arXiv:2301.01676v1 [cs.CC] 4 Jan 2023

齐次非交换电路的新下界

Prerona Chatterjee * Pavel Hrubeˇs†

2023年1月5日

摘要

我们给出了齐次非交换电路规模的若干新下界。我们给出一个显式的、次数为d 的齐次二元多项式，它要求齐次非交换电路的规模至少为 $\Omega(d/\log d)$。对于一个n元多项式，当$n > 1$时，如果$d \leq n$，结果可改进为 $\Omega(nd)$；如果$d \geq n$，则可改进为 $\Omega(nd^{\log_n \log d})$。在相同假设下，我们还为中心对称多项式的有序版本给出了一个二次下界。

1 引言

算术电路复杂性旨在根据多项式在代数计算模型中的计算难度对其进行分类。最自然的模型是算术电路：从变量或常数出发，电路通过加法和乘法运算计算出新的多项式。问题在于需要多少次这样的运算。最具挑战性的问题是，针对计算低次数多项式的算术电路证明超多项式下界。这被称为VP vs VNP 问题，是著名的 P vs. NP 问题的代数类比。Baur 和 Strassen 的经典结果[Str73, BS83] 给出了一个 $\Omega(n \log d)$ 下界，适用于一个 n 元次数为 d 的多项式。此后，人们通过对计算模型施加各种限制，获得了多种下界，例如针对算术公式或单调电路的结果 [Kal85, Val80]。但 Baur 和 Strassen 的结果仍然是针对不受限制的算术电路所知的最强下界。

本文关注非交换情形，即乘法不满足乘法交换性。从 Hyafil 的开创性工作开始 [Hya77] 以及 Nisan 的工作 [Nis91],

*以色列特拉维夫大学。本文是在作者于布拉格捷克科学院数学研究所从事博士后研究期间完成的，并得到捷克科学基金会 GA ˇCR 项目 19-27871X 的资助。电子邮箱：prerona.ch@gmail.com

†布拉格捷克科学院数学研究所。本文得到捷克科学基金会 GAˇCR 项目 19-27871X 的资助。电子邮箱：pahrubes@gmail.com。

非交换电路是一个受到广泛研究的对象。缺乏交换性会严重限制计算能力，因此证明电路下界似乎更容易。Nisan 为非交换公式给出了指数下界，而在交换情形下，最佳下界仅为二次 [Kal85, CKSV22]。此后，人们似乎认为，非交换电路的指数下界已近在咫尺。最近，Limaye、Srinivasan 和 Tavenas [TLS22] 在齐次常数深度情形下证明了这样的下界。他们证明，对于 Δ 迭代矩阵乘法多项式的任意常数深度非交换齐次电路，若该多项式定义在 n 个变量上且次数为 d，则电路规模至少为 $n^{\Omega(d^{\frac{1}{\Delta}})}$。然而，对于一般电路，即使在非交换情形下，最强的下界仍然是 $\Omega(n \log d)$[Str73, BS83]。

我们将这一 $\Omega(nd/\log d)$ 下界提升到第 2 节，但需要额外假设非交换电路也是齐次的（定义见）。在非交换情形下，当 $= 2$ 时，这一结果已颇有意义：我们得到一个次数为 d 的二元多项式，其所需的电路规模几乎与 d 成线性关系。众所周知，计算次数为 d 的齐次多项式的电路（无论是否交换），都可以转换为等价的齐次电路，且规模至多增加 d^2 倍（例如参见 [HWY11]）。因此，如果 d 较小，或者目标是证明超多项式下界（如 VP 与 VNP 问题），那么齐次性并非严格限制。不过，我们的结果不属于这两类，而且我们不知道如何去掉齐次性限制。尽管如此，我们坚信这一限制可以去除，非交换电路下界的突破已近在眼前。

2 符号与预备知识

设 $\mathbb{F}$ 是一个域。$\mathbb{F}$ 上的非交换多项式是由变量和域元素的乘积构成的形式和。我们假设变量之间的乘法不满足交换律，但满足加法交换律，且变量与 $\mathbb{F}$ 的元素可交换。以变量 $x_1, \ldots, x_n$ 为变量的非交换多项式环记作 $\mathbb{F}\langle x_1, \ldots, x_n \rangle$。如果 f 中所有非零系数单项式的次数都相同，则称多项式为齐次。

非交换算术电路 $\mathcal{C}$ 是如下的一个有向无环图。入度为零的节点（或门）标记为一个变量或 $\mathbb{F}$ 中的一个域元素。所有其他节点的入度均为二，并标记为 $+$ 或 $\times$。指向标记为 $\times$ 的门的两条边分别标记为*左*和*右*，以表示乘法顺序。入度为零的门称为*输入门*；出度为零的门称为*输出门*。

