是 $\mathbb{F}_q$ 的一组基，并将其视为 $\mathbb{F}_2$ 上的 ℓ 维向量空间。设 $\phi\colon \mathbb{F}_q \to \mathbb{F}_2^\ell$ 是一个映射，将元素 $v \in \mathbb{F}_q$ 映射到其关于基 $\mathcal{B}$ 的坐标向量：也就是说，对于每个 $v \in \mathbb{F}_q$，令 $\phi(v) \in \mathbb{F}_2^\ell$ 为满足下式的唯一向量

$$v = \sum_{i\in[\ell]} \phi(v)_i b_i.$$

注意，ϕ 是 $\mathbb{F}_q$ 与 $\mathbb{F}_2^\ell$之间的线性同构。令 $\gamma\colon \mathbb{F}_q^m \to \mathbb{F}_2^{\ell m}$为如下映射：对每个 $v_1, \ldots, v_m \in \mathbb{F}_q$,

$$\gamma(v_1, \ldots, v_m) := (\phi(v_1), \ldots, \phi(v_m)).$$

再次注意，γ 是 $\mathbb{F}_q^m$与 $\mathbb{F}_2^{\ell m}$之间的线性同构；特别是 r:

$$\gamma(0) = 0 \text{ and } \gamma \text{ is a linear bijection.}$$

Let

$$\mathcal{C} := \{\, \gamma(w) \mid w \in \mathcal{L} \},$$

并令 $g_1, \ldots, g_n \in \mathbb{F}^m$ 为 G的各行。注意，对每个 $w \in \mathbb{F}_q^k$,

$$G^\top w = \sum_{i\in[n]} w_i g_i = \sum_{i\in[n]} \sum_{j\in[\ell]} \phi(w_i)_j b_j g_i,$$

因此

$$\gamma(G^\top w) = \sum_{i\in[n]} \sum_{j\in[\ell]} \phi(w_i)_j \gamma(b_j g_i).$$

令 $M \in \mathbb{F}_2^{r\times s}$（其中 $r := \ell n$ 且 $s := \ell m$）为以向量 $\gamma(b_j g_i)$为行的矩阵，即

$$M := \sum_{i\in[n]} \sum_{j\in[\ell]} e_{(i-1)\ell+j} \gamma(b_j g_i)^\top = \begin{bmatrix} \gamma(b_1 g_1)^\top \\ \vdots \\ \gamma(b_n g_\ell)^\top \end{bmatrix}, \tag{8}$$

其中 $e_1, \ldots, e_{n\ell}$是 $\mathbb{F}_2^{n\ell}$的标准基向量。由于 ϕ是一个线性同构，我们可以证明

$$\mathcal{C} = \{\, M^\top w \mid w \in \mathbb{F}_2^{n\ell} \}.$$

现在来证明所声称的 $\mathcal{C}$的距离界。首先注意，如果 $v \in \mathcal{C}$ 满足 $v = \gamma(w)$ =($\phi(w_1)$……， $\phi(w_m)$)，其中 $w \in \mathcal{L} \subseteq \mathbb{F}_q^m$为某个值，那么，由于 $\phi(x)$ 当且仅当 $= 0$ 当且仅当 $x = 0$，我们有

$$|\operatorname{supp}(w)| \leq |\operatorname{supp}(v)|,$$

这意味着 $d(\mathcal{L}) \leq d(\mathcal{C})$，并且 $|\mathsf{supp}(v)| \leq \ell|\operatorname{supp}(w)|$，这意味着

$$d(\mathcal{C}) \leq \ell d(\mathcal{L}).$$

为了证明 $\mathcal{C}$ 的对偶距离界，我们将使用以下对码的对偶距离的刻画：

命题4.14 (第5章中的定理8，出自 [MS77])。 我们称集合 $S \subseteq \mathbb{F}_q^m$是 t-重独立的，如果对于均匀选取的（x_1，……， x_m）：$= x \sim \mathrm{Unif}(S)$，以及所有满足 $I \subseteq [m]$ 的 $|I| \leq t$，变量（x_i）$_{i \in I}$ 相互独立，并且在 $\mathbb{F}_q$上均匀分布。那么，线性码 $\mathcal{C} \subseteq \mathbb{F}_q^m$是 t-重独立的，当且仅当 $t \leq d^*(\mathcal{C}) - 1$。

现在证明 $d^*(\mathcal{L}) \leq d^*(\mathcal{C})$。对于任意 $t \leq d^*(\mathcal{L})-1$，根据命题4.14，我们知道 $\mathcal{L}$ 在 $\mathbb{F}_q$ 上是 t-重独立的。这意味着，对于均匀选取的（x_1，……， x_m）：$= x \sim \mathsf{Unif}(\mathcal{L})$，以及满足 $|I| \leq t$ 的 $I \subseteq [m]$ ，变量（x_i）$_{i \in I}$ 相互独立，并且在$\mathbb{F}_q$上均匀分布。令

$$(y_1, \ldots, y_{\ell m}) := y \sim \mathrm{Unif}(\mathcal{C}).$$

由于对于任意 $i \in I$ ， x_i 在 $\mathbb{F}_q$ 上均匀分布，且 ϕ 是从 $\mathbb{F}_q$ 到 $\mathbb{F}_2^\ell$ 的双射，因此 ($y_{i,1}, \ldots, y_{i,\ell}$) := $\phi(x_i)$ 是相互独立且在 $\mathbb{F}_2$ 上均匀分布的随机变量。因此，随机变量 $(y_{i,p})_{i \in I, p \in [\ell]}$ 的任意子集 $J \subseteq I \times [\ell]$ ，只要满足 $|J| \leq t$ ，就有 $(y_j)_{j \in J}$ 是相互独立且在 $\mathbb{F}_2$ 上均匀分布的随机变量。因此， $\mathcal{C}$ 是 t-wise 独立的，并且根据命题4.14，

$$d^*(\mathcal{L}) \leq d^*(\mathcal{C}).$$

现在假设

$$d^*(\mathcal{C}) \geq \ell d^*(\mathcal{L}) + 1.$$

根据命题4.14，我们得到 $\mathcal{C}$ 是 ($\ell d^*(\mathcal{L})$)-wise 独立的。再次利用 ϕ 是从 $\mathbb{F}_q$ 到 $\mathbb{F}_2^\ell$ 的双射这一事实，可以证明：对于均匀选取的 $(x_1, \ldots, x_m) := x \sim \mathsf{Unif}(\mathcal{L})$，以及满足 $|I| \leq d^*(\mathcal{L})$ 的 $I \subseteq [m]$ ，变量 $(x_i)_{i \in I}$ 相互独立且在 $\mathbb{F}_q$ 上均匀分布。根据命题4.14，我们得到 $d^*(\mathcal{L}) + 1 \leq d^*(\mathcal{L})$，这与假设矛盾。因此，

$$d^*(\mathcal{C}) \leq \ell d^*(\mathcal{L}).$$

现在我们来讨论该构造的显式性。注意：

- （通过 $\mathbb{F}_q$的一个基进行）元素表示，以及在域 $\mathbb{F}_q$ 上的运算，都可以在 $\mathsf{poly}(\ell)$ [Sho88]时间内完成。
- 对于任意给定的 $(v_1, \ldots, v_m) := v \in \mathbb{F}_q^m$，元素 $\gamma(v) \in \mathbb{F}_2^{\ell m}$都可以在 $\mathsf{poly}(m, \ell)$ 时间内均匀分布地计算出来，因为它只是 $\phi(v_1) \ldots, \phi(v_m) \in \mathbb{F}_2^\ell$的拼接，而 $\phi(v_i)$ 是 v_i 作为 $\mathbb{F}_q$中一个元素的表示。
- 生成矩阵$M \in \mathbb{F}_2^{\ell n \times \ell m}$（方程8）对于 $\mathcal{C} \subseteq \mathbb{F}_2^{\ell m}$可以在 $\mathsf{poly}(n, m, \ell)$ 时间内均匀计算。■

