arXiv:2302.06984v1 [cs.CC] 14 Feb 2023

迈向代数公式深度约简的最优方案

Herv´e Fournier[1],Nutan Limaye[2], Guillaume Malod[3], Srikanth Srinivasan*[4]，以及 S´ebastien Tavenas[5]

[1,3]巴黎西岱大学，IMJ-PRG 电子邮箱：herve.fournier@imj-prg.fr, guillaume.malod@imj-prg.fr[2]哥本哈根信息技术大学，电子邮箱：nuli@itu.dk[5]奥胡斯大学，电子邮箱：srinivasan.srikanth@gmail.com[3]萨瓦-勃朗峰大学，法国国家科学研究中心，LAMA 电子邮箱：sebastien.tavenas@univ-smb.fr

摘要

Brent、Kuck 和 Maruyama（IEEE《计算机汇刊》，1973 年）以及 Brent（《ACM计算机学报》，1974 年）的经典结果表明，任何规模为 s 的代数公式都可以转换为深度为 $O(\log s)$ 的公式，且规模只会发生多项式级膨胀。本文研究这一结果的精细化版本，该版本取决于代数公式所计算的多项式的次数。

给定一个规模为 s 、计算次数为 d的多项式 P 的齐次代数公式，我们证明 P 也可以由一个深度为 $O(\log d)$ 、规模为 poly(s). 的（无界扇入）代数公式计算。我们的证明表明，这一结果在单调、非交换代数公式这一高度受限的情形下同样成立。

当 d 较小时（即 $d = s^{o(1)}$），这一结果改进了先前的成果。特别是，对于 $d = O(\log s)$的情形，结合 Raz 的结果（STOC 2010，ACM计算机学报 2013），我们的结果表明，即使对于非齐次公式，也能实现相同的深度约简。考虑到近期的代数公式下界研究恰恰针对这种“低次数”和“低深度”情形，这一点尤其值得关注。

我们还证明，在单调情形下，即使对于交换公式，这些结果也无法改进。

*作者感谢在2022年夏季于巴黎西岱大学进行的、由客座研究人员计划资助的学术访问。

1 引言

本文研究了一个关于代数公式模型中两种资源之间计算权衡的基本问题。

多变量多项式 $P(x_1, ..., x_n)$ 的代数公式 F，简单来说，就是由嵌套的加法和乘法构成的代数表达式 P。等价地，它可以定义为一棵有根有向树，其中叶节点标记为变量，内部节点（或门）对子节点计算线性组合或乘积（下面第 2 节将给出形式化定义）。除非另有说明，否则我们不限制一个门的子节点数量（换言之，我们考虑无界扇入的公式）。

描述代数公式 F 复杂性的两种基本计算资源是规模和深度：规模是底层树中叶节点的数量，深度则自然是树的深度。具有高效（即规模为 poly(n)）代数公式的多项式 [1] 构成代数复杂性类 VF。与其布尔对应类 NC[1], 一样，这是一个自然且重要的复杂性类。

自 20 世纪 70 年代初以来，许多早期研究都聚焦于公式及相关计算模型中规模与深度之间的权衡 [Spi71, BKM73, Bre74, VSBR83, SS80, Nis91, Raz06, RY08, AV08, Koi12, Tav15, GKKS16, KSS14, CKSV16, LST21a]。下面介绍其中一些结果。

- 在布尔情形下，Spira [Spi71] 以及独立地，Khrapchenko（见 [YK68]）证明，任何规模为 s 的布尔公式都可以转换为深度为 $O(\log s)$的布尔公式，同时将规模限制在 $s^{O(1)}$. 以内。Brent、Kuck 和 Marayuma [BKM73] 以及 Brent [Bre74]的研究也在代数情形下得到了相应结果。后续许多研究改进了深度和规模界中的常数 [PM75, PM76, Kos86, BCE95, BB94]。

- 对于更一般的代数电路模型，人们也研究了这一问题；在该模型中，底层树被有向无环图（DAG）取代。Valiant、Skyum、Berkowitz 和 Rackoff 的一个著名结果 [VSBR83] 表明，规模为 s 、计算次数为 poly(s) 的多项式的代数电路，可以转换为深度为[2]$O(\log s)$、规模为 poly(s) 的电路。Raz 和 Yehudayoff [RY08] 也证明，这些结果对多线性[3] 电路同样成立。

- 众所周知，上述结果在各种情形下都是紧的。在单调情形[4]中，Shamir 和 Snir [SS80] 证明，存在一个显式多项式 P，其电路规模为 poly(n)，但任何深度为 $o(\log n)$ 、计算 P 的电路都具有超多项式规模。Raz [Raz06] 以及 Chillara 、 Limaye 和 Srinivasan [CLS 18]也在多线性情形下得到了类似结果（分别针对多线性电路和公式）。

- 从 Agrawal 和 Vinay 的工作 [AV08], 开始，近期一系列研究 [Koi12, Tav15, GKKS16, KSS14, CKSV16, KdOS19] 表明，代数电路和公式可以转换为常数深度公式，同时规模仅发生亚指数级膨胀。相比之下，本文主要关注在规模保持为多项式级（poly(s)）的前提下，尽可能降低深度，这与前文列出的结果一致。

[1]严格来说，这里应当指无限多项式序列，但我们忽略这一差别。[2]在有界扇入的情况下，深度则应为 $O(\log^2 s)$ 。[3]如果一个电路或公式中的每个门都计算一个多线性多项式，则称该电路或公式是多线性的。[4]其中底层域为 $\mathbb{R}$ ，且所有常数均为非负数，因此不会发生抵消。

问题。本文探讨：已知代数公式所计算的多项式 $P(x_1,\ldots,x_n)$ 的次数上界 d 时，能否证明更强的深度约简结果。一般而言，规模为 s 的代数公式可以计算次数至多为 s 的多项式。当 $d=s$ （或 $d=s^{\Omega(1)}$）时，上述结果意味着，代数公式 F 可以在规模没有显著膨胀的情况下，转换为深度为 $O(\log\ d)$ 的另一个公式 F'，用于计算 P。对于任意 d （或者更具体地说，当 $d=s^{o(1)}$ 时），这样的结果是否成立?

注意，这个问题只有对无界扇入的代数公式才有意义。如果每个门的扇入都由一个常数界定，那么任何规模为 s 的公式，其深度都至少为 $\Omega(\log s)$ （因此，Brent、Kuck 和 Marayuma 的结果 [BKM73] 是最优的）。然而，在许多情形下（例如，参见下文第三个动机），我们希望对无界扇入公式所能达到的公式深度进行更精细的分析。

动机。虽然在我们看来，这个问题相当自然，但还有许多具体原因促使我们探究这一方向。

- 从 Valiant、Skyum、Berkowitz 和 Rackoff [VSBR83] 的证明很容易看出，任何代数电路都可以在规模仅发生多项式(s,d) 膨胀的情况下，将深度约简至 $O(\log\ d)$。因此，对于小次数情形的自然推广在代数电路这一设定下确实成立。

- 从先前的结果还可以推出，当次数为 $d=o(\log s)$. 时， $O(\log s)$ 的深度上界可以改进。这得益于 Raz 的一个结果 [Raz13]: 任意一个计算 P 次数为 d 的齐次多项式 F 的公式，都可以高效地转换为齐次公式[5]F' 。此外，很容易看出，任何计算次数为 d 的多项式的齐次公式，其深度均为 $O(d)=o(\log s)$. 。因此，在这一次数范围内，标准的深度约简结果可以得到加强。

- 最后，代数复杂性方面非常近期的结果 [LST21b] 提出了一种针对计算低次数多项式的低深度代数公式证明下界的方法，这自然引出了一个问题：在这一情形下，如何获得尽可能好的深度约简结果。