$\mathcal{C}$ 中的每个节点都以显然的方式计算一个非交换多项式。若 $\mathcal{C}$ 中存在一个门计算 f（不一定是输出门），则称 $\mathcal{C}$ *计算多项式* f。若 $\mathcal{C}$ 中的每个门都计算一个齐次多项式，则称 $\mathcal{C}$ *是齐次的*。给定一个电路 $\mathcal{C}$，令 $\widehat{\mathcal{C}} := \{f : \text{若 } \mathcal{C} \text{ 中的某个门计算 } f\}$。

如果一个乘积门的两个输入都计算非零次多项式，则称该乘积门为非标量。我们将 $\mathcal{C}$ 的规模定义为其中非输入门的数量，将 $\mathcal{C}$的非标量规模 定义为其中非标量乘积门的数量。

给定整数 n_1, n_2, $[n_1, n_2]$，区间为 $\{n_1, n_1+1, \ldots, n_2\}$，且 $[n] := [1, n]$。

注意：除非另有说明，电路和多项式均假定为非交换的，且底域 $\mathbb{F}$ 固定但任意。

3 主要结果

对于单变量多项式，交换计算与非交换计算之间没有区别。即使只有两个变量，非交换多项式也呈现出丰富得多的结构。次数为d 的变量 x_0,x_1 的单项式有 2^d 个（而交换情形下只有 $d+1$ 个）；因此，一般二元多项式需要规模随d呈指数增长的电路。

我们的第一个结果是一个关于d的近乎线性的下界。困难多项式是一个二元单项式（变量x_0,x_1的一个特定乘积）。

定理 1。对于每个 $d > 1$，都存在一个次数为 d 的显式二元单项式，使得任何计算它的齐次非交换电路都具有 $\Omega(d/\log d)$的非标量规模。

在备注 10中，我们指出了一个互补结果：对于每个二元单项式，都有$O(d/\log d)$ 的上界。请注意，在交换情形下，每个这样的单项式都可以由规模为$O(\log d)$的电路计算。

对于n元多项式，我们得到了一个更强的结果（困难多项式不再是单项式）。

定理 2。对于每个 n,$d > 1$，都存在一个显式的 n 元齐次多项式，其次数为 d；若 $d \le n$，则该多项式需要一个非标量规模为 $\Omega(nd)$ 的齐次非交换电路；若 $d \ge n$，则需要一个非标量规模为 $\Omega\left(nd^{\log n / \log d}\right)$ 的齐次非交换电路。

定理 1和定理 2分别在第 4.1 节和第 4.2 节中证明 .

给定 $0 \le d$,n，有序对称多项式 OS_n^d 是多项式[1]

$$\mathrm{OS}_n^d(x_1, \ldots, x_n) = \sum_{1 \le i_1 < \cdots < i_d \le n} \left(\prod_{j=1}^{d} x_{i_j} \right).$$

可以将其看作交换基本对称多项式的有序版本。在第 5 节中，我们将证明该多项式的一个下界。

定理 3。若 $2 \le d \le n/2$，则任何计算 $\mathrm{OS}_n^d(x_1, \ldots, x_n)$ 的齐次非交换电路，其非标量规模必须为 $\Omega(dn)$。

[1]因此，当$d > n$时，$\mathrm{OS}_n^0 = 1$和 $\mathrm{OS}_n^d = 0$。

对于中心有序对称多项式 $\mathrm{OS}_n^{\lfloor n/2 \rfloor}$，下界变为 $\Omega(n^2)$。我们还发现，已知的初等对称多项式交换情形上界在非交换情况下同样成立。

命题4。 OS_n^1，……，OS_n^n 可以由规模为 $O(n \log^2 n \operatorname{loglog} n)$ 的非交换电路同时计算，也可以由规模为 $O(n^2)$ 的齐次非交换电路同时计算。

命题中的多对数因子取决于底域，并且对于某些 $\mathbb{F}$s 可以得到改进。此外，在衡量非标量规模时，如果 $\mathbb{F}$ 是无限域，则可以得到 $O(n \log n)$ 上界；由 [BS83]可知该上界是紧的。

有序对称多项式可以与真正对称多项式进行对比

$$S_n^k = \sum_{i_1,\ldots,i_k \in [n] \text{ distinct}} x_{i_1} \cdots x_{i_k},$$

在非交换情形下，早在 S_n^n 就已经与永久式一样难 [HWY11]，并且预计需要指数规模电路。

备注*5*。次数为 d 的多项式可以唯一地写成 $f = \sum_{k=0}^{d} f^{(k)}$，其中 $f^{(k)}$ 是次数为 k 的齐次多项式。众所周知，如果 f 有一个规模为 s 的电路，那么齐次部分 $f^{(0)}$、……、$f^{(d)}$ 可以由一个规模为 $O(sd^2)$ 的齐次电路同时计算（非交换情形也成立[HWY11]）。注意，OS_n^0，……，OS_n^n 是 $\prod_{i=1}^{n}(1 + x_i)$ 的齐次部分，而后者有一个规模为线性的电路。定理 *3* 表明，在这种情况下，齐次化的代价确实是次数的一个因子。◊