推论 4.15。对于每个 n，$m \in \mathbb{N}$ 满足 $m > n$ 且对于 $\ell := \lceil \log_2 m \rceil$，存在一个二元码$\mathcal{C} \subseteq \mathbb{F}_2^{\ell m}$，使得我们可以显式构造生成矩阵 $M \in \mathbb{F}_2^{\ell n \times \ell m}$，它对应于 $\mathcal{C}$，并且

$$m - n \leq d(\mathcal{C}) \leq 2\ell(m-n) \text{ and } n \leq d^*(\mathcal{C}) \leq 2\ell n.$$

证明。对于 $q := 2^\ell$，令 $\mathcal{L} \subseteq \mathbb{F}_q^m$为定义在 $\mathbb{F}_q$ 上的里德–所罗门码，其生成矩阵为 $G \in \mathbb{F}_q^{n \times m}$。以下是编码理论中的标准结果（例如，参见 [MS77]的第 10 章）：

- 矩阵 G 的每个元素都可以在 poly(n, m, ℓ) 时间内构造出来。
- $\mathcal{L}$ 的距离为
$$d(\mathcal{L}) = m - n + 1.$$
- $\mathcal{L}$的对偶码的距离为
$$d^*(\mathcal{L}) = m - (m-n) + 1 = n + 1.$$

根据引理 4.13，存在一个二元码 $\mathcal{C} \subseteq \mathbb{F}_2^{\ell m}$，使得我们可以显式构造其生成矩阵 $M \in \mathbb{F}_2^{\ell n \times \ell m}$，用于 $\mathcal{C}$，并且

$$m - n \leq d(\mathcal{L}) \leq d(\mathcal{C}) \leq \ell d(\mathcal{L}) \leq 2\ell(m-n), \text{ and } n \leq d^*(\mathcal{L}) \leq d^*(\mathcal{C}) \leq \ell d^*(\mathcal{L}) \leq 2\ell n. \quad \blacksquare$$

定理 4.16（定理 1.5）。对于每个充分大的 $n \in \mathbb{N}$，并且对于

$$m := \lceil n^{3/2} (\log n)^2 \rceil \text{ and } \ell := \lceil \log_2 m \rceil,$$

存在一个 ℓm 元单调布尔函数 $f\colon \{0,1\}^{\ell m} \to \{0,1\}$，满足以下条件：

1. f 可由一个规模关于 n 为多项式、深度为 $O(\log \ell m)^2$ 的一致布尔电路计算。
2. 任何计算 f 的单调布尔电路，其规模至少为 $2^{(\ell m)^{1/3 - o(1)}}$。

证明。根据推论 4.15，存在一个二元码 $\mathcal{C} \subseteq \mathbb{F}_2^{\ell m}$，使得我们可以显式构造生成矩阵 $M \in \mathbb{F}_2^{\ell n \times \ell m}$，对应于 $\mathcal{C}$，并且

$$m - n \leq d(\mathcal{C}) \leq 2\ell(m-n) \text{ and } n \leq d^*(\mathcal{C}) \leq 2\ell n. \tag{9}$$

令 $f := f_M$ 为对应于 ℓm 的 M 元布尔函数。根据引理 4.1，函数f 可由一个规模为 poly(ℓm)、深度为 $O(\log \ell m)^2$ 的一致布尔电路计算。令

$$d := d(\mathcal{C}) - 1 \text{ and } t := d^*(\mathcal{C}) - 1.$$

注意，对于充分大的 n，

$$d \geq 2n\ell.$$

By 定理 4.3，我们得到单调复杂度 $S^+(f)$ 的 f 至少为 st

$$\Omega\left(\frac{d}{\ell n w \log(\ell m)}\right)^w,$$

对于 $w := \sqrt{t/(b \log(\ell m))}$。根据等式 9，我们得到

$$\Omega(m^{1/3}/(\log m)^2) \leq w \leq O(n^{1/2}/(\log m)^{1/2}).$$

因此，

$$S^+(f) \geq \Omega\left(\frac{d}{\ell n w \log(\ell m)}\right)^w \geq \Omega\left(\frac{m}{n^{3/2}(\log m)^{3/2}}\right)^w \geq \Omega(\log m)^{w/2} \geq 2^{\Omega(m^{1/3} \log\log m/(\log m)^2)}. \quad \blacksquare$$

5 混合分离

本节借鉴了第4 节中的一些思路，以证明 f_M 在 M 为实矩阵时的一个下界。我们还得到了单调电路规模的较弱（但仍是超多项式）下界。

5.1 非单调低深度电路上界

我们首先证明定理1.4的上界部分。

引理 5.1 （上界）。 对于任意矩阵 $A \in \mathbb{R}^{n\times m}$，多项式 $P_A \in \mathbb{R}[x_1,\ldots,x_m]$（如方程 2中所定义）可由规模为 poly($m$)、深度为 $O(\log m)^2$.的算术电路计算。

证明。令

$$I_X := \sum_{i=1}^{m} x_i e_i e_i^\top \in \mathbb{R}[X]^{m\times m}$$

为对角元素替换为变量 x_1、.....、 x_m 的 m 维单位矩阵。根据柯西-比内公式，我们有

$$\det((AI_X)A^T) = \sum_{\substack{S\subseteq[m]:\\ |S|=n}} \det((AI_X)[[n],S])\det(A^T[S,[n]]) = \sum_{\substack{S\subseteq[m]:\\ |S|=n}} \det((AI_X)[[n],S])\det(A[S]),$$

并且，根据 I_X 的分块结构以及行列式的乘法性质，

$$\det((AI_X)[[n],S]) = \det(A[[n],S]I_X[S,S]) = \det(A[[n],S])\det(I_X[S,S]) = \det(A[S])\prod_{i\in S} x_i.$$

因此，

$$\det((AI_X)A^T) = \sum_{\substack{S\subseteq[m]:\\ |S|=n}} \left(\det(A[S])\prod_{i\in S} x_i\right)\det(A[S]) = P_A(x_1,\ldots,x_m).$$

通过高效计算符号矩阵的行列式 [Ber84, MV97], 我们得到，多项式 $P_A = \det(AI_XA^T)$ 可由大小为 poly(m)、深度为 $O((\log m)^2)$ 的算术电路计算。 ■

5.2 良态 $\mathbb{R}$-矩阵的选择

令 $k := k(n) \in \mathbb{N}$ 为一个增长函数，稍后将具体说明，并满足 $k \le n^{0.1}$。令

$$m := n^2 \qquad \text{and} \qquad s := 200k^2. \tag{10}$$

令 M_n为一个 $n\times m$随机矩阵，其每一列 $M_n[i]$都从 $\{0,1\}^n$ 中汉明重量至多为 s的向量集合中独立均匀随机采样得到。

出于技术原因，使用汉明重量至多为s的点来采样矩阵更为方便，不过下面的引理表明，这与采样重量接近 s. 的点并无太大区别

引理 5.2. 以至少 $1-1/n$, M_n 的每一列的汉明重量都至少为 $s/2$.