  更具体地说，Limaye、Srinivasan 和 Tavenas [LST21b] 展示了如何针对小深度的代数公式（甚至电路）证明下界。他们的证明通过将一个规模为 s 且深度为 Δ 的代数公式转换为一个规模为 poly(s) 且深度为 $O(\Delta)$ 的齐次代数公式，然后针对深度为 $O(\Delta)$ 的齐次代数公式证明下界。第一步的一个重要特点是，它只在 $d=O(\log\ s/\log\log\ s)$. 这一“低次数情形”下成立。第二步则针对深度至多为 $O(\log\log d)$. 的齐次公式证明下界。

  为了让这一证明思路适用于一般的（深度无界）代数公式，我们希望能够尽可能地对代数公式进行齐次化和深度约简。Raz 的上述结果 [Raz13] 已表明，在低次数情形下，我们可以高效地对代数公式进行齐次化。因此，自然要探究低次数情形下齐次代数公式所能达到的最佳深度约简。

结果。我们的主要结果是关于齐次公式的深度约简结果，可将深度高效地约简至 $O(\log d)$，与 [VSBR83] 的结果已知的代数电路情形相匹配。

[5]齐次公式是指每个门都计算一个齐次多项式的公式。这意味着该公式不会计算次数大于 d 的中间多项式。

定理 1（主要结果）。设 F 是一个规模为 s 、计算次数为 $d \geqslant 2$ 的多项式 P 的齐次代数公式。那么， P 也可由一个规模为 $\mathrm{poly}(s)$ 、深度为 $O(\log d)$. 的齐次公式 F' 计算。此外，如果 F 是单调的和/或非交换的，那么F'也具有相同性质。

这里，单调代数公式是指不以任何方式利用抵消的公式；非交换公式则描述定义在这样一个域中的多项式表达式，其中输入变量相乘时彼此不交换（形式化定义见第 2 节）。在这两种情形下，要证明公式的上界都更为困难，因此，这些情形下的深度约简结果蕴含标准情形下的结果。还可以验证，上述深度约简过程会保留公式的其他有趣性质，例如多线性和集合多线性。

利用 Raz 的上述结果（该结果允许我们在低次数情形下将代数公式齐次化），我们甚至可以对非齐次公式得到如下深度约简结果。

推论 2。令 $d = O(\log n)$。那么，在 n 个变量上定义、次数为 $d \geqslant 2$ 的齐次多项式 P 有规模为 $\mathrm{poly}(n)$ 的代数公式，当且仅当它有深度为 $O(\log d)$ 、规模为 $\mathrm{poly}(n)$. 的代数公式

特别地，这意味着，要在低次数情形下证明针对一般代数公式的超多项式下界，只需针对深度为 $O(\log d)$. 的齐次代数公式证明这类下界。据我们所知，在此类蕴含关系中，此前对于这样的结果，除了平凡的 $O(d)$ 下界之外，尚无任何已知结果。这使我们更加接近于那些已有下界的深度范围 [LST21b]。

在非交换情形下，这些结论更加引人注目：证明代数分支程序（ABPs）与公式之间的分离是一个长期存在的问题。在近期工作 [TLS22], 中，研究者展示了如何对深度为 $o(\sqrt{\log d})$ 的情形证明这一结果。本文的结果表明，只需对深度为 $O(\log d)$.[6] 的情形证明这一结果即可。

最后，我们还表明，除非采用某种能够利用抵消的技术，否则就深度而言，我们的结果无法在渐近意义上得到改进。

定理 3（下界）。设 n 和 $d = d(n)$ 是增长参数，且满足 $d(n) \leqslant \sqrt{n}$。那么，存在一个规模至多为 n 、深度为 $O(\log d)$ 的单调代数公式 F ，它计算次数至多为 d的多项式 $P \in \mathbb{F}[x_1, \ldots, x_n]$ ；任何深度为$o(\log d)$ 且计算 P 的单调公式 F'，其规模必须为 $n^{\omega(1)}$.

值得注意的是，Gupta、Kamath、Kayal 和 Saptharishi 的一个著名结果 [GKKS16]展示了如何利用抵消来获得更好的深度约简结果。然而，一般而言，在不导致规模显著膨胀的情况下，这种方法无法将给定公式的深度降低超过一个常数因子。[7] 因此，我们认为上述结果强有力地表明，我们的深度约简结果在深度上是紧的，差距至多为一个常数因子。

2 预备知识

基本记号。除非另有说明，全文讨论域 $\mathbb{F}$ 上的多项式。我们将使用多元多项式环 $\mathbb{F}[x_1, \ldots, x_n]$，或其非交换版本 $\mathbb{F}\langle x_1, \ldots, x_n \rangle$.

[6]我们注意到，Raz 的结果虽然仅针对交换情形表述，但同样适用于非交换情形。[7]更确切地说， [GKKS16] 的结果展示了如何高效地将低次 *homogeneous* 深度 4 公式转换为 *inhomogeneous* 深度 3 公式。一般而言，这可以用来将小深度公式的深度缩减一半。

2.1 代数公式

我们先简要介绍一些与代数公式相关的定义和结果。关于这一模型的更多内容，请参阅标准文献 [SY10、Sap15]。

模型。多元多项式环 $\mathbb{F}[x_1, \ldots, x_n]$ 上的代数公式是一个有根有向树，边的方向指向根。叶节点标记为变量$x_1, \ldots, x_n$或常数 1，边标记为非零域常数。内部节点（即门）标记为 $+$ 和 $\times$，并计算其子节点的线性组合（依据边权）或乘积。不失一般性，我们假设，如果节点 α 有一个标记为 1 的叶节点作为子节点，那么 α 是一个 $+$门；如果一个 $+$门 α 的所有子节点都标记为 1，那么 α 就是该公式的输出。[8] 多元多项式环 $\mathbb{F}\langle x_1, \ldots, x_n \rangle$ 上的非交换代数公式定义类似，但还需假设任意×门的子节点都是线性有序的，并按照此顺序计算相应的乘积。

除非另有明确说明，我们考虑的代数公式均具有无界扇入（即一个门可以有任意数量的输入）。 F 的规模表示叶节点的数量，[9] 的深度表示 F 中从叶节点到根的最长路径。 F 的乘积深度和求和深度分别定义为从叶节点到根的路径上经过的乘积门和求和门的最大数量。

公式 F 的解析树是 F 的一个子公式，它对应于在 F的求值过程中构造一个单项式的方式。 F 的解析树可按如下方式归纳定义：

- 如果 F 的顶层是一个 $+$门，那么 F 的一棵解析树由其某个子节点的一棵解析树，以及连接到 F根的相应边构成；
- 如果 F 的顶层是一个 $\times$门，那么 F 的一棵解析树由其每个子节点的一棵解析树，以及 F根的入边构成；
- 叶节点的唯一解析树就是它自身。

解析树计算出的多项式是一个单项式，它等于标记其叶节点的变量的乘积，再乘以标记其边的标量的乘积。容易看出，公式 F 计算出的多项式等于其所有解析树所计算的单项式之和。

如果公式 F 的解析树所计算出的任何单项式，在 F计算出的多项式中都具有非零系数，则称公式 F 为单调公式。

现在我们回顾一些关于代数公式的文献中的著名结果。需要注意的是，这些结果（具体而言，即后文的定理4、5和10）通常是在交换公式的一般情形下证明的。然而，很容易看出，这些结果的证明可以在不作重大改动的情况下推广到单调、非交换情形。