4 齐次非交换电路的下界

现在定义我们用于证明下界的测度。设 $f \in \mathbb{F}\langle x_1, \ldots, x_n \rangle$ 是一个次数为 d 的齐次多项式。给定一个区间 $J = [a,b] \subseteq [d],$，多项式 f_J 通过将位置在 *outside* J 之外的变量设为 1 得到。更精确地，若 $\alpha = \prod_{i=1}^{d} x_{j_i}$ 是一个单项式，则 $\alpha^J := \prod_{i=a}^{b} x_{j_i}$，并将该映射线性扩展，使得当$f = \sum_k c_k \alpha_k$时，$f_J = \sum_k c_k \alpha^J{}_k$。给定一个非负整数 ℓ，令

$$\mathcal{F}_\ell(f) = \left\{ f^J \,:\, J \subseteq [d] \text{ is an interval of length } \ell \right\}.$$

给定齐次多项式 $f_1, \ldots, f_m$，我们的困难度量定义为 a s

$$\mu_\ell(f_1, \ldots, f_m) := \dim(\operatorname{span}(\bigcup_{i=1}^{m} \mathcal{F}_\ell(f_i))).$$

这里，$\operatorname{span}(\mathcal{F})$ 表示 $\mathcal{F}$ 中多项式的 $\mathbb{F}$-线性组合所构成的向量空间，而 dim 是其维数。

以下引理给出了测度关于电路规模的界。

引理 6. 设 $\mathcal{C}$ 是一个含有 s 个非标量乘法门的齐次电路。那么对于每个 $\ell \geq 2, \mu_\ell(\widehat{\mathcal{C}}) \leq (\ell-1)s$。

证明。 对 $\mathcal{C}$ 的规模使用归纳法即可。若 $\mathcal{C}$ 仅由输入门组成，则 $\mathcal{F}_\ell(\widehat{\mathcal{C}}) = \emptyset$，因为我们假设 $\ell \geq 2$，且 $\mathcal{C}$ 由线性多项式组成。

否则，假设u 是 $\mathcal{C}$ 的某个输出门，并令 $\mathcal{C}'$ 为移除该门后得到的电路。若u 是加法门或标量乘法门，则

$$\mu_\ell(\widehat{\mathcal{C}}) \leq \mu_\ell(\widehat{\mathcal{C}'}).$$

因为若 u 计算出 f，则 $f = a_1 f_1 + a_2 f_2$，其中 a_1, a_2 是某些常数，且 $f_1, f_2 \in \mathcal{C}'$。若 f 的次数为 d，则对于每个长度为 ℓ 的区间 J，$\subseteq [d]$，$f_J = (a_1 f_1 + a_2 f_2)_J = a_1 f_J + a_2 f_J \in$ 张成空间$(\mathcal{F}_\ell(\widehat{\mathcal{C}'})$。

若u 是一个计算$f = f_1 \cdot f_2$ 的非标量乘积门，则

$$\mu_\ell(\widehat{\mathcal{C}}) \leq \mu_\ell(\widehat{\mathcal{C}'}) + (\ell-1).$$

为证明这一点，假设 f_1, f_2 的次数分别为 d_1 和 d_2，并令 $J \subseteq [d_1 + d_2]$ 为长度为 ℓ的区间。若 J 包含于 $[d_1]$,，则 $f_J = (f_1 f_2)_J = f_J 1 f_2^{\emptyset}$是 $f_J 1$ 的一个标量倍数，因此 f_J 包含于 $\mathrm{span}(\mathcal{F}_\ell(\mathcal{C}'))$；类似地，若 J 包含于 $[d_1 + 1, d_2]$。否则，d_1 和 $d_1 + 1$都包含在 J 中。但这样的区间只有 $\ell - 1$ 个。因此，$\mathcal{F}_\ell(\widehat{\mathcal{C}})$中至多有 $\ell - 1$个多项式不属于 $\mathrm{span}(\mathcal{F}_\ell(\mathcal{C}'))$。

这意味着，μ_ℓ 仅在乘积门处增加，并且在此类门处仅增加 $\ell - 1$。因此，$\mu_\ell(\widehat{\mathcal{C}}) \leq (\ell-1)s$。 □

备注 7。 如果 f 有 n 个变量且次数为 d，则测度 $\mu_\ell(f)$ 至多为 $d - (\ell-1)$ 和 n^ℓ中的较小者。因此，引理 6 本身最多只能给出数量级为 $d \log n / \log d$ 的下界。◊