证明。 注意到 $s = 200k^2 = O(n^{0.2})$。我们注意到，对于 $i \in [n]$, $\binom{n}{i} \le n^i$ ，并利用 s 上的界得出结论

$$\binom{n}{\le s} \ge \binom{n}{s} \ge \left(\frac{n}{s}\right)^s \ge n^{0.7s}.$$

综合起来，任意固定列 $M_n[j]$ 的汉明重量小于 $s/2$ 的概率至多为

$$\sum_{i=0}^{s/2} \frac{\binom{n}{i}}{\binom{n}{\le s}} \le \frac{(s/2+1)\cdot n^{s/2}}{n^{0.7s}} \le \frac{n}{n^{0.2s}}.$$

对 $m = n^2$ 列应用并集界，并利用 $s \ge 200$这一事实，存在汉明重量至多为 $s/2$的列的概率至多为 $1/n$。 ■

为了构造困难分布，下面的引理将发挥重要作用。

引理 5.3 （满秩引理）。 若 S在 $\binom{[m]}{10n\log n}$ 上均匀分布，且与M_n相互独立，那么

$$\Pr_{M_n}\left[\Pr_{S}\left[M_n[S] \text{ is full rank}\right] \ge 1/10\right] \ge 1/10.$$

证明。 思路是进行一个类似于优惠券收集问题解法的论证，以证明对每个 $S \in \binom{[m]}{10n\log n}$，都有

$$\Pr_{M_n}\left[M_n[S] \text{ is full rank}\right] \ge \frac{4}{5}. \tag{11}$$

由以下平均论证可知，引理的结论随即由公式 11 推出。定义随机变量

$$X := \Pr_{S\in\binom{[m]}{n}}\left[M_n[S] \text{ is full rank}\right], \text{ and } Y := 1 - X.$$

Thus

$$\begin{aligned}\mathbb{E}_{M_n}[X] &= \mathbb{E}_{M_n}\left[\frac{1}{\binom{m}{n}}\sum_{S\subseteq[m]:|S|=n}\mathbb{1}_{\mathrm{rank}(M_n[S])=n}\right]\\ &= \frac{1}{\binom{m}{n}}\sum_{S\subseteq[m]:|S|=n}\Pr_{M_n}\left[\mathrm{rank}(M_n[S])=n\right] \ge \frac{4}{5},\end{aligned}$$

和 $\mathbb{E}_{M_n}[Y] \le \frac{1}{5}$。 由马尔可夫不等式可得

$$1 - \Pr_{M_n}\left[X \ge \frac{1}{10}\right] = \Pr_{M_n}\left[Y \ge \frac{9}{10}\right] \le \frac{10\mathbb{E}_{M_n}[Y]}{9} \le \frac{2}{9},$$

这意味着

$$\Pr_{M_n}\left[X \ge \frac{1}{10}\right] \ge \frac{7}{9} > \frac{1}{10}.$$

现在来证明公式 11中的概率界。不失一般性，设$S = \{1,\dots,10n\log n\}$。假设我们选取一个由向量组成的无限序列 $\{v_i\}_{i\in\mathbb{N}}$ 个向量

独立且均匀随机地 $\{0,1\}^n_{\leq s}$。对于每个 $d \leq n$，令 X_d 表示最小的r，使得 v_1、.....、v_r 张成一个维数为 d的子空间。只需证明 $\mathbb{E}X_n \leq 2n\log n$，因为由马尔可夫不等式可得公式11 ，这是因为我们可以将 M_n的定义理解为选取向量 v_1、$\cdots$、$v_{10n\log n}$作为 M_n的列。对于 $X_0 := 0$，我们有 $X_n := \sum_{d=0}^{n-1} X_{d+1} - X_d$，这意味着

$$\mathbb{E}X_n = \sum_{d=0}^{n-1} \mathbb{E}[X_{d+1} - X_d].$$

为了计算 $\mathbb{E}[X_{d+1}-X_d]$，我们对取值 $X_d = r$ 以及向量 $v_1,\ldots,v_r$进行条件化，它们张成了一个向量空间 V，其维数为 d. 令 p_d 表示均匀随机的 $v \in \{0,1\}^n_{\leq s}$位于 V之外的概率。根据下文证明的子空间引理（引理 5.4），可得

$$1 - p_d \leq \frac{\binom{d}{\leq s}}{\binom{n}{\leq s}} \leq \frac{d+1}{n+1}$$

w这里，后一个不等式由以下简单的二项分布估计得出 :

$$\binom{d}{\leq s} = 1 + d + \sum_{i=2}^{s} \binom{d}{i} \leq 1 + d + \sum_{i=2}^{s} \frac{d+1}{n+1} \cdot \binom{n}{i} = \frac{d+1}{n+1} \cdot \binom{n}{\leq s}.$$

因此， $X_{d+1} - X_d$（在给定 $v_1,\ldots,v_r$ 的条件下）服从成功概率为 $p_d \geq (n-d)/(n+1)$ 的几何分布，故其期望至多为 $(n+1)/(n-d)$。因此

$$\mathbb{E}X_n \leq \sum_{d=0}^{n-1} \frac{n+1}{n-d} \leq 2n\log n.$$

至此，我们得到了所需的 $\mathbb{E}X_n$ 上界，从而完成了该引理的证明。■

上述证明用到了以下引理，它表明，均匀随机选取的$v \in \{0,1\}^n_s$ 以高概率不会落在 $\mathbb{R}^n$ 的任何真子空间中。

引理 5.4（子空间引理）。设 $\mathbb{F}$ 是任意一个域， V 是 $\mathbb{F}^n$ 的一个维数为 d 的子空间， $\{0,1\}^n_{\leq s}$ 是所有汉明重量至多为 s 的二进制串的集合。那么，

$$|V \cap \{0,1\}^n_{\leq s}| \leq \binom{d}{\leq s}.$$

我们注意到，上述引理是紧的，见证是由任意 d 个标准基向量生成的子空间 V。

证明。由于 V 的维数为 d，因此存在 V 的一组基 B，使得存在一个集合 $R \in \binom{[n]}{d}$，用于对 B 中的元素进行如下索引：

$$B = \{\, b^{(r)} \mid r \in R\}$$

使得，对于每个 $r \in R$ 和 $v \in B$,

$$\begin{cases} v_r = 1 & \text{if } v = b^{(r)}, \text{ and} \\ v_r = 0 & \text{otherwise.} \end{cases}$$

注意，我们可以对 V的任意一组基进行高斯消元，从而找到这样一组基，因为上面的集合 R 对应于列阶梯形矩阵中主元所在的行。对于每个 $v \in X := V \cap \{0,1\}^n_{\leq s}$，令 $\alpha_v \in \mathbb{R}^B$ 为满足 $v = \sum_{b\in B} \alpha_{v,b} b$的唯一向量。因此，对于每个 $r \in R$,

$$v_r = \sum_{b\in B} \alpha_{v,b} b_r = \alpha_{v,b^{(r)}},$$

这意味着，$\mathrm{supp}(v) \cap R$唯一确定了 α_v（即 $v_r \in \{0,1\}$），进而唯一确定了 v。由于对每个 $v \in X$，$|\mathrm{supp}(v) \cap R| \leq |\mathrm{supp}(v)| \leq s$，因此我们得到

$$|X| \leq \left|\binom{|R|}{\leq s}\right| = \binom{d}{\leq s}. \qquad \blacksquare$$

我们还需要以下引理来证明：以高概率，任意小列元组 M_n 中的大多数列，其支撑集与其前面各列支撑集的并集相交的部分所占比例很小。

定义 5.5. 对于 $[m]$中的 $\tau := (i_1, \ldots, i_t)$个互不相同元素组成的列元组，我们称 i_j关于 τ 是 c-包含的，如果集合 $\mathrm{supp}(M_n[i_j])$ 与 $\bigcup_{p<j} \mathrm{supp}(M_n[i_p])$至少有 c 个元素相同。◀

引理 5.6. 令 S_τ 为以下（随机）集合

$$S_\tau := \{\, j \in [t] \mid i_j \text{ is } 10k\text{-contained w.r.t. } \tau\}.$$

那么，对任意正整数 $t \leq n^{0.1}$，我们有

$$\Pr_{M_n}[\exists\ \tau \text{ such that } |S_\tau| \geq t/2k] \leq \frac{1}{n}.$$

证明。令 $r := \lceil t/2k \rceil$ 和 $\kappa := 10k$。对 $\tau \in [m]^t$ 和 $S \in \binom{[t]}{r}$ 的所有取值应用并集界，可得

$$\Pr_{M_n}[\exists\ \tau \text{ such that } |S_\tau| \geq t/2k] \leq m^t \cdot \binom{t}{r} \max_{\tau,S} \Pr_{M_n}[S \subseteq S_\tau].$$