深度约简。经典结果 [BKM73、Bre74] 表明，任何规模较小的代数公式都可以由一个深度较小且规模不会大很多的公式来模拟。形式化地，

定理 4. 设 F 是一个规模为 s 、计算多项式 P的（非交换或交换）代数公式。那么存在一个规模至多为 $\mathrm{poly}(s)$、深度为 $\Delta = O(\log s)$、计算 P的代数公式 F'。我们还可以假设 F' 中的每个门的扇入为 2。此外，如果 F 是齐次和/或单调的，那么 F'也具有相同性质。

[8]这确保公式能够计算含有常数项的多项式，同时禁止仅为了计算常数而使用大量算术运算。[9]只要每个门的扇入至少为 2（这不失一般性），这就与门的数量相差一个常数因子。

齐次性。代数公式中的每个门都有一种自然定义的语法次数。标记为常数 1 的叶节点的语法次数为 0，标记为变量的叶节点的语法次数为 1， $\times$-门的语法次数等于其子节点语法次数之和，而 $+$-门的语法次数等于其子节点语法次数中的最大值。公式的语法次数定义为其输出的语法次数。注意，在公式中，任何门的语法次数都不超过该公式的语法次数。

我们还将假设没有门计算零多项式。

如果公式中的每个门都计算齐次多项式，则称该公式为齐次公式。等价地，从语法次数来看，这意味着求和门的所有子节点具有相同的语法次数。

Raz [Raz13] 展示了如何将可能是非齐次的公式 F 转换为齐次公式，同时使规模的膨胀相对较小。

定理 5. 设 F 是一个规模为 s 、乘积深度为 Δ 的（非交换或交换）代数公式，计算多项式 P，且 F 中的所有门的扇入均为 2。那么存在一个齐次代数公式 F'，其规模至多为 $O\left(s \cdot \binom{\Delta+d+1}{d}\right)$，乘积深度为 Δ，并计算 P。特别地，若 $\Delta = O(\log\ s)$ 且 $d = O(\log\ s)$, 则公式 F'的规模为 $\mathrm{poly}(s)$.

3 主要结果

证明概述。虽然主要结果的证明相当简短，而且（在我们看来）十分简洁，但我们在此补充一些说明，以阐明为何先前的深度约简证明不适用于我们的情形。

证明定理 1 时，首先想到的做法是尝试采用定理 4 背后的证明策略。在这里，我们从一个规模为 s 的公式 F 出发，找到一个规模约为 $s/2$ 、以 α 为根的 F 的子公式 G 。不难证明，由 F 计算的多项式可以写成

$$F = G \times H_1 + H_2$$

其中， H_1 和 H_2 也分别可由规模为 $s/2$ 的公式计算。[10] 然后我们对这三个子公式应用归纳法，得到所需结果。遗憾的是，这种策略完全没有利用公式的次数，因此只能得到一个深度为 $O(\log s)$. 的公式

在齐次情形下，对底层公式的次数进行归纳有时更为自然；此时， G 和 H_1 （在上述分解中）将是次数约为 $d/2$ 的子公式。我们得到以下关于 F 的降深版本最坏情况规模的递推关系，记为 $T(s,\ d)$

$$T(s,d) \leqslant T(s_1,d/2) + T(s-s_1,d/2) + T(s-s_1,d)$$

其中 s_1 表示 G的规模。不幸的是，在这种情况下，公式 H_1 和 H_2 的规模可能接近 s，从而导致显著的规模膨胀。事实上，当 s_1 远小于 s时（例如 $s_1 = s^{o(1)}$），上述递归只能得到 $T(s$、$d) = s^{O(\log d)}$，这会造成超多项式规模膨胀。

或许可以交错进行关于规模和深度的递归，但我们没能让这种方法奏效。

[10]这里，为简单起见，我们假设 F是一个交换公式。在非交换情形下，我们则会得到 $F = H_1' G H_1'' + H_2$.

另一种可能的策略是沿用 [VSBR83] 的工作，构造出深度符合要求的电路。遗憾的是，[VSBR83] 的证明采用了记忆化过程，即使应用于公式 F，似乎也会得到电路。将得到的深度为$O(\log\ d)$ 的电路转换成公式，似乎会使规模增至 $s^{\Omega(\log d)}$。

我们采用的方法比上文概述的递归策略更为整体化。我们的第一个启发性例子，似乎是深度约简的最坏情况：一个深度大于 d 、由交替的和与积构成的梳状结构。更形式化地说，梳状结构计算以下多项式（允许变量相互识别）。

$$C(x) = x_1 + (x_2 \times (x_3 + (x_4 \times \cdots)))$$

注意，上述方法得到的公式深度大于 d ，其中 d 是底层多项式的次数。然而，我们观察到，这样的梳状结构实际上只计算含有少数几个单项式的多项式，因此无需显著增加规模，就能轻易将其写成深度为 $2\sum\prod$ 的公式。

基于这一观察，总体策略是将公式分解为顶层部分 G（它是一个（广义）梳状结构），其叶节点是 F 的子公式；我们将对这些子公式递归地应用同一过程。然后，我们将 G 写成一个 $\sum\prod$ 公式，并用子公式的降深版本替换它的叶节点。由此得到 F 的降深版本。

G的正确定义至关重要，而且有些微妙（至少对我们而言如此）；不过，只要定义恰当，证明便能顺利进行。

3.1 定理 1 的证明

本节证明我们的主要结果（定理 1）。我们先针对偏斜公式的情形，给出一个简单的深度约简结果。若一个公式中的每个乘法门至多有 1 个非平凡子节点（即非叶节点），则称该公式为偏斜公式。

我们称偏斜公式中的一个叶节点为 $+$叶节点，当且仅当该叶节点的父节点是一个 $+$ 门；否则称其为 $\times$叶节点。我们证明，任何偏斜公式都可以高效地转化为深度-2公式，即 $\sum\prod$公式。

引理 6. 设 G是一个求和深度为 δ的偏斜公式，其中所有门的扇入为 2，且叶节点均标记为互异变量。那么，由 G 计算出的多项式是一个至多含有 2^δ 个单项式的多线性多项式。此外，G中的任意变量标记

- a $+$-叶节点，
- 或者一个 $\times$-叶节点，其兄弟节点也是叶节点

恰好出现在一个单项式中。我们称它们为不可重复变量。

证明。我们对公式的深度进行归纳法证明。基础情形是深度为 0 或 1 的情况。在这两种情况下，结论显然成立。

对于归纳情形，假设深度至少为 2。设 $G = G_1 + G_2$。 G_1和 G_2的深度和至多为 $\delta - 1$。设 f_1、f_2分别是由 G_1、G_2计算得到的多线性多项式。我们知道， G 的叶节点都标记着互异变量。因此， G_1、G_2 也具有相同的性质，并且标记 G_1 和 G_2的叶节点的变量集互不相交。G_1 和 G_2 的深度都严格小于 G的深度。根据归纳假设， f_1 和 f_2 至多有 $2^{\delta-1}$ 个单项式。此外，G_1 中的任何不可重复变量在 f_1中至多出现在一个单项式中。同理，G_2 中的任何不可重复变量在 f_2中至多出现在一个单项式中。因此，由 G计算得到的多项式，即 $f_1 + f_2$，

至多有 2^δ 个单项式，并且其中每个不可重复变量至多出现在一个单项式中。

假设 G 的顶层门是一个 $\times$ 门。由于 G 是偏斜公式，它必定是 $x \times G_1$ 或 $G_1 \times x$，其中 x 是一个变量。特别地，由于 G 的深度至少为二，变量 x 可以重复。令 f_1 为 G_1 所计算的多线性多项式。根据我们的假设，变量 x 不出现在 f_1 中。G_1 的深度严格小于 G。根据归纳假设，f_1 至多有 2^δ 个单项式，并且 G_1 中任何不可重复变量至多出现在一个单项式中。由于 x 可以分配到 f_1 的各个单项式上，因此 G 所计算的多项式是多线性多项式，至多有 2^δ 个单项式，并且任何不可重复变量至多出现在一个单项式中。