4.1 单项式的下界

有趣的是，引理 6 为仅仅是变量乘积的 f 也给出了非平凡下界。最简单的例子是一个具有 n个变量且次数为二的乘积。

命题 8。 每个计算 $f = \prod_{i=1}^{n} \prod_{j=1}^{n} (x_i x_j)$ 的齐次电路至少包含 n^2 个非标量乘积门。

证明。 这是引理 6 与 $\ell = 2$ 的一个应用。族 $\mathcal{F}_2(f)$ 由所有单项式$x_i x_j$组成。因此，$\mu_2(f) = n^2$。如果 $\mathcal{C}$计算f，则有 $\mu_2(\widehat{\mathcal{C}}) \geq \mu_2(f)$，因此 $\mathcal{C}$至少包含n^2个乘积门。

□

另一个值得关注的情形是二元单项式，x_0,x_1，，其次数为 d。设 $f = \prod_{i=1}^{d} x_{\sigma_i}$，其中 $\sigma = (\sigma_1, \ldots, \sigma_d) \in \{0,1\}^d$。那么 $\mu_\ell(f)$ 等于 σ 中长度为 ℓ 的不同子串数量。因此，我们希望找到一个 σ 尽可能包含更多子串的对象。德布鲁因序列 [dB46]为这种对象提供了一种构造方法。

德布鲁因序列 对于给定的 k，字母表 A 上的 k 阶德布鲁因序列是一个循环序列 σ，其中来自 A^k 的每个长度为 k 的字符串都恰好作为子串出现一次。注意，σ 的长度必须为 $|A|^k$。此外，恰有 $k-1$ 个子串与序列的首尾重叠；将其视为普通序列时，σ 包含 $|A|^k - (k-1)$ 个子串。德布鲁因序列受到广泛研究，尤其是这类序列确实存在。并且，已有高效算法可用于构造德布鲁因序列（例如参见 [SWW16] 及其参考文献）。对于二元字母表 $A = \{0,1\}$，情况尤其如此。我们可以从一个由 k 个零组成的字符串开始。每一步都将序列延长 1，除非这样会导致一个长度为 k 的字符串再次出现；否则就延长 0。

给定 $d \geq 2$，令 σ 为一个二元 k 阶德布鲁因序列，其中 $\lceil \log_2 d \rceil$。它的长度为 $2^{\lceil \log_2 d \rceil} \geq d$。定义多项式

$$B_d(x_0, x_1) := \prod_{i=1}^{d} x_{\sigma_i}.$$

以下内容推出了定理 1的结论。

命题 9. *Eve* 齐次电路计算 B_d 时包含 $\Omega(d/\log d)$ 个非标量乘积门 .

证明。由引理 6 可得此结论，其中 $\ell = \lceil \log_2 d \rceil$。 [d] 包含 d 个长度为 ℓ 的区间，它们都能产生 σ 的不同子串。族 $\mathcal{F}_\ell(B_d)$ 由 d 个不同的 $-(\ell-1)$ 单项式组成，因此 $\mu_\ell(B_d) = d - (\ell-1)$。根据引理，假设 $\ell > 1$，则计算 B_d 的齐次电路必须包含 $(d-(\ell-1))/(\ell-1) = \Omega(d/\log d)$ 个乘积门。 □

备注 10. 利用字母表大小为 n 的德布鲁因序列，可以构造一个显式单项式，它含有 n 个 >1变量且次数为 $d \geq n$，其所需齐次电路的非标量规模为 $\Omega(d \log n/\log d)$。也可以将次数为 k 的二元单项式视作一个变量，从而由命题 *9* 推得此结论。

反过来，每个这样的单项式 α 都可以通过规模为 $O(d \log n/\log d)$ 的电路计算得出，且只使用乘法门（这样的计算自动是齐次的）。事实上，我们可以先用规模为 $O(n^{k+1})$ 的电路计算出所有次数不超过 k 的单项式，然后用 α 再通过 $\lceil d/k \rceil$ 个额外的乘法门计算得出。取 k 约为$0.5\log_2 d \log_2^{-1} n$ 即可。这也意味着定理 *2* 中的界是紧的。♢

4.2 同时计算偏导数

为了得到更强的下界，我们将把 Baur 和 Strassen 的经典定理 [BS83] 从计算偏导数推广到非交换情形。

我们定义关于第一个位置的偏导数如下。给定多项式f和变量x，f可以唯一地写成$f = xf_0 + f_1$，其中f_1中的任何单项式在第一个位置都不包含x。我们令$\partial_x f := f_0$。