现在我们将为每个 $\tau =: (i_1, \ldots, i_t)$ 和 $S \in \binom{[t]}{r}$ 求 $\mathbf{Pr}_{M_n}[S \subseteq S_\tau]$ 的上界。令 $\{s_1, \ldots, s_r\} := S$ 满足 $s_1 < \ldots < s_r$，并且对每个 $j \in [r]$，令

$$T_j := \cup_{p<s_j} \mathrm{supp}(M_n[i_p]).$$

首先注意到 $|T_j| \leq ts$，并且

$$\begin{aligned}
\Pr_{M_n}[S \subseteq S_\tau] &\leq \Pr_{M_n}\left[\cap_{j=1}^r \{|\mathrm{supp}(M_n[i_{s_j}]) \cap T_j| \geq \kappa\}\right] \\
&= \prod_{j=1}^r \Pr_{M_n}\left[|\mathrm{supp}(M_n[i_{s_j}]) \cap T_j| \geq \kappa \,\middle|\, \cap_{i=1}^{j-1} \{|\mathrm{supp}(M_n[i_{s_i}]) \cap T_i| \geq \kappa\}\right] \\
&= \prod_{j=1}^r \Pr_{M_n}\left[|\mathrm{supp}(M_n[i_{s_j}]) \cap T_j| \geq \kappa\right],
\end{aligned}$$

最后一个等式是由 M_n 各列选择的独立性得出的。对于每个 $j \in [r]$，再次根据各列的独立性，我们有：

$$\begin{aligned}\Pr_{M_n}\left[|\operatorname{supp}(M_n[i_{s_j}]) \cap T_j| \geq \kappa\right] &= \sum_{T\subseteq[n],\kappa\leq|T|\leq ts} \Pr_{M_n}\left[|\operatorname{supp}(M_n[i_{s_j}]) \cap T| \geq \kappa\right] \Pr_{M_n}\left[T_j = T\right] \\ &\leq \max_{T\subseteq[n],\kappa\leq|T|\leq ts} \Pr_{M_n}\left[|\operatorname{supp}(M_n[i_{s_j}]) \cap T| \geq \kappa\right].\end{aligned}$$

对于每个满足 $\kappa \leq |T| \leq ts$ 的 $T \subseteq [n]$，我们得到

$$\begin{aligned}\Pr_{M_n}\left[|\operatorname{supp}(M_n[i_{s_j}]) \cap T| \geq \kappa\right] &= \Pr_{M_n}\left[\exists R \in \binom{T}{\kappa} \text{ s.t. } R \subseteq \operatorname{supp}(M_n[i_{s_j}])\right] \\ &\leq \frac{\binom{|T|}{\kappa}\binom{n-\kappa}{\leq(s-\kappa)}}{\binom{n}{\leq s}} \leq \frac{\binom{|T|}{\kappa}\cdot(s+1)\cdot\binom{n-\kappa}{s-\kappa}}{\binom{n}{s}} \\ &\leq (s+1)(tse/\kappa)^{\kappa}(2s/n)^{\kappa} \\ &\leq n^{-0.5\kappa} = n^{-5k}.\end{aligned}$$

因此，我们得到

$$\Pr_{M_n}\left[S \subseteq S_\tau\right] \leq n^{-5kr} \leq n^{-2.5t}$$

进而，

$$\Pr_{M_n}\left[\exists\ \tau \text{ such that } |S_\tau| \geq t/2k\right] \leq \binom{t}{r}\cdot m^t n^{-2.5t} = \binom{t}{r}\cdot n^{-0.5t} \leq 1/n. \qquad \blacksquare$$

我们在下面的定义中汇总证明下界所需的矩阵性质。

定义 5.7。 如果矩阵 $M \in \mathbb{R}^{n\times m}$ 满足以下性质，我们就称其为良态：

1. 每一列 $M[i]$ 的支撑大小至少为 $s/2$,
2. $\Pr_{S\in\binom{[m]}{10n\log n}}[M[S]$ 是满秩的$] \geq 1/10$，并且
3. 对任意以及来自 $[m]$ 的任意元组 $\tau = (i_1, \ldots\ldots, i_t)$（其中元素各不相同），满足 i_j 相对于 τ 是 $10k$-包含的$j \in [t]$ 数量小于 $t/2k$. 。特别地，如果 $t \leq k$，则不存在满足 i_j 相对于 τ是 $10k$-包含的 $j \in [t]$ 。

◀

根据引理 5.2、引理 5.3 和引理 5.6 (再对所有 $t \leq n^{0.1}$应用并集界)，我们知道， M_n 对于每个充分大的 n，以正概率是一个良态矩阵。本节余下部分中，我们将 M 记作一个固定的良态矩阵。

5.3 单调通过良态矩阵证明单调布尔电路下界 es

本节余下部分将证明，布尔函数 f_M 无法由规模较小的单调布尔电路计算。这是定理 1.4的下界部分。与第 4.2 节一样，我们先定义 f_M 输入上的两个概率分布。

定义 5.8。 我们通过均匀随机抽取一个汉明重量为 $10n\log\ n$ 的 $a \in \{0,1\}^m$ 来定义分布 $a \sim D_1$ 。我们通过均匀随机抽取一个 $u \in \{-1,0,1\}^n$ 来定义分布 $a \sim D_0$，并且对每个 $j \in [m]$，令

$$a_j := 1 \text{ if } \langle M[j], u\rangle = 0, \text{ and}$$
$$a_j := 0 \text{ otherwise,}$$

其中，内积是在 $\mathbb{R}$ 上取的。 ◀

观察 5.9。 由于矩阵 M 是良态的（见定义 5.7），分布 D_1满足 $\Pr_{a\sim D_1}[f(a) = 1] \geq 1/10.$

此外，只要 $u \neq 0$，从 D_0 中抽取的点 a 就是 f_M^{-1} (0) 的一个元素。因此我们有

$$\Pr_{a\sim D_0}[f_M(a) = 0] = 1 - \frac{1}{3^n}.$$

因此，要通过单调电路下界判据（定理 3.3）证明下界，与之前一样，只需证明 D_1 具有扩散性，并证明 (D_0, ε)-向日葵的界。

引理 5。 **10** （ D_1 的扩散性）。 分布 D_1 是 $n^{0.1}$-阶 $(n/(10\log\ n))$-扩散的 .

证明。 设 T 是 $[m]$ 的一个子集，其大小为 $k \leq n^{0.1}$。该引理的证明与引理 4.8 的证明类似。注意，对于 $\ell :\ = 10n\log\ n$ 以及 $S \sim \text{Unif}(\binom{m}{\ell})$,

$$\Pr_{a\sim D_1}\left[\bigwedge_{i\in T} a_i = 1\right] = \Pr_S[T \subseteq S] = \frac{\binom{m-k}{\ell-k}}{\binom{m}{\ell}} = \prod_{i=0}^{k-1}\frac{\ell-i}{m-i} \leq \left(\frac{\ell}{m}\right)^k,$$

其中最后一个不等式由 $\frac{\ell-i}{m-i} \leq \frac{\ell}{m}$ 对 $i \leq k-1$ 得出。由于 $m = n^2$，我们有

$$\Pr_S[T \subseteq S] \leq \left(\frac{10n\log n}{n^2}\right)^k = (n/(10\log n))^{-k}.$$ ■

向日葵界。 为了证明向日葵界，我们首先证明 D_0 具有一种较弱形式的有界独立性。

引理 5.11 （ D_0的弱独立形式）。 假设 $t \leq n^{0.1}$。任取由 $[m]$ 和 $j \in [t]$ 中的不同元素组成的元组 $\tau :=(i_1, \ldots, i_t)$，使得相对于 τ， i_j并非 $10k$-包含。那么，

$$\Pr_{a\sim D_0}\left[a_{i_j} = 1 \mid a_{i_1}, \ldots, a_{i_{j-1}}\right] \geq \Omega(1/k).$$