（注意，也可以利用解析树看出这一点，因为所计算的多项式是各解析树所计算的单项式之和。其多线性显而易见。注意，由于偏斜性，解析树在乘法门处并不会真正“分支”，因此它们是梳状结构。从根开始构建解析树时，对于路径上遇到的每个加法门，我们都有两种选择，而这样的门至多有 δ 个，因此至多得到 2^δ 棵解析树。包含某个给定不可重复变量的唯一解析树，由从根到该叶节点的路径确定。）

□

如果一个公式是齐次的，那么对于任意门 α，由 α 计算的多项式的次数都与 α 的语法次数 d_α 一致。基于这一观察，下面我们证明一个比定理 1 更强的结论。具体来说，定理 1 针对的是齐次公式。而在这里，我们证明了对语法次数较小的公式进行深度约简的方法。

定理 7（定理 1 的改进）。设 F 是一个规模为 s、语法次数为 $d_F \geqslant 2$ 的代数公式。那么 P 也可由一个规模为 $\mathrm{poly}(s)$、深度为 $O(\log d_F)$ 的公式 F' 计算。此外，如果 F 是齐次、单调和/或非交换的，那么 F' 也具有相同性质。

证明。我们先从对 F 应用定理 4 后得到的公式开始。也就是说，我们假设有一个规模为 $\mathrm{poly}(s)$ 的公式，其中每个门的扇入为 2，求和深度和乘积深度均不超过 $O(\log s)$。为简化符号，从现在起，F 指代这个新公式。

令 δ 为正整数。对于语法次数为 $d_G \geqslant 1$、求和深度为 $\Delta(G)$ 的公式 G，我们定义势函数 $\phi_\delta(G)$ 如下。

$$\begin{cases} \phi_{\delta,1}(G) = \lceil \log(d_G) \rceil \\ \phi_{\delta,2}(G) = \lceil \Delta(G)/\delta \rceil \end{cases}$$

并令

$$\phi_\delta(G) = \phi_{\delta,1}(G) + \phi_{\delta,2}(G).$$

我们将证明，势函数能够界定我们将构造的深度约简公式的深度。我们还将用它来界定所得公式的规模。具体而言，我们证明以下引理。

引理 8。设 δ 为正整数。任何具有扇入为 2、语法次数为 $d \geqslant 1$、求和深度为 Δ和规模为 s 的公式 F，都可以并行化为一个公式 F'（扇入任意），其乘积深度至多为 $\phi_\delta(F)$，规模至多为 $s \cdot 2^{\delta \log(d)}$。此外，如果 F是齐次、单调和/或非交换的，那么 F'也具有相应性质。

由于我们确保求和深度被 $O(\log\ s)$所界定，取 $\delta = \left\lceil \frac{s}{\log d} \right\rceil_{\log}$并应用引理 8，我们得到最终公式 F' 的规模至多为 $\mathrm{poly}(s)$ ，且乘积深度至多为

$$\phi_\delta(F) = O\left(\lceil \log d \rceil + \left\lceil \log(s) \frac{\log d}{\log s} \right\rceil\right) = O(\log d).$$

通过合并输入其他求和门的求和门，我们可以假设 F' 的深度至多为其乘积深度的两倍，即为 $O(\log d)$。由此，定理的证明得以完成。

□

现在我们证明引理 8。

引理 8 的证明。对于 F 中的任意门 α ，令 F_α 表示以 α 为根的子公式，并令 d_α 表示其语法次数。我们对 $\phi_\delta(F)$ 进行归纳证明。

基础情形 $\phi_\delta(F) = 0$ 显然成立。考虑 F 的以下门集合：

$$\mathcal{A} = \left\{\alpha \mid \alpha \text{ is a not a leaf labelled 1 and } \phi_\delta(F_\alpha) < \phi_\delta(F) = \phi_\delta(F_{\mathrm{parent}(\alpha)})\right\}.$$

对于 $\mathcal{A}$ 中的任意门 α ，归纳假设告诉我们，可以构造一个乘积深度至多为 $\phi_\delta(F)-1$、规模至多为 $s_\alpha \cdot 2^{\delta \log(d_\alpha)}$ 的公式 F'_α ，计算出与 F_α. 相同的多项式

考虑将 F 中 $\mathcal{A}$ 的这些门替换为叶节点（标记为互异变量）后得到的公式 G 。注意，对于 F 中的乘积门 β，其子节点中至多有一个的语法次数大于 $d_\beta/2,$ ，其中 d_β 是 β 的语法次数。因此， G 是一个偏斜公式。 β 的另一个子节点是 G 中的一个 $\times$-叶节点。此外， G 的求和深度至多为 δ （因为对于下方的门，$\phi_{\delta,2}$ 严格递减）。

因此，我们可以用引理 6 来简化 G：得到由 G计算的多项式是关于其叶节点的多线性多项式，且有 2^δ 个单项式。接着，我们可以将 G 写成一个$\sum\prod$-公式 G' ，使得每个可复制门出现在至多 2^δ 个单项式中，而每个不可复制门至多出现在 1 个单项式中。

关于 F 的新公式 F' 由 G' 得到：将每个变量叶子（它对应于 F中的某个门 α ）替换为使用上述归纳假设构造的降深版本F'_α 。

F' 的乘积深度不超过门 $\alpha \in \mathcal{A}$ 的乘积深度加上 G的乘积深度；将其重写为 $\sum\prod$-公式后，后者等于 1。也就是说，乘积深度至多为 $(\phi_\delta(F)-1)+1 = \phi_\delta(F)$。根据构造，如果 G 不包含标记为 1 的叶节点，那么 G'也不包含此类叶节点；否则， G' 仍至多有一个这样的叶节点。所得公式的规模不超过

$$\sum_{\alpha \text{ non-duplicable}} \left(s_\alpha \cdot 2^{\delta \log(d_\alpha)}\right) + \left(2^\delta \cdot \sum_{\alpha \text{ duplicable}} \left(s_\alpha \cdot 2^{\delta \log(d_\alpha)}\right)\right) + \mathbb{I}^{\text{G' has a constant leaf}}.$$

注意，如果 α 是可复制门，那么它必定是一个 $\times$-叶节点，且其兄弟节点 β 不是叶节点。这意味着 $d_\alpha \leqslant d_\beta \leqslant d$ ，因为语法次数在根处达到最大值。因此 $d_\alpha \leqslant d/2$ ，所以可复制门的贡献有如下界：

$$\sum_{\alpha \text{ duplicable}} 2^\delta \left(s_\alpha \cdot 2^{\delta(\log(d)-1)}\right) \leqslant \sum_{\alpha \text{ duplicable}} \left(s_\alpha \cdot 2^{\delta \log(d)}\right).$$

不可复制门的贡献上界为

$$\sum_{\alpha \text{ non-duplicable}} s_\alpha \cdot 2^{\delta \log d}$$

因为 F 中的任意门的语法次数至多为 d。根据 $\mathcal{A}$ 的选取，子公式 F_α 彼此不相交，因此 $\sum_{\alpha\in\mathcal{A}} s_\alpha \leqslant s$；若 G' 含有常数叶节点，则不等式严格成立。因此， F' 的规模上界为 $s\cdot 2^{\delta\,\text{对数}(d)}$。

最后，很容易验证该构造保留了齐次性、单调性和／或非交换性。

□

备注 9. 很容易看出，我们的深度约简过程不会增加公式的语法次数。

我们还注意到，将定理 1 与定理 4 和定理 5 结合起来，立即可得推论 2。

推论 2 的证明。给定一个规模为 $s=$poly(n)、计算次数为 $d=O(\log n)$ 的多项式的（可能非齐次）公式 F，我们首先应用标准深度约简（定理 4），得到一个等价公式 F_1，其规模为 $s_1=$ poly (n)、深度为 $\Delta_1=O(\log n)$，且每个门的扇入为 2。对 F_1 应用 Raz 的齐次化定理（定理 5），得到一个等价的齐次公式 F_2，其规模为 $s_2=$ poly(n)、深度为 $\Delta_2=O(\log n)$。现在我们可以对 F_2 应用定理 1，得到一个等价公式 F'，其规模为 $s'=$poly(n)、深度为 $\Delta'=O(\log\ d)$.