下面引理的证明与 Baur 和 Strassen 的证明几乎相同。由于我们希望通过齐次电路计算导数，因此增加了一个额外的变化。这要求将齐次性的概念推广到允许任意变量权重的情形。我们强调，在非交换情形中，关于第一个位置求导是至关重要的。

引理 11. 假设$f \in \mathbb{F}\langle x_1,\ldots,x_n\rangle$可以由规模为$s$、非标量规模为$s_\times$的齐次电路计算。那么$\partial_{x_1} f,\ldots,\partial_{x_n} f$可以由规模为$O(s)$、非标量规模为$O(s_\times)$的齐次电路同时计算。

证明。给定$\mathbf{w} = (w_1,\ldots,w_n) \in \mathbb{N}^n$，令$w_i$为权重$x_i$的权重，并将单项式$\alpha = \prod_{j=1}^d x^{i_j}$的权重定义为$\mathrm{wt}(\alpha) = \sum_{j=1}^d w^{i_j}$。若多项式$f \in \mathbb{F}\langle x_1,\ldots,x_n\rangle$中的每个单项式都具有相同的权重，则称其为$\mathbf{w}$-齐次多项式。我们称此权重为$f$的权重，记作$\mathrm{wt}(f)$。此外，若电路$\mathcal{C}$中的每个门计算的都是$\mathbf{w}$-齐次多项式，则称该电路为$\mathbf{w}$-齐次电路。在$\mathbf{w}$-齐次电路中，任意节点$v$的权重定义为该节点所计算多项式的权重。

注意，若$(w_1,\ldots,w_n) = (1,\ldots,1)$，那么$\mathbf{w}$-齐次性与通常的齐次性概念一致。因此，引理 11 可由下面的断言推出。

断言 12. 对于任意$\mathbf{w} = (w_1,\ldots,w_n) \in \mathbb{N}^n$，如果存在一个计算$f \in \mathbb{F}\langle x_1,\ldots,x_n\rangle$的$\mathbf{w}$-齐次电路，其规模为$s$，非标量规模为$s_\times$，那么就存在一个计算$\mathbb{D}(f) = \{\partial_{x_1} f,\ldots,\partial_{x_n} f\}$的$\mathbf{w}$-齐次电路，其规模至多为$5s$，非标量规模至多为$2s_\times$。

我们通过对s进行归纳法来证明这一断言。回顾一下，电路规模由非输入门的数量衡量。基础情形为$s = 0$时，电路仅由叶节点构成。因此，导数要么为 0，要么为 1，并且仍可用规模为零的电路计算。

假设$s > 0$。任意固定$\mathbf{w} = (w_1,\ldots,w_n) \in \mathbb{N}^n$。此外，假设存在一个$\mathbf{w}$-齐次电路$\mathcal{C}$，计算$f \in \mathbb{F}\langle x_1,\ldots,x_n\rangle$，其规模为$s$。选取一个顶点$v$，使其两个子节点都是叶节点，并令$\hat{}v$表示它所计算的多项式。$\hat{}v$是一个至多含两个变量、次数至多为二的齐次多项式；不失一般性，我们还可以假设$\hat{}v$的次数至少为一次（否则可以用一个叶节点替换v）。

令$\mathcal{C}'$为从$\mathcal{C}$中移除指向v的入边，并将顶点v标记为一个新变量（例如x_0）后得到的电路。令其权重为$w_0 := \mathrm{wt}(\hat{}v)$。

令f'为由 $\mathcal{C}'$计算得到的多项式。那么， $\mathbb{D}(f)=\{\partial_{x_1}f$、……、 $\partial_{x_n}f\}$ 可以利用以下版本的链式法则，从 $\mathbb{D}(f')=\{\partial_{x_0}f'$、 $\partial_{x_1}f'$、……、 $\partial_{x_n}f'\}$ 中恢复：

$$\partial_{x_k}f=(\partial_{x_k}f'+\partial_{x_k}\widehat{v}\cdot\partial_{x_0}f')|_{x_0:=\widehat{v}}\,.$$

注意， $\partial_{x_k}\widehat{}v$ 是一个变量或常数，并且除至多两个x_k外，它对其他所有项都为零。

令 $w'=(w'_0,w_1,\ldots,w_n)$。注意， $\mathcal{C}'$ 中每个顶点的权重都与 $\mathcal{C}$中对应顶点的权重相同。因此，由于 $\mathcal{C}$ 是 w-齐次的， $\mathcal{C}'$ 是 w′-齐次的。此外， $\mathcal{C}'$ 有 $s-1$ 个非输入门，并且根据归纳假设，存在一个规模为 $5(s-1)$ 的 w′-齐次电路 $\mathcal{D}'$，它计算 $\mathbb{D}(f')$。利用上文的 $\mathcal{D}'$和链式法则，我们可以构造一个额外增加 5 个门、用于计算 $\mathbb{D}(f)$ 的电路。这个电路的规模至多为 $5(s-1)+5=5s$，并且很容易看出它是 w-齐次的。