证明。 令 $S_\ell :=$ supp $M[i_\ell]$ 对于 $\ell \in [j]$，且 $R := S_j \setminus \bigcup_{\ell=1}^{j-1} S_\ell$。对于每个 $T \subseteq [n]$，令

$$X_T := \sum_{\ell\in T} u_\ell,$$

其中 u_ℓ's 是用于定义 D_0 的随机变量。如果 i_j 不是关于 τ 的 $10k$-包含的，则有

$$|R| \geq |S_j| - 10k \geq (s/2) - 10k.$$

由于 $X_{[n]} = 0$，我们有

$$\begin{aligned}
&\Pr_{a\sim D_0}\left[a_{i_j} = 1 \mid a_{i_1}, \ldots, a_{i_{j-1}}\right] \\
&\quad= \sum_{p=-10k}^{10k} \Pr_{a\sim D_0}\left[X_{S_j\setminus R} = -p, X_R = p \mid a_{i_1}, \ldots, a_{i_{j-1}}\right] \\
&\quad= \sum_{p=-10k}^{10k} \Pr_{a\sim D_0}\left[X_R = p \mid X_{S_j\setminus R} = -p, a_{i_1}, \ldots, a_{i_{j-1}}\right] \Pr_{a\sim D_0}\left[X_{S_j\setminus R} = -p \mid a_{i_1}, \ldots, a_{i_{j-1}}\right] \\
&\quad= \sum_{p=-10k}^{10k} \Pr_{a\sim D_0}\left[X_R = p\right] \Pr_{a\sim D_0}\left[X_{S_j\setminus R} = -p \mid a_{i_1}, \ldots, a_{i_{j-1}}\right],
\end{aligned}$$

其中最后一个等式是由 u 各坐标之间的独立性得出的。注意，对于每个 $p \in [-10k, 10k]$ 和 $r := |R|$，以及 $Y_\ell \sim \text{Rademacher}(\ell)$ 是一个拉德马赫随机变量，对每个 $\ell \in \{0, \ldots, r\}$ 取 ℓ 个独立样本，我们有

$$\begin{aligned}
\Pr_{a\sim D_0}\left[X_R = p\right] &= \sum_{U\subseteq R} \Pr_{a\sim D_0}\left[u^{-1}(0) = U, X_R = p\right] \\
&= \sum_{U\subseteq R} \Pr_{a\sim D_0}\left[X_{R\setminus U} = p \mid u^{-1}(0) = U\right] \Pr_{a\sim D_0}\left[u^{-1}(0) = U\right] \\
&\geq \sum_{U\subseteq R, ||U|-r/3|\leq \delta r/3} \Pr_{a\sim D_0}\left[Y_{r-|U|} = p\right] \Pr_{a\sim D_0}\left[u^{-1}(0) = U\right] \\
&\geq \left(\min_{w\in[r] \text{ s.t. } |w-r/3|\leq \delta r/3} \Pr_{a\sim D_0}\left[Y_{r-w} = p\right]\right) \left(\sum_{U\subseteq R, ||U|-r/3|\leq \delta r/3} \Pr_{a\sim D_0}\left[u^{-1}(0) = U\right]\right),
\end{aligned}$$

对任意 $\delta \in [0, 1]$。注意 $u^{-1}(0) \sim$ 二项分布$(r,\ 1/3) =:\ B$；因此，根据切尔诺夫不等式 [MU17]，

$$\Pr_B\left[|B - \mathbb{E}B| > \delta \mathbb{E}B\right] \leq 2e^{-\delta^2 \mathbb{E}B/3},$$

并且，对于 $\delta := \sqrt{18/r}$，

$$\Pr_B\left[|B - r/3| > \delta r/3\right] \leq 2e^{-2} \leq 1/2.$$

因此，

$$\sum_{U\subseteq R, ||U|-r/3|\leq \delta r/3} \Pr_{a\sim D_0}\left[u^{-1}(0) = U\right] \geq 1/2.$$

现在我们只需　　求出 $\mathbf{Pr}_{a\sim D_0}\left[Y_v = p\right]$ 的良好估计，其中 $v :\ = r - w$ 满足 $w \in [r]$

$$|w - r/3| \leq \sqrt{2r}.$$

为了得到这些估计，我们将使用标准不等式来处理二项式系数。首先注意到

$$\Pr_{a\sim D_0}[Y_v = p] = \binom{v}{(v+p)/2} 2^{-v}.$$

利用对每个 $x \le 1$ 都有 $1 - x \ge e^{-x/(1-x)}$，我们得到

$$\begin{aligned}
\frac{\binom{v}{(v+p)/2}}{\binom{v}{v/2}} &= \prod_{i=0}^{p/2-1} \frac{v/2 - i}{v/2 + p/2 - i} \\
&\ge \left(\frac{v/2 - p/2}{v/2}\right)^{p/2} \\
&\ge \left(e^{-\frac{p}{v}\frac{1}{1-p/v}}\right)^{p/2} \\
&\ge e^{-\frac{p^2}{2(v-p)}},
\end{aligned}$$

并且，利用 $\binom{v}{v/2} = \Theta\left(2^v/\sqrt{v}\right)$，我们得到

$$\begin{aligned}
\Pr_{a\sim D_0}[Y_v = p] &\ge e^{-\frac{p^2}{2(v-p)}} \binom{v}{v/2} 2^{-v} \\
&\ge \Omega\left(\frac{e^{-\frac{p^2}{2(v-p)}}}{\sqrt{v}}\right).
\end{aligned}$$

由于 $p \in [-10k, 10k]$ 且

$$200k^2 = s \ge v \ge 2r/3 - \sqrt{18r} \ge r/3 \ge \frac{1}{3}((s/2) - 10k) = \frac{1}{3}(200k^2 - 10k) \ge 60k^2$$

当 k 足够大时，我们得到

$$\begin{aligned}
\Pr_{a\sim D_0}[Y_v = p] &\ge \Omega\left(\frac{e^{-\frac{200k^2}{2\cdot(60k^2-10k)}}}{\sqrt{k^2}}\right) \\
&\ge \Omega\left(1/k\right).
\end{aligned}$$

因此，我们得到

$$\Pr_{a\sim D_0}\left[a_{i_j} = 1 \mid a_{i_1}, \ldots, a_{i_{j-1}}\right] \ge \Omega\left(1/k\right) \cdot \frac{1}{2} = \Omega(1/k). \qquad \blacksquare$$

我们的主要组合工具是经典向日葵引理 [ER60](另见 [Juk11，第 6 节。1])。回想一下，向日葵是由集合 $S_1, \ldots, S_r$ 组成的集合族，其两两交集$S_i \cap S_j$ 都相同。 [ALWZ21] 改进后的界以及后续研究的结果，都不会对我们的界产生实质性影响。

引理 5.12 （向日葵引理）。 如果 $\mathcal{S}$ 是一个集合大小至多为 $\ell \in [k]$ 的集合族，且 $|\mathcal{S}| \ge \ell!(r-1)^\ell$，那么 $\mathcal{S}$ 包含一个有 r 个集合的向日葵。

现在我们来证明 D_0-向日葵界。为了使这个界更简洁，也更容易证明，我们现在设定 k的取值。我们令

$$k := \lceil (\log m)^{1/2} \rceil. \tag{12}$$

由于使用了经典的向日葵引理，这是唯一需要设定 $k = n^{o(1)}$ 的地方。

引理 5.13 （D_0-向日葵引理）。对于每个 $\ell \in [k]$，都有 $r(D_0,\ \ell,\ m^{-4k}) \leq 2k^{2\ell+1}\ell \log\ m$。