□

3.2 缩小规模膨胀

我们注意到，上述策略很容易调整，从而得到一个规模为 s' 的小深度公式，其规模几乎与原公式的规模 s 呈线性关系，代价是深度增加一个较大的常数。

证明与上文定理 1 的证明几乎完全相同。新的要点是在不对上述公式的次数作任何假设的情况下，实现近线性深度约简。更准确地说，Bshouty、Cleve 和 Eberly [BCE95]（另见 Bonet 和 Buss [BB94] 的工作）证明了以下结论（为完整起见，我们在附录 A 中概述 Bonet 和 Buss 的证明）。

定理 10（近线性规模的深度约简）。对于任意 $\varepsilon>0$. Let$F$，若其为一个规模为 s、计算多项式 P 的（非交换或交换）代数公式，则存在一个代数公式 F'，其规模至多为 $s^{1+\varepsilon}$、深度为 $\Delta=2^{O(1/\varepsilon)}\cdot\log\ s$，并计算 P。我们还可以假设 F' 中的每个门的扇入均为 2。此外，若 F 是齐次和 / 或单调的，则 F' 也具有相同性质。

利用上述结果，我们可以证明以下改进版的深度约简。

定理 11. 假设 F 是一个规模为 s、语法次数为 $d\geqslant 1$ 且计算多项式 P 的（交换或非交换）公式。那么 P 也可由一个规模至多为 $s^{1+\varepsilon}$、深度为 $\Delta=2^{O(1/\varepsilon)}\cdot\log d.$ 的公式 F'' 计算。此外，如果 F 是齐次公式和/或单调公式，那么 F'' 也是如此。

证明. 若 $d^{4/\varepsilon}\geqslant s,$，那么定理 10 的深度约简已能给出令人满意的解答。事实上，规模至多为 $s^{1+\varepsilon}$，深度至多为

$$2^{O(1/\varepsilon)}\log s\leqslant\frac{4}{\varepsilon}2^{O(1/\varepsilon)}\log d\leqslant 2^{O(1/\varepsilon)}\log d.$$

因此我们假设 $s>d^{4/\varepsilon}$。首先应用定理 10（用 $\varepsilon/2$ 替代 ε），得到一个扇入为 2、计算 P 的公式 F'，其规模至多为 $s^{1+\varepsilon/2},$，深度为 $\Delta'=2^{O(1/\varepsilon)}\cdot\log\ s$。

现在，我们应用引理 8，并令 $\delta=\lfloor(\varepsilon\log\ s)/(2\log\ d)\rfloor$。注意，由于 $\varepsilon\log\ s>4\log\ d$，因此可得 $\delta>(\varepsilon\log\ s)/(4\log\ d)>1$。

然后，该策略生成一个乘积深度至多为 F'' 的公式

$$\phi_\delta(F') \leqslant \phi_{\delta,1}(F') + \phi_{\delta,2}(F') < \lceil \log d \rceil + 2^{O(1/\varepsilon)} \log s \frac{4 \log d}{\varepsilon \log s} = 2^{O(1/\varepsilon)} \log d$$

且规模至多

$$s^{1+\varepsilon/2} \cdot 2^{\delta \log d} \leqslant s^{1+\varepsilon/2} s^{\varepsilon/2}.$$

这就证明了该定理。 □

3.3 将乘积扇入降至 2

自然会想到，能否在保证每个门的扇入均不超过 2 的同时证明定理 1，就像定理 1 和定理 10 中那样。这是不可能的，因为扇入为 2、深度为 $O(\log d)$ 的公式至多只能计算关于 $\mathrm{poly}(d)$ 个变量的多项式，而规模为 s的公式最多可以有 s 个变量。不过，这并不排除将乘积门的扇入降至 2。事实上， [VSBR83] 的电路深度约简正是这样做的。下面我们将证明，对于语法次数有界的代数公式，也可以做到这一点。

定理 12. 设 F 是一个规模为 s、深度为 Δ、语法次数为 $d \geqslant 1$ 的（交换或非交换）代数公式 F，它计算多项式 P。那么， P 也可以由一个规模为 s、深度为 $\Delta' = O(\Delta + \log d)$ 的公式 F' 计算，其中 F' 的每个乘积门的扇入均为 2。此外，如果 F 是齐次公式和/或单调公式，那么 F' 也具有相同的性质。

将其代入定理 7，可得到一个深度为 $O(\log d)$ 、规模为 $\mathrm{poly}(s)$ 的公式深度约简，使得所有乘积门的扇入至多为 2。将该结论与定理 11 结合，还可以得到类似的结果，并进一步减小规模的膨胀。

证明。只需证明上述定理的一个较弱版本，即每个乘积门的扇入至多为 3。随后，我们可以将每个扇入为 3 的乘积替换为由扇入为 2 的乘积门组成的树，其规模为 3。这样做至多会使深度增加一倍，而这不会影响整体结果。

因此，我们将证明这个稍弱的版本。在这种情况下，我们的目标是得到深度为 $\Delta' = \Delta + \log d$.

这是通过对公式的深度 Δ 进行归纳法完成的。 $\Delta = 0$ 的情形是平凡的。设 F 是一个深度为 $\Delta > 0$ 、语法次数为 d 的公式。

假设 F的输出门是求和门，且 $F_1, \ldots, F_t$ 是 F中深度为 $\Delta - 1$的子公式。根据定义，每个 F_i 的语法次数至多为 d。对每个 F_i 应用归纳假设，可得到一个乘积门扇入至多为 3 的公式F_i' 。随后可将这些公式之和定义为公式 F' 。

现在讨论主要情形，即 F 的输出门是乘积门。假设 $F_1, \ldots, F_t$ 是 F中深度为 $\Delta - 1$ 的子公式，并按照它们在 F中出现的顺序排列为[11]。令 d_i 表示 F_i的语法次数。定义

$$m = \min\{j \mid \sum_{i=1}^{j} d_i \geqslant d/2\}.$$

令 F_ℓ 为从 F中仅保留子公式 $F_1, \ldots, F_{m-1}$后得到的公式，并令F_r 为仅保留 $F_{m+1}, \ldots, F_t$. 后得到的公式。我们对F_ℓ、 F_m和 F_r 应用归纳假设，得到公式 F_ℓ'、 F_m'和 F_r'。最后，令

$$F' = F_\ell' \times F_m' \times F_r'.$$

规模[1] [2] F'的规模是 F_ℓ'、 F_m'和 F_r'的规模之和，根据归纳假设，该规模至多为 s n

[11]在非交换情形下，顺序很重要。[12]回想一下，公式的规模是其叶节点的数量。

。设 Δ'_ℓ、 Δ'_m和 Δ'_r分别表示 F'_ℓ、 F'_m和 F'_r的深度。F' 的深度为

$$1+\max\{\Delta'_\ell,\Delta'_m,\Delta'_r\}\leqslant 1+\max\{\Delta+\log(d/2),\Delta-1+\log d,\Delta+\log(d/2)\}=\Delta+\log d$$