计算非标量复杂度时，请注意，在该构造中，只有非标量乘积门会引入非标量门，而且我们引入的此类门始终至多为两个。 □

现在我们可以证明定理 2。

定理 *2*的证明。设n、d 满足[2] $n>1$， $d>2$。设k 为满足$n^k\geq n(d-1)$的最小整数。取一个字母表为 $[n]$、阶为k 的德布鲁因序列 σ。取序列 σ^1、……、 $\sigma^n\in[n]^{d-1}$，使得它们的拼接 $\sigma^1\ldots\sigma^n$ 是 σ 的初始片段。定义多项式

$$f=x_1\alpha_1+\cdots+x_n\alpha_n\,,\text{ where }\alpha_i=\prod_{j=1}^{d-1}x_{\sigma^i_j}\,.$$

假设 f 有一个非标量规模为 s 的齐次电路。那么，根据引理 11， α_1、……、 α_n可以由一个规模为 $s'=O(s)$ 的齐次电路同时计算。现在我们将引理 6 应用于 $\ell=k$。根据构造， $\mu_k(\alpha_1$、……、 $\alpha_n)=n(d-1-(k-1))=n(d-k)$。这是因为对于不同的 i 和长度为 k 的区间， $\alpha^J i$ 都是不同的单项式。于是该引理给出 $s'\geq n(d-k)/(k-1)$。若 $d\leq n$，则 $k=2$，因此 $s'\geq n(d-2)$。若 $d>n$，则 $k\leq c_1\log_2 d/\log_2 n$，且 $d-k\geq c_2 d$，其中 $c_1,c_2>0$ 为某些常数。因此确有 $s'\geq\Omega(nd^{\log}n\log d)$。—— □

4.3 有序对称多项式的下界

我们现在证明定理 3。首先注意：

注 13。OS_n^2 需要 $\Omega(n)$ 个非标量乘积门（即使在交换情形下也是如此）。这可以通过标准的偏导数论证来证明，如 *[NW97]*所示。◊

因此，我们可以聚焦于次数 $d>2$ 的情形，此时我们给出以下加强版的定理 3：

[2]如果 $d=2$，则 OS_n^2 满足该定理；参见注 13。

定理 14。 若 $1 < k < n$，则任何计算 $\mathrm{OS}_n^{k+1}(x_1, \ldots, x_n)$ 的齐次电路都需要非标量规模 $\Omega(k(n-k))$。

证明。 假设一个齐次电路计算 $f = \mathrm{OS}_n^{k+1}(x_1, \ldots, x_n)$，使用 s 个非标量乘积门。那么根据 引理 11，存在一个非标量规模为$O(s)$ 的齐次电路，可同时计算 $\{\partial_{x_1} f, \ldots, \partial_{x_n} f\}$。令该电路为 $\mathcal{C}$。那么，根据引理 6， $\mu_2(\widehat{\mathcal{C}}) \leq O(s)$。注意，

$$\partial_{x_i} f = \mathrm{OS}_{n-i}^{k}(x_{i+1}, \ldots, x_n).$$

设 $\mathrm{f}_{i,j} := (\partial_{x_i} \mathrm{f})^{[j,j+1]}$。我们声称，F 中的多项式：$= \{\mathrm{f}_{i,j} : \mathrm{i} \in [\mathrm{n} - \mathrm{k}], \mathrm{j} \in [\mathrm{k} - 1]\}$ 线性无关。这意味着 $\mu_2(\widehat{\mathcal{C}}) \geq (\mathrm{n} - \mathrm{k})(\mathrm{k} - 1)$，并给出所需的下界$\Omega(\mathrm{k}(\mathrm{n} - \mathrm{k}))$。

现在我们证明F 确实线性无关。考虑S 上的字典序：$= [n-k] \times [k-1]$，定义如下：

$$(i_0, j_0) < (i, j) \text{ iff } (j_0 > j) \text{ or } (j_0 = j \text{ and } i_0 < i).$$

给定$(i_0, j_0) \in S$。记 $\delta_{i_0,j_0}(g)$ 为单项式$x_{i_0+j_0} x_{n+j_0-k+1}$在$g$中的系数。那么对于每个$(i,j) \in S$，

$$\delta_{i_0,j_0}(f_{i,j}) = \begin{cases} 1 & \text{if } (i_0, j_0) = (i, j) \\ 0 & \text{if } (i_0, j_0) < (i, j). \end{cases} \tag{15}$$