证明。设 $\varepsilon : = m^{-4k}$。设 $\mathcal{S}$ 是一个 ℓ-均匀分布的集合族，其大小大于（$2k^{2\ell}\ell\log(1/\varepsilon)$）$^{\ell}$。根据引理 5.12，存在一个向日葵 $\mathcal{S}' \subseteq \mathcal{S}$，其

$$r := 2k^{2\ell}\log(1/\varepsilon)$$

集合具有某个核 $K := \bigcap_{S\in\mathcal{S}'} S$。注意，

$$r = 8k^{2\ell+1}\log m \ll n^{0.1},$$

根据我们对$k = \sqrt{\log m}$的选择以及(公式（10）)。

现在我们证明 $\mathcal{S}'$ 是一个（$\mathcal{D}_0$，ℓ，ε）-向日葵。设 $\mathcal{F}$:= $\{S \setminus K :\ S \in \mathcal{S}'\}$。只需证明，对于 F: $= F_{\mathcal{F}}$，我们有

$$\Pr_{a\sim\mathcal{D}_0}[F(a) = 0] \leq \varepsilon.$$

令 F_1、F_2、.....、F_r 为 $\mathcal{F}$ 的集合。令

$$\tau := (i_1, i_2, \ldots, i_t)$$

F_1、F_2、.....、F_r 这些项中出现的变量所对应的所有指标，按这些项的顺序排列而成的序列（在每一项内部，变量的顺序任意）。由于 $t \leq rk \leq n^{0.1}$，且根据 M 的选择（见定义 5.7，第 (3) 项），τ 中至多有 $t/2k \leq r/2$ 个指标相对于 τ 是$10k$-包含的。特别地，这些指标分布在 F_1、.....、F_r 中至多 $r/2$ 个“受损”项中。在其余项中，所有指标相对于 τ 都不是 $10k$-包含的。移除受损项后，得到一个含有 $r' \geq r/2$ 个集合的子族 $\mathcal{F}' \subseteq \mathcal{F}$，其中所有指标相对于 τ 都不是 $10k$-包含的。令 F'_1、.....、$F'_{r'}$ 为 $\mathcal{F}'$ 的集合。

对于任意 $j \in [r']$，我们都可以对 F'_j的每个元素应用引理5.11（回顾一下，F'_j至多含有ℓ个文字），从而得到

$$\Pr_{a\sim D_0}\left[F'_j(a) = 1 \mid F'_1(a) = 0, \ldots, F'_{j-1}(a) = 0\right] \geq \Omega(1/k)^{\ell}.$$

因此，我们得到

$$\Pr_{a\sim D_0}\left[F'_j(a) = 0 \mid F'_1(a) = 0, \ldots, F'_{j-1}(a) = 0\right] \leq 1 - \Omega(1/k)^{\ell},$$

因此，作为结果，

$$\Pr_{a\sim D_0}[F(a) = 0] \leq \Pr_{a\sim D_0}\left[F'(a) = 0\right] \leq \left(1 - \Omega(1/k)^{\ell}\right)^{r'} \leq \exp(-rk^{-2\ell}/2) = \varepsilon,$$

当 k足够大时。 ■

总结一下。 现在我们可以应用定理3.3，完成证明。

定理 *1.4*的证明。 我们已经证明，存在一个矩阵序列 $(M_n)_{n\in\mathbb{N}}$，其元素来自 $\mathbb{R}$，使得 M_n 是一个 $n \times m$ 矩阵，其中 $m := n^2$ 并且 M_n 是 良态的 （定义 5.7）。我们还构造了两个分布 D_1, D_0（定义 5.8），它们支撑在字符串 $\{0,1\}^m$上，并满足

1. $\Pr_{x\sim D_i}[f_M(x) = i] \geq \alpha$ 对每个 $i \in \{0,1\}$均成立，其中 $\alpha > 0$ 是某个常数（定义 5.7 和观察 5.9）；

2. D_1 是 $n^{0.1}$-重（$n/(10 \log n)$）-扩展的（引理 5.10）；3. $r(D_0, \ell, m^{-4k}) \leq 8k^{2\ell+1} \log m$ 对每个 $\ell \in [k]$ 均成立（引理 5.13）。

取 $w := k$ 在定理 3.3 中，并注意到 $\alpha m^{-3k} \leq m^{-4k}$，我们得到存在一个常数 $\beta > 0$，使得 f_M 的单调复杂度为

$$\left(\frac{\beta n}{k^{2k+1}\log^2 n}\right)^k = m^{\Omega(\sqrt{\log m})}.$$

非单调电路上界 f_M 在引理 5.1中得到了证明。 ■

参考文献

[AB87] Noga Alon 和 Ravi B. Boppana。《布尔函数的单调电路复杂度》。组合学，7(1):1–22，1987。doi:10.1007/BF02579196。[ABO99] Eric Allender、Robert Beals 和 Mitsunori Ogihara。《矩阵秩与可行线性方程组的复杂度》。计算复杂性，8(2):99–126，1999。URL: https://doi.org/10.1007/s000370050023，doi:10.1007/S000370050023。[AG87] Mikl´os Ajtai 和 Yuri Gurevich。《单调与正》。ACM杂志，34(4):1004– 1015，1987。doi:10.1145/31846.31852。[AGG+25] Yaroslav Alekseev、Mika G¨o¨os、Ziyi Guan、Gilbert Maystre、Artur Riazanov、Dmitry Sokolov 和 Weiqiang Yuan。《广义 Linial–Nisan 猜想对析取范式公式不成立》。载于 Srikanth Srinivasan（编），第 40 届计算复杂性会议，CCC 2025，2025 年 8 月 5–8 日，加拿大多伦多，LIPIcs 第 339 卷，第 29:1–29:13 页。Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2025。URL: https://doi.org/10.4230/LIPIcs.CCC.2025.29，doi:10.4230/LIPICS. CCC.2025.29。[ALWZ21] Ryan Alweiss、Shachar Lovett、Kewen Wu 和 Jiapeng Zhang。《向日葵引理的改进界》。数学年刊，2(194(3)):795–815，2021。doi:10.4007/annals.2021.194.3.5。[AW24] Robert Andrews 和 Avi Wigderson。《用于线性代数问题的常数深度算术电路》。载于第 65 届 IEEE 计算机科学基础年会，FOCS 2024，2024 年 10 月 27–30 日，美国伊利诺伊州芝加哥，第 2367–2386 页。IEEE，2024。doi:10.1109/ FOCS61266.2024.00138。[AY24] Daniel Avraham 和 Amir Yehudayoff。《矩阵的块状秩》。计算复杂性，33(1):2，2024。URL: https://doi.org/10.1007/s00037-024-00248-1，doi:10.1007/S00037-024-00248-1。[Baz09] Louay M. J. Bazzi。《多对数级独立性可以欺骗析取范式公式》。SIAM 计算杂志，38(6):2220–2272，2009。doi:10.1137/070691954。