其中第二个不等式用到了归纳假设，以及 F_ℓ 和 F_r 的语法次数至多为 $d/2$，且 F_m的深度至多为 $\Delta-1$. 这一事实 □

4 紧性

给定整数 $k\geqslant 1$ 和 $r\geqslant 2$，我们将定义一个多项式 $H^{(k,\ r)}$。直观地说，我们希望将这个多项式定义为公式的标准通用多项式。它由 k层嵌套内积组成，每个内积的规模为 r。下文中，我们将省略 $H^{(k,\ r)}$ 中的上标，并简写为 H 。

多项式 H 将定义在由 $(2r)^k$ 个变量组成的集合上

$$\{x_{\sigma,\tau}\mid\sigma\in[2]^k,\tau\in[r]^k\}.$$

令我们 递归地定义多项式 $H_{u,\ v}$，对所有满足 $|u|=|v|$的 $(u、\ v)\in[2]^{\leqslant k}\times[r]^{\leqslant k}$：

$$H_{u,v}=x_{u,v}\qquad\text{when } |u|=|v|=k$$
$$H_{u,v}=\sum_{a=1}^{r}H_{u1,va}H_{u2,va}\qquad\text{否则。}$$

多项式 H 定义为多项式 $H_{\varepsilon,\ \varepsilon}$。注意， H 是一个次数为$d=2^k$ 、含有 r^{d-1} 个单项式的多项式。

根据其定义， H 由一个规模为 $(2r)^k$ 、深度为 $2k$的单调公式 M 计算得出。该公式顶层是一个 $+$门，层间交替排列着 $+$门和 $\times$门，其中 $+$门的扇入为 r， $\times$门的扇入为 2，叶节点标记着互不相同的变量。

对于同一字母表上的词 u 和 v，如果 u 是 v的前缀，我们记作 $u\sqsupset v$ 。词 $([r]\times[2])^k$ 的前缀与 M的节点之间存在自然的一一对应关系，具体如下。设 $\sigma=\sigma_1\dots\sigma_k\in[2]^k$，且 $\tau=\tau_1\dots\tau_k\in[r]^k$。词 $\tau_1\sigma_1\dots\tau_k\sigma_k$对应于一条从 M 的根到标记为 $x_{\sigma,\ \tau}$的叶节点的路径，而$\tau_1\sigma_1\dots\tau_k\sigma_k$的真前缀则对应于这条路径上 M中的内部门。对于 $\ell<k$、 $u=u_1\dots u_\ell\in[2]^\ell$和 $v=v_1\dots v_\ell\in[r]^\ell$，与词 $v_1u_1\dots v_\ell u_\ell$对应的节点是$M$ 中计算 $H_{u,\ v}$的 $+$门。

容易看出，多项式 H 关于变量集合 $\{X_\sigma\mid\sigma\in[2]^k\}$ 是集合多线性的，其中 $X_\sigma=\{x_{\sigma,\ \tau}\mid\tau\in[r]^k\}$。这意味着每个单项式恰好从每个集合 X_σ 中取一个变量。

注 13。对于 $|u|=|v|=\ell\leqslant k$、 $u\in[2]^\ell$ 和 $v\in[r]^\ell$，多项式 $H^{(k,\ u\,v^{r)},}$ 定义在变量集合

$$X_{u,v}=\{x_{\sigma,\tau}\mid\sigma\in[2]^k,\ \tau\in[r]^k,u\sqsupset\sigma,\ v\sqsupset\tau\}$$

上，并且是多项式 $H^{(k-\ell,\ r)}$ （对变量进行重命名即可得到）。特别地，其次数为 $d'=2^{k-\ell}$，包含 $r^{d'-1}$ 个单项式，并且关于 $\{X_\sigma\mid\sigma\in[2]^k、\ u\sqsupset\sigma\}$ 是集合多线性的。

在证明 H 小深度单调公式的困难性之前，我们需要说明，计算 H 的单调公式中的门不能计算过多单项式。下文的引理 15 将证明这一点。

命题 14。考虑两个变量 $x_{\sigma,\ \tau}$ 和 $x_{\sigma',\ \tau'}$。如果 $x_{\sigma,\ \tau}x_{\sigma',\ \tau'}$ 出现在 H 的某个单项式中，并且 σ 和 σ' 有长度为 $\ell < k$ 的公共前缀，那么 τ 和 τ' 有长度为 $\ell+1$ 的公共前缀。

证明。观察可知，$x_{\sigma_1,\ \tau_1}\cdots x_{\sigma_p,\ \tau_p}$ 是 H 的一个单项式，当且仅当这些变量构成 M解析树的叶节点。如上所述，通向 M 中变量$x_{\sigma_i,\ \tau_i}$ 的根到叶路径，依次取 τ_i的第一个字母、 σ_i的第一个字母、 τ_i的第二个字母，等等即可得到。

如果乘积$x_{\sigma,\ \tau}x_{\sigma',\ \tau'}$ 出现在 H的一个单项式中，那么就必须能够将从根到$x_{\sigma,\ \tau}$ 的路径与从根到$x_{\sigma',\ \tau'}$的路径的并补全为公式 M的一棵解析树。

如果 τ 和 τ' 的最长公共前缀长度至多为 ℓ，那么 M 中$x_{\sigma,\ \tau}$ 与$x_{\sigma',\ \tau'}$ 的最近公共祖先将是一个 $+$-门；但在每个 $+$-门都只有一个子节点的解析树中，这是不可能的。

□

引理 15. 若 F 是一个计算多项式 H 的单调公式，且 α 是 F 中次数为 d_α的一个门，则在门 α 处计算得到的多项式的单项式数量至多为 $r^{d_\alpha-1}$。

证明。由于 H 有 r^{d-1} 个单项式，当 $d_\alpha = d$ 时，根据单调性，结论成立。现在假设 $d_\alpha < d$。

Let

$$I = \{\sigma \in [2]^k \mid \text{some variable of } X_\sigma \text{ appears in } \alpha\}.$$

对于 $u \in [2]^{\leqslant k}$，令 $I_u = \{\sigma \in [2]^k \mid u \sqsupset \sigma\}$。令 $\{u_1,\dots,u_p\}$ 为满足 $I_w \subseteq I$的最短词 w 组成的集合。那么 I 是 $\bigcup_{\ell\in[p]} I_{u_\ell}$的不相交并。由于 $d_\alpha < d$, $I \neq [2]^k$，因此没有u_ℓ 是空词。

考虑某个 $\ell \in [p]$。令 $\bar{u}_\ell$ 为将 u_ℓ的最后一个字母替换后得到的词。根据 u_ℓ长度的最小性，必有 $I_{\bar{u}_\ell} \not\subseteq I$。令 σ 为 $I_{\bar{u}_\ell}\backslash I$中的一个词。由于 F 是单调的，且计算一个集合多线性多项式，因此它是一个集合多线性公式，所以在 α 处计算得到的多项式必定要乘以某个变量 $x_{\sigma,\ \tau}$。令 v_ℓ 为 τ长度为 $|u_\ell|$ 的前缀。考虑出现在 α 中的任意变量 $x_{\sigma',\ \tau'}$，使得 $u_\ell \sqsupset \sigma'$。由于乘积 $x_{\sigma,\ \tau}x_{\sigma',\ \tau'}$根据单调性必定出现在 H的某个单项式中，因此由命题 14 可知，必有 $v_\ell \sqsupset \tau'$。