为证明 (15)，假设 $\partial_{x_i}\mathrm{f}$ 在某个系数非零的单项式中第 $\mathrm{j}+1$ 个位置包含 $\mathrm{x}_{n+j_0-\mathrm{k}+1}$。 α 的次数为 k，而位置 $\mathrm{j}+1, \ldots, \mathrm{k}$ 必须按升序填入来自 $\mathrm{x}_{n+j_0-\mathrm{k}+1}, \ldots, \mathrm{x}_n$ 的变量。这样的 位置有 $\mathrm{k} - \mathrm{j}$ 个，而这样的变量有 $\mathrm{k} - \mathrm{j}_0$ 个。因此 $\mathrm{j} \geq \mathrm{j}_0$。此外，如果 $\mathrm{j} = \mathrm{j}_0$，，那么 α 中最后 $\mathrm{k} - \mathrm{j}_0$ 个位置唯一确定为依次排列的变量 $\mathrm{x}_{n+j_0-\mathrm{k}+1}, \ldots, \mathrm{x}_n$。类似地，如果 $\partial_{x_i}\mathrm{f}$ 在某个 α的第 j_0 个位置包含 $\mathrm{x}_{i_0+\mathrm{j}_0}$，那么前 j_0 个位置必须填入来自 $\mathrm{x}_{i+1}, \ldots, \mathrm{x}_{i_0+\mathrm{j}_0}$的变量。因此 $\mathrm{i} \leq \mathrm{i}_0$，，且在相等时，前 j_0 个位置唯一确定。这意味着当 $(\mathrm{i}_0, \mathrm{j}_0) < (\mathrm{i}, \mathrm{j})$ 时，$\delta_{i_0,\mathrm{j}_0}(\mathrm{f}_{i,j}) = 0$。此外，$\alpha := \prod_{=}^{i_0+} \mathrm{j}_0 \mathrm{p}\, \mathrm{i}_{0+1}\, \mathrm{x}_p \prod_{p=n+j_0-\mathrm{k}+1}^{n} \mathrm{x}_p$ 是 $\mathrm{f}_{i_0,\mathrm{j}_0}$ 中唯一满足 $\delta_{i_0,\mathrm{j}_0}(\alpha) = 1$的单项式，至此证明了 (15)。

最后，为了导出矛盾，假设存在一个非平凡线性组合

$$\sum_{(i,j)\in S} \gamma_{i,j} f_{i,j} = 0.$$

令(i_0,j_0) 为满足 $\gamma_{i_0,j_0} \neq 0$ 的字典序中的第一对。那么我们有

$$0 = \sum_{(i,j)\in S} \gamma_{i,j}\delta_{i_0,j_0}(f_{i,j}) = \gamma_{i_0,j_0}\delta_{i_0,j_0}(f_{i_0,j_0}) + \sum_{(i,j)>(i_0,j_0)} \gamma_{i,j}\delta_{i_0,j_0}(f_{i,j})\,.$$

利用（15），最后一个和为零，且 $\gamma_{i_0,j_0}\delta_{i_0,j_0}(f_{i_0,j_0}) = \gamma_{i_0,j_0} = 0$，这与假设 $\gamma_{i_0,j_0} \neq 0$ 矛盾。

□

5 有序对称多项式的上界

在 命题4中，我们承诺给出初等对称多项式复杂度的上界。现在我们兑现这一承诺。

齐次情形下的二次上界 我们要证明，对于 $d \in \{0,\dots,n\}$，OS_n^d 可以由一个规模为$O(n^2)$ 的齐次电路同时计算。

注意，

$$\mathrm{OS}_n^d(x_1,\dots,x_n) = \mathrm{OS}_{n-1}^{d-1}(x_1,\dots,x_{n-1})\cdot x_n + \mathrm{OS}_{n-1}^{d}(x_1,\dots,x_{n-1}).$$

因此，一旦我们计算出 $\mathrm{OS}_{n-1}^d, d \in \{0,\dots,n-1\}$，就可以再用$O(n)$ 个额外的门计算出 $\mathrm{OS}_n^d, d \in \{0,\dots,n\}$。整体复杂度为二次。

非齐次情形下的近线性上界 我们要证明，$\mathrm{OS}_n^d, d \in \{0,\dots,n\}$ 可以由一个规模为$n\cdot\mathrm{poly}(\log n)$的非交换电路同时计算。