[BCW21] Tolson Bell、Suchakree Chueluecha 和 Lutz Warnke。《关于向日葵的注记》。离散数学，344(8):112328，2021。预印本：https://arxiv.org/abs/2009.09327。arXiv:arXiv: 2009.09327, doi:10.1016/j.disc.2021.112328。[Bei11] Amos Beimel。《秘密共享方案：综述》。载于 Yeow Meng Chee、Zhenbo Guo、San Ling、Fengjing Shao、Yuansheng Tang、Huaxiong Wang 和 Chaoping Xing（编），编码与密码学——第三届国际研讨会 IWCC 2011，2011 年 5 月 30 日至 6 月 3 日，中国青岛。论文集，计算机科学讲义第 6639 卷，第 11–46 页。施普林格，2011。doi:10.1007/978-3-642-20901-7_2.[Ber84] Stuart J. Berkowitz。《使用少量处理器在短并行时间内计算行列式》。信息处理快报，18(3):147–150，1984。doi:10.1016/0020-0190(84)90018-8。[BGW99] L´aszl´o Babai、Anna G´al 和 Avi Wigderson。《单调张成程序的超多项式下界》。组合学，19(3):301–319，1999。URL: https://doi.org/10.1007/s004930050058，doi:10.1007/S004930050058。[BM25] Jaroslaw Blasiok 和 Linus Meierh¨ofer。《单调电路进行团近似的困难性》。载于 Srikanth Srinivasan（编），第 40 届计算复杂性会议，CCC 2025，2025 年 8 月 5–8 日，加拿大多伦多，LIPIcs 第 339 卷，第 4:1–4:20 页。Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2025。URL: https://doi.org/10.4230/LIPIcs.CCC.2025.4，doi: 10.4230/LIPICS.CCC.2025.4。[Cav20] Bruno Cavalar。《计算复杂性中的向日葵定理》。硕士论文，Instituto de Matem´atica e Estat´ıstica，圣保罗大学，2020。doi:10.11606/D.45.2020. tde-25112020-162107。[CDGM22] Arkadev Chattopadhyay、Rajit Datta、Utsab Ghosal 和 Partha Mukhopadhyay。《生成树多项式的单调复杂度再探》。载于 Mark Braverman（编），第 13 届理论计算机科学创新会议，ITCS 2022，2022 年 1 月 31 日至 2 月 3 日，美国加利福尼亚州伯克利，LIPIcs 第 215 卷，第 39:1–39:21 页。Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2022。URL: https://doi.org/10.4230/LIPIcs.ITCS.2022.39，doi: 10.4230/LIPICS.ITCS.2022.39。[CDM21] Arkadev Chattopadhyay、Rajit Datta 和 Partha Mukhopadhyay。《通过通信复杂度证明单调算术电路的下界》。载于 Samir Khuller 和 Virginia Vassilevska Williams（编），STOC ’21：第 53 届 ACM SIGACT计算理论研讨会，线上会议，意大利，2021 年 6 月 21–25 日，第 786–799 页。ACM，2021。doi:10.1145/3406325. 3451069。[CGM22] Arkadev Chattopadhyay、Utsab Ghosal 和 Partha Mukhopadhyay。《通过图内积分离算术单调层级》。载于 Anuj Dawar 和 Venkatesan Gu- ruswami（编），第 42 届 IARCS软件技术基础与理论计算机科学年会，FSTTCS 2022，2022 年 12 月 18–20 日，印度理工学院马德拉斯分校，印度金奈，LIPIcs 第 250 卷，第 12:1–12:20 页。Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2022。URL: https://doi.org/10.4230/LIPIcs.FSTTCS.2022.12，doi:10.4230/ LIPICS.FSTTCS.2022.12。[CGR+25] Bruno Cavalar、Mika G¨o¨os、Artur Riazanov、Anastasia Sofronova 和 Dmitry Sokolov。《匹配的单调电路复杂度》。CoRR，abs/2507.16105，2025。URL: https://doi.org/ 10.48550/arXiv.2507.16105, arXiv:2507.16105，doi:10.48550/ARXIV.2507.16105。[CKR22] Bruno Pasqualotto Cavalar、Mrinal Kumar 和 Benjamin Rossman。《基于鲁棒向日葵的单调电路下界》。Algorithmica，84(12):3655–3685，2022。URL: https://doi. org/10.1007/s00453-022-01000-3，doi:10.1007/S00453-022-01000-3。

[CO23] Bruno Cavalar 和 Igor Oliveira。常深度电路与单调电路。在第 38 届计算复杂性会议（CCC）论文集，第 264 卷 LIPIcs，第 29:1–29:37 页。Schloss Dagstuhl，2023 年。doi:10.4230/LIPIcs.CCC.2023.29。[COS17] Xi Chen、Igor Oliveira 和 Rocco Servedio。对于浅层单调电路而言，加法比计数难度高出指数级。在第 49 届计算理论研讨会（STOC）论文集，第 1232–1245 页。ACM，2017 年。doi:10.1145/3055399.3055425。[Csa76] L´aszl´o Csanky。快速并行矩阵求逆算法。SIAM计算杂志，5(4):618–623，1976 年。doi:10.1137/0205042。[ˇDHJ04] Pavol ˇDuriˇs、Juraj Hromkoviˇc 和 Stasys Jukna。论多分区通信复杂度。Information and Computation，194(1):49–75，2004 年。doi:10.1016/j.ic.2004.05.002。[dRV25] Susanna F. de Rezende 和 Marc Vinyals。利用彩色向日葵进行提升。在 Rahul San- thanam（编）所编的第 40 届计算复杂性会议（CCC 2025）论文集，第 339 卷《莱布尼茨国际信息学会议录》（LIPIcs），第 36:1–36:19 页，德国 Dagstuhl，2025 年。Schloss Dagstuhl – Leibniz-Zentrum f¨ur Informatik。doi:10.4230/LIPIcs.CCC.2025.36。[ER60] P. Erd¨os 和 R. Rado。集合系统的交集定理。J. Lond. Math. Soc.，35(1):85–90，1960 年。[Erd45] Paul Erd˝os。论 Littlewood 和 Offord 的一个引理。Bull. Amer. Math. Soc.，51(12):898–902，1945 年。[FGT19] Stephen A. Fenner、Rohit Gurjar 和 Thomas Thierauf。二分图完美匹配的确定性并行算法。Communications of the ACM，62(3):109–115，2019 年。doi:10.1145/ 3306208。[FMP+15] Samuel Fiorini、Serge Massar、Sebastian Pokutta、Hans Raj Tiwary 和 Ronald de Wolf。组合优化中多面体的指数下界。J. ACM，62(2):17:1–17:23，2015 年。doi:10.1145/2716307。[GGKS20] Ankit Garg、Mika G¨o¨os、Pritish Kamath 和 Dmitry Sokolov。由归结得到的单调电路下界。Theor. Comput.，16:1–30，2020 年。URL: https://doi.org/10.4086/toc.2020. v016a013，doi:10.4086/TOC.2020.V016A013。[GKRS18] Mika G¨o¨os、Pritish Kamath、Robert Robere 和 Dmitry Sokolov。单调复杂度与 TFNP 中的探索。Electron. Colloquium Comput. Complex.，TR18-163，2018 年。URL: https: //eccc.weizmann.ac.il/report/2018/163，arXiv:TR18-163。[GS92] Michelangelo Grigni 和 Michael Sipser。单调复杂度。在《布尔函数复杂度》，伦敦数学学会讲义系列，第 57–75 页。剑桥大学出版社，1992 年。doi:10.1017/CBO9780511526633.006。[Hay11] Thomas P. Hayes。分离 k-方通信复杂度层次：Zarankiewicz 问题的一个应用。离散数学与理论计算机科学，13(4):15–22，2011 年。doi:10.46298/dmtcs.546。[HR00] Danny Harnik 和 Ran Raz。关于单调规模的更高下界。在第三十二届 ACM 计算理论研讨会论文集，STOC ’00，第 378–387 页，纽约州纽约，美国，2000 年。计算机协会。doi:10.1145/335305.335349。[HY09] Pavel Hrubes 和 Amir Yehudayoff。常次数多项式的单调分离。Inf. Process. Lett.，110(1):1–3，2009 年。URL: https://doi.org/10.1016/j.ipl.2009.09.003，doi:10.1016/J.IPL.2009.09.003。