多项式 m 中由门 α 计算出的任意单项式，都可以唯一地写成 $m = m_1\cdots m_p$，其中 m_ℓ 相对于 $\{X_\sigma \mid u_\ell \sqsupset \sigma\}$是集合多线性的。由上可知， m_ℓ 是变量 $X_{u_\ell,\ v_\ell}$ 上的一个次数为 $|I_{u_\ell}|$ 的单项式。根据单调性，应当可以将 M 中标记为变量 m_ℓ 的叶节点补全为 M 的一棵解析树，该树出现在 H中；这证明了 m_ℓ 是 $H_{u_\ell,\ v_\ell}$的一个单项式。根据注 13，这类子单项式至多有 $r^{|I_{u_\ell}|-1}$ 个m_ℓ 。由此可知，节点 α 中计算出的多项式的单项式数量至多为

$$\prod_{\ell=1}^{p} r^{|I_{u_\ell}|-1} \leqslant r^{|I|-1} = r^{d_\alpha-1}.$$

□

我们现在准备证明多项式 H 的单调计算是困难的。我们将使用以下“乘积引理”；该引理有多种形式，例如见 [SY10、HY11、Sap15]。

引理 16. 一个次数为 d 、规模为 s、乘积深度为 Δ 的齐次公式 F，可以写成 $O(s)$ 个多项式的和，其中每个多项式都是由 $\Omega(\Delta d^{1/\Delta})$ 个正次数多项式相乘得到的。此外，这些多项式中的每一个都由 F 中的某个门计算。

命题 17. 如果 F 是一个乘积深度为 $\Delta \leqslant \log d$ 、计算 H 的单调公式，那么其规模至少为 $r^{\Omega(\Delta d^{1/\Delta})}$。

证明。设 $t = \Delta d^{1/\Delta}$。由于 F 是单调的，因此它是齐次的，并且根据引理 16，可以写成

$$F = \sum_{i=1}^{s'} \prod_{j=1}^{t_i} F_{i,j}$$

其中 $s' = O(s)$ 且 $t_i = \Omega(t)$ 对所有 i 成立，并且 $F_{i,\,j}$ 的次数至少为 1，且由 F 中的某个门计算。

设 $d_{i,\,j}$ 为 $F_{i,\,j}$ 的次数。根据引理 15，每个 $F_{i,\,j}$ 至多计算 $r^{d_{i,\,j}-1}$ 个单项式。因此，$\prod_{i=1}^{t_j} F_{i,\,j}$ 的单项式数量有如下界

$$\prod_{j=1}^{t_i} r^{d_{i,j}-1} \leqslant r^{\sum_{j=1}^{t_i} d_{i,j} - t_i} \leqslant r^{d-t}$$

因为 $\sum_{j=1}^{t_i} d_{i,\,j} = d$。由此可知，$F$ 计算的单项式数量至多为 $s \cdot r^{d-t}$。由于 F 计算了 H，它有 r^{d-1} 个单项式，因此得到 $s = r^{\Omega(t)}$。 □

现在，我们可以推出引言中的定理 3；为方便起见，这里重述如下。

定理 18。设 n 和 $d = d(n)$ 是增长参数，且满足 $d(n) \leqslant \sqrt{n}$。那么存在一个单调代数公式 F，其规模至多为 n，深度为 $O(\log d)$，计算次数至多为 d 的多项式 $P \in \mathbb{F}[x_1, \ldots, x_n]$；并且任何深度为 $o(\log d)$、计算 P 的单调公式 F'，其规模都必须为 $n^{\omega(1)}$.

定理 3 的证明。选择参数 $k(n)$ 和 $r(n)$，使得 $P(n) := H^{(k,\,r)}$ 有 $\Theta(n)$ 个变量，次数为 $\Theta(d)$：令 $k = \log d$ 和 $r = \frac{1}{2} n^{1/\log d}$。条件 $d(n) \leqslant \sqrt{n}$ 保证 $r \geqslant 2$。多项式 P 有一个规模为 $O(n)$ 、深度为 $O(\log d)$ 的单调公式。根据命题 17，任何计算 P、乘积深度为 $\Delta \leqslant \log d$ 的单调公式，其规模为

$$r^{\Omega(\Delta d^{1/\Delta})} = \left(\frac{1}{2} n^{1/\log d}\right)^{\Omega(\Delta d^{1/\Delta})} = (n/d)^{\left(\frac{\Delta d^{1/\Delta}}{\log d}\right)}$$

根据假设 $d(n) \leqslant \sqrt{n}$，其为 $n^{\Omega\left(\frac{\Delta d^{1/\Delta}}{\log d}\right)}$。由于当 $\Delta = o(\log d)$ 时，$\frac{\Delta d^{1/\Delta}}{\log d} \to +\infty$，因此这个界为 $n^{\omega(1)}$.

□

5 结论与开放问题

本文研究了将一个规模为 s 、计算次数为 d 的多项式的公式深度降低至 $O(\log d)$，同时保持规模为 $s^{O(1)}$ 的可能性。

我们证明了（定理 1），当 F 为齐次时，可以进行这样的变换。更一般地，定理 7 表明，只要 F 的语法次数在 d 中有多项式界，我们就能实现这一点。

VF 内部结构。考虑一个多项式序列 (f_n)，其变量数和次数关于 n 有多项式界（这样的族通常称为 p-族，¨例如参见 [B00]）。于是，我们可以考虑此类族的三个类别：

- $\mathrm{hom}\mathsf{F}[s(n)] = \{(f_n) \mid f_n$ 由一个规模为 $\mathsf{poly}(s(n))\}$ 的齐次公式计算得出，

- lowSynDegF$[s(n)] = \{(f_n) \mid f_n$ 由一个规模为 poly$(s(n))$ 、语法次数为 poly(deg$(f_n))\}$ 的公式计算得出
- lowDepthF$[s(n)] = \{(f_n) \mid f_n$ 由一个规模为 poly$(s(n))$ 、深度为 $O($logdeg$(f_n))\}$ 的公式计算。

显然，我们有包含关系 homF$[s(n)] \subseteq$ lowSynDegF$[s(n)]$。此外，本文证明了包含关系 lowSynDegF$[s(n)] \subseteq$ lowDepthF$[s(n)]$。因此，

$$\text{homF}[\text{poly}(n)] \subseteq \text{lowSynDegF}[\text{poly}(n)] \subseteq \text{lowDepthF}[\text{poly}(n)] \subseteq \text{VF},$$

我们不知道这些包含关系是否为真包含。

初等对称多项式的复杂度。上述问题中一个特别有趣的特例来自初等对称多项式。给定参数 d, n ，其中 $d \leqslant n$，回顾一下，初等对称多项式 $S_n^d(x_1, \ldots, x_n)$ 是所有次数恰为 d 的多线性单项式之和。Ben-Or 的一个简单而优雅的构造（见 [SW01]）表明，对于任意 d，多项式 S_n^d 都有一个深度 3、规模为 $O(n^2)$. 的非齐次公式。这使得这族多项式属于类 lowDepthF[poly(n)]. 。此外，Shpilka 和 Wigderson [SW01, 定理 5.3],证明了 S_n^d 有语法次数至多为 poly(d) 的深度 6 公式，因此它属于类 lowSynDegF[poly(n)].