证明与初等对称多项式的交换类比相同，参见[BS83] 或 Burgisser 等人的专著 [BCS，第 2.1–2 章。3]。

主要观察是，多项式乘法可以高效完成。令

$$f = \sum_{i=0}^{n} y_i t^i, \qquad g = \sum_{i=0}^{n} z_i t^i,$$

其中，f、g ∈ ∈ $\mathbb{F}\langle y_0,\dots,y_n、z_0,\dots,z_n\rangle$ [t]。换句话说，我们假设 t 与其他情况下不交换的变量 $y_0,\dots,y_n、z_0,\dots,z_n$交换。我们将 f、g 视为以变量 t 为自变量、系数为非交换系数的单变量多项式。于是 fg = $= \sum_{i=0}^{2n} c_i t^i$，其中 $c_i = \sum_{j=0}^{i} y_j z^{i-j}$。在交换情形下，多项式 $c_0,\dots,c_{2n}$ 可由一个小型电路同时计算。事实上，如果$\mathbb{F}$ 包含足够多的单位根，就可以利用快速傅里叶变换得到规模为 O(n log n) 的电路；在其他域中，稍作修改后可得到规模为 O(n log n log log n) 的电路，见 [SS71、BCS]。如果只计算非标量乘积门的数量，当 $\mathbb{F}$ 足够大时，还可将其改进为 O(n)。我们发现，即使 f、g 的系数不交换，结论仍然成立。这是因为

多项式 c_k 关于$y_0, \ldots$、y_n、$z_0, \ldots$、z_n是双线性的。在这种情况下，交换性不会造成区别（留作练习）。

现在考虑多项式 $h_n(t) = \prod_{i=1}^{n}(x_i + t) \in \mathbb{F}\langle x_1, \ldots, x_n\rangle[t]$。于是可以看出，$OS_n^d(x_1, \ldots, x_n)$ 是 $h(t)$ 中 t^{n-d} 的系数。这些系数可以通过以下方式递归计算：首先计算 $\prod_{i=1}^{\lceil n/2\rceil}(x_i + t)$、$\prod_{i=\lceil n/2\rceil+1}^{n}(x_i + t)$，然后利用上述快速多项式乘法将二者合并。这就得到了所声称的复杂度。

6 个开放问题

最后，我们提出两个开放问题。

开放问题 1。 找出一个次数为 d 的显式二元多项式，它需要规模为*superlinearin d*的非交换齐次电路

开放问题 2。 给定一个非交换单项式 α，加法门能否帮助计算 α?

请注意，本文得到的界关于 d 几乎只是线性的。问题 1 只是要求定量改进。没有加法门的电路自动就是齐次的——因此，若问题 2 的答案是否定的，就可以在定理 1中去掉齐次性假设。

致谢

第一作者感谢Cafedu 提供了如此舒适的工作场所。第二作者感谢 Amir Yehudayoff 提供了关于这一主题的宝贵想法，这些想法是在遥远而愉快的往昔交流的。

参考文献

[BCS] Peter B¨urgisser, Michael Clausen, 和 M Amin Shokrollahi。 代数复杂性理论，与 Thomas Lickteig 合作。 数学科学基础丛书，315。[BS83] Walter Baur 和 Volker Strassen。 偏导数的复杂性。 理论计算机科学，22:317–330，1983。[CKSV22] Prerona Chatterjee、Mrinal Kumar、Adrian She 和 Ben Lee Volk。 代数分支程序和公式的二次下界。 计算复杂性，31(2):8，2022。[dB46] N.G. de Bruijn。 组合问题。 阿姆斯特丹荷兰皇家科学院科学部论文集，49(7):758–764，1946。

[HWY11] Pavel Hrubes、Avi Wigderson 和 Amir Yehudayoff。非交换电路与平方和问题。《美国数学会会刊》，24(3):871–898，2011。[Hya77] Laurent Hyafil。交换性的力量。载于《第18届计算机科学基础年度研讨会》，美国罗得岛州普罗维登斯，1977年10月31日至11月1日，第171–174页。IEEE计算机学会，1977。[Kal85] K. Kalorkoti。有理函数公式规模的下界。《SIAM计算杂志》，14(3):678–687，1985。[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计算理论年度研讨会论文集》，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。[NW97] Noam Nisan 和 Avi Wigderson。基于偏导数的算术电路下界。《计算复杂性》，6(3):217–234，1997。[SS71] Arnold Sch¨onhage 和 Volker Strassen。大数的快速乘法。《计算》，7(3-4):281–292，1971。[Str73] Volker Strassen。初等对称函数及插值系数的计算复杂性。《数值数学》，20(3):238–251，1973。[SWW16] Joe Sawada、Aaron Williams 和 Dennis Wong。推广德布鲁因序列和通用循环的经典贪心构造与项链构造。《电子组合学杂志》，23(1):1，2016。[TLS22] S´ebastien Tavenas、Nutan Limaye 和 Srikanth Srinivasan。迭代矩阵乘法的集合多线性公式下界与非交换公式下界。载于Stefano Leonardi和Anupam Gupta编，《STOC ’22：第54届ACM SIGACT计算理论年度研讨会》，意大利罗马，2022年6月20日至24日，第416–425页。ACM，2022。[Val80] Leslie G. Valiant。否定的力量可以呈指数级。《理论计算机科学》，12:303–314，1980。