[HY13] Pavel Hrubes 和 Amir Yehudayoff。非交换情形下，公式比单调电路强大得多。在第 28 届计算复杂性会议论文集，CCC 2013，美国加利福尼亚州 K.lo Alto，2013 年 6 月 5–7 日，第 10–14 页。IEEE计算机学会，2013 年。doi:10.1109/CCC.2013.11。[HY16] Pavel Hrubes 和 Amir Yehudayoff。论等周剖面与计算复杂性。在 Ioannis Chatzigiannakis、Michael Mitzenmacher、Yuval Rabani 和 Davide Sangiorgi（编）所编的第 43 届国际自动机、语言与程序设计学术会议，ICALP 2016，2016 年 7 月 11–15 日，意大利罗马，第 55 卷 LIPIcs，第 89:1–89:12 页。Schloss Dagstuhl - Leibniz- Zentrum f¨ur Informatik，2016 年。URL: https://doi.org/10.4230/LIPIcs.ICALP.2016.89，doi: 10.4230/LIPICS.ICALP.2016.89。[HY21] Pavel Hrubes 和 Amir Yehudayoff。牛顿多面体的影子。在 Valentine Kabanets（编）所编的第 36 届计算复杂性会议，CCC 2021，2021 年 7 月 20–23 日，加拿大安大略省多伦多（线上会议），第 200 卷 LIPIcs，第 9:1–9:23 页。Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2021 年。URL: https://doi.org/10.4230/LIPIcs.CCC.2021.9，doi:10.4230/LIPICS.CCC.2021.9。[JS20] Stasys Jukna 和 Hannes Seiwert。纯动态规划的近似局限性。SIAM 计算杂志，49(1):170–205，2020 年。doi:10.1137/18M1196339。[Juk11] Stasys Jukna。极值组合学——及其在计算机科学中的应用。理论计算机科学文本：EATCS 系列。施普林格，2011 年。doi:10.1007/ 978-3-642-17364-6。[Juk15] Stasys Jukna。热带电路与动态规划的下界。Theory Comput. Syst.，57(1):160–194，2015 年。doi:10.1007/s00224-014-9574-4。[Kas67] P. W. Kasteleyn。图论与晶体物理学。在 Frank Harary（编）所编的《图论与理论物理学》，第 43–110 页。Academic Press，伦敦，1967 年。编著中的章节。[KW93] Mauricio Karchmer 和 Avi Wigderson。论张成程序。在第八届复杂性理论结构会议论文集，美国加利福尼亚州圣迭戈，1993 年 5 月 18–21 日，第 102–111 页。IEEE计算机学会，1993 年。doi:10.1109/SCT.1993.336536。[KW15] Volker Kaibel 和 Stefan Weltge。相关多胞体的扩展复杂性呈指数增长的一个简短证明。Discrete Comput. Geom.，53(2):397–401，2015 年。doi:10.1007/ s00454-014-9655-9。[LO43] J. E. Littlewood 和 A. C. Offord。随机代数方程实根的数量。iii。Rec. Math. /Mat. Sbornik/ N.S.，12(54):277–286，1943 年。[Lov79] L´aszl´o Lov´asz。论行列式、匹配与随机算法。在 L. Budach（编）所编的《计算理论基础》（FCT’79），第 565–574 页，柏林，1979 年。Akademie-Verlag。[MS77] F. J. MacWilliams 和 N. J. A. Sloane。纠错码理论。第一、二部分，《北荷兰数学图书馆》第 16 卷。Elsevier（北荷兰），阿姆斯特丹，1977 年。[MU17] Michael Mitzenmacher 和 Eli Upfal。《概率与计算》。剑桥大学出版社，剑桥，第二版，2017 年。算法与数据分析中的随机化和概率技术。[Mul87] Ketan Mulmuley。在任意域上计算矩阵秩的快速并行算法。组合学，7(1):101–104，1987 年。doi:10.1007/BF02579205。[MV97] Meena Mahajan 和 V. Vinay。行列式：组合学、算法与复杂性。Chic. J. Theor. Comput. Sci.，1997，1997 年。URL: http://cjtcs.cs.uchicago.edu/articles/1997/ 5/contents.html。

[Nis91] Noam Nisan。非交换计算的下界（扩展摘要）。载于Cris Koutsougeras和Jeffrey Scott Vitter编，《第23届ACM计算理论研讨会论文集》，1991年5月5日至8日，美国路易斯安那州新奥尔良，第410–418页。ACM，1991。doi:10.1145/103418.103462.[NNP04] Ventzislav Nikov、Svetla Nikova和Bart Preneel。单调跨度程序的规模。载于Carlo Blundo和Stelvio Cimato编，《通信网络安全：第4届国际会议（SCN 2004）论文集》，意大利阿马尔菲，2004年9月8日至10日，修订精选论文，计算机科学讲义第3352卷，第249–262页。施普林格，2004。doi:10.1007/978-3-540-30598-9_18.[Oko82] Elizaveta Okol' nishnikova。否定对有界深度公式实现单调布尔函数复杂度的影响。《离散分析方法》，(38):74–80，1982。[PS96] Pavel Pudl´ak和Jir´ı Sgall。代数计算模型与代数证明系统的插值。载于Paul Beame和Samuel R. Buss编，《证明复杂性与可行算术：DIMACS研讨会论文集》，美国新泽西州新不伦瑞克，1996年4月21日至24日，DIMACS离散数学与理论计算机科学丛书第39卷，第279–295页。DIMACS/AMS，1996。URL: https://doi.org/10.1090/dimacs/039/ 15，doi:10.1090/DIMACS/039/15。[Rao25] Anup Rao。向日葵族的故事，2025 年。URL: https://arxiv.org/abs/2509.14790，arXiv:2509.14790。[Raz85] Alexander Razborov。某些布尔函数单调复杂度的下界。《苏联科学院通报》，281(4):798–801，1985。[Raz92] Alexander A. Razborov。不相交性的分布复杂度。《理论计算机科学》，106(2):385–390，1992。doi:10.1016/0304-3975(92)90260-M。[Ros14] Benjamin Rossman。随机图上 k-团的单调复杂度。《SIAM计算杂志》，43(1):256–279，2014。doi:10.1137/110839059。[Rou15] Tim Roughgarden。通信复杂度（面向算法设计者），2015。URL: https: //arxiv.org/abs/1509.06257。[RW92] Ran Raz和Avi Wigderson。匹配问题的单调电路需要线性深度。《ACM杂志》，39(3):736–744，1992。doi:10.1145/146637.146684。[RY11] Ran Raz和Amir Yehudayoff。多线性公式、最大划分差异与混合源提取器。《计算机与系统科学杂志》，77(1):167–190，2011。doi:10.1016/j.jcss.2010.06. 013。[Sho88] Victor Shoup。有限域上寻找不可约多项式的新算法。载于《第29届年度计算机科学基础研讨会》，美国纽约州怀特普莱恩斯，1988年10月24日至26日，第283–290页。IEEE计算机学会，1988。doi:10.1109/SFCS.1988.21944。[Sri20] Srikanth Srinivasan。单调VP与单调VNP之间的强指数分离。《ACM计算理论汇刊》，12(4):12，2020。编号23。doi:10.1145/3417758。[Sta97] Richard P. Stanley。《枚举组合学》。第1卷，剑桥高等数学研究第49卷。剑桥：剑桥大学出版社，1997。[SY10] Amir Shpilka和Amir Yehudayoff。算术电路：近期成果综述与开放问题。《理论计算机科学前沿与趋势》，5(3-4):207–388，2010。doi:10.1561/0400000039。[Tal17] Avishay Tal。AC0傅里叶谱的紧确界。载于Ryan O'Donnell编，《第32届计算复杂性会议（CCC 2017）论文集》，2017年7月6日至9日，拉脱维亚里加，LIPIcs第79卷，第15:1–15:31页。Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2017。URL: https://doi.org/10.4230/LIPIcs.CCC.2017.15，doi:10.4230/LIPICS.CCC.2017.15。

[Tar88] ´Eva Tardos。单调与非单调电路复杂度之间的差距是指数级的。组合学，8(1):141–142，1988。doi:10.1007/BF02122563。[Val79] Leslie G. Valiant。代数中的完备性类。载于Michael J. Fischer、Richard A. DeMillo、Nancy A. Lynch、Walter A. Burkhard和Alfred V. Aho编，第*11*届年度*ACM*计算理论研讨会论文集，*1979*年*4*月*30*日至*5*月*2*日，美国佐治亚州亚特兰大，第249–261页。ACM，1979。doi:10.1145/800135.804419。[Val80] Leslie G. Valiant。否定即使在较小深度下也能发挥强大作用。理论计算机科学，12:303–314，1980。doi:10.1016/0304-3975(80)90060-2。[W70] Moon J W。标记树计数。加拿大数学大会，蒙特利尔，1970。[Yeh19] Amir Yehudayoff。分离单调VP与单调VNP。载于Moses Charikar和Edith Cohen编，第*51*届*ACM SIGACT*计算理论研讨会（*STOC 2019*）论文集，*2019*年*6*月*23*日至*26*日，美国亚利桑那州菲尼克斯，第425–429页。ACM，2019。doi:10.1145/3313276.3316311。