然而，据我们所知，目前还没有已知的规模为 poly(n) 的齐次公式能够计算这族多项式。[13] 事实上，在一些额外限制下，Hrubeˇs 和 Yehudayoff 证明了 [HY11] 一个超多项式齐次公式下界，当 $d = n/2$ 时成立。去除这些限制将证明 homF[poly(n)] 与 lowSynDegF[poly(n)] 之间存在分离。另一方面，如果初等对称多项式确实存在规模为 poly(n) 的齐次公式，那么便可据此论证，[14] 任何由规模为多项式的深度 3 公式计算的多项式也具有同样性质，这暗示 homF[poly(n)] 与 lowSynDegF[poly(n)] 之间可能发生坍缩。

高深度公式的下界。得益于 [LST21b], 近期的下界结果，我们知道存在一个次数为 d 、含有 n 个变量的显式齐次多项式 $P(X)$ ，对于某个绝对常数 $\varepsilon > 0$，任何规模为 poly(n) 且深度为 $\varepsilon \cdot$ log log d 的公式都无法计算它。事实证明，多项式 P 可以由代数分支程序计算，因此属于称为 VBP 的复杂度类。

众所周知，VF 包含于 VBP。然而，我们尚不清楚这种包含是否是严格的。我们的下界结果有助于将这个问题细化。具体而言，该结果表明，如果能将 [LST21b] 中的下界从 Ω(log log d) 提高到 $\omega(\log d)$，那么我们就能分离 VF 和 VBP。

我们的深度约简能够推广到非交换情形，这一事实有力地说明，值得重新审视非交换情形下的 VF 与 VBP 问题。具体而言， [TLS22] 最近的一项结果表明，存在一个显式的非交换多项式 $P(X)$, 其次数为 d ，涉及 n 个变量，且无法由任何规模为 poly(n) 、深度为 $\varepsilon \cdot \sqrt{}$ log d 的非交换公式计算。因此，若能将此情形下的下界从 $\Omega(\sqrt{\log d})$ 提高到 $\omega(\log d)$，就能在非交换情形下区分 VF 和 VBP。

[13] Nisan 和 Wigderson 曾提出一个更强的猜想 [NW97], , 但后来被 Hrubeš 和 Yehudayoff [HY11] 推翻。不过，这仍未能为所有初等对称多项式给出多项式规模的齐次公式。[14] 标准论证见例如 [LST21b, Section III]

参考文献

[AV08] Manindra Agrawal 和 V. Vinay。算术电路：深度四的鸿沟。载于《计算机科学基础研讨会》（FOCS）论文集，第 67–75 页，2008 年。.[B00] Peter B¨urgisser。Cook 猜想与 Valiant 猜想。理论计算机科学，235(1)：71–88，2000 年。[BB94] Maria Luisa Bonet 和 Samuel R. Buss。布尔公式的规模-深度权衡。信息处理快报，49(3)：151–155，1994 年。[BCE95] Nader H. Bshouty、Richard Cleve 和 Wayne Eberly。代数公式的规模-深度权衡。SIAM计算杂志，24(4)：682–705，1995 年。[BKM73] R. Brent、D. Kuck 和 K. Maruyama。无除法算术表达式的并行求值。IEEE 计算机汇刊，C-22(5)：532–534，1973 年。[Bre74] Richard P. Brent。一般算术表达式的并行求值。ACM 杂志，21(2)：201–206，1974年4月。[CKSV16] Suryajith Chillara、Mrinal Kumar、Ramprasad Saptharishi 和 V. Vinay。深度四的鸿沟与张量秩：旧结果，新见解。CoRR，abs/1606.04200，2016 年。[CLS18] Suryajith Chillara、Nutan Limaye 和 Srikanth Srinivasan。迭代矩阵乘法的小深度多线性公式下界及其应用。载于 STACS，LIPIcs 第 96 卷，第 21:1–21:15 页。Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik，2018 年。[GKKS16] Ankit Gupta、Pritish Kamath、Neeraj Kayal 和 Ramprasad Saptharishi。算术电路：深度 3 的鸿沟。SIAM计算杂志，45(3)：1064–1079，2016 年。[HY11] Pavel Hrubeˇs 和 Amir Yehudayoff。齐次公式与对称多项式。计算复杂性，20(3)：559–578，2011 年。[KdOS19] Mrinal Kumar、Rafael Mendes de Oliveira 和 Ramprasad Saptharishi。面向语法多线性电路的最优深度约简。载于 Christel Baier、Ioannis Chatzigiannakis、Paola Flocchini 和 Stefano Leonardi 编，《第 46 届自动机、语言与编程国际研讨会》，ICALP 2019，2019年7月9日至12日，希腊帕特雷，LIPIcs 第 132 卷，第 78:1–78:15 页。Schloss Dagstuhl - Leibniz-Zentrum f¨ur Informatik，2019 年。[Koi12] Pascal Koiran。算术电路：深度四的鸿沟进一步扩大。理论计算机科学，448：56–65，2012 年。[Kos86] S Rao Kosaraju。无除法算术方程的并行求值。载于第十八届 ACM 计算理论研讨会论文集，第 231–239 页，1986 年。[KSS14] Neeraj Kayal、Chandan Saha 和 Ramprasad Saptharishi。正则算术公式的超多项式下界。载于 David B. Shmoys 编，《计算理论研讨会》，STOC 2014，美国纽约州纽约市，2014年5月31日至6月3日，第 146–153 页。ACM，2014 年。

[LST21a] Nutan Limaye、Srikanth Srinivasan 和 S´ebastien Tavenas。《低深度代数电路的超多项式下界》。《电子计算复杂性讨论会》，TR21-081，2021年。[LST21b] Nutan Limaye、Srikanth Srinivasan 和 S´ebastien Tavenas。《低深度代数电路的超多项式下界》。载于第62届 IEEE 年度计算机科学基础研讨会（FOCS 2021），美国科罗拉多州丹佛，2022年2月7日至10日，第804–814页。IEEE，2021年。[Nis91] Noam Nisan。《非交换计算的下界》。载于第二十三届 ACM 计算理论年度研讨会论文集，第410–418页，1991年。[NW97] Noam Nisan 和 Avi Wigderson。《通过偏导数得到算术电路的下界》。《计算复杂性》，6(3):217–234，1997年。[PM75] Franco P. Preparata 和 David E. Muller。《求值无除法算术表达式所需的时间》。《信息处理快报》，3(5):144–146，1975年。[PM76] Franco P. Preparata 和 David E. Muller。《布尔表达式的高效并行求值》。《IEEE 计算机汇刊》，25(5):548–549，1976年。[Raz06] Ran Raz。《多线性电路与公式规模的分离》。《计算理论》，2(1):121–135，2006年。[Raz13] Ran Raz。《算术公式的张量秩与下界》。《ACM 杂志》，60(6):40:1–40:15，2013年。[RY08] Ran Raz 和 Amir Yehudayoff。《语法多线性算术电路的平衡化》。《计算复杂性》，17(4):515–535，2008年。[Sap15] Ramprasad Saptharishi。《算术电路复杂性下界综述》。Github 综述，2015年。[Spi71] Philip M. Spira。《布尔函数中的时间—硬件复杂性权衡》。载于 Shu Lin 编，第4届夏威夷国际系统科学会议论文集，第525–527页。Western Periodicals Company，美国加利福尼亚州北好莱坞，1971年。[SS80] Eli Shamir 和 Marc Snir。《关于公式的深度复杂性》。《数学系统理论》，13:301–322，1980年。[SW01] Amir Shpilka 和 Avi Wigderson。《特征为零的域上的深度 3 算术电路》。《计算复杂性》，10(1):1–27，2001年。[SY10] Amir Shpilka 和 Amir Yehudayoff。《算术电路：近期成果综述与开放问题》。《理论计算机科学基础与趋势》，5:207–388，2010年3月。[Tav15] S´ebastien Tavenas。《归约到深度4和深度3的改进界》。《信息与计算》，240:2–11，2015年。[TLS22] S´ebastien Tavenas、Nutan Limaye 和 Srikanth Srinivasan。《迭代矩阵乘法的集合多线性与非交换公式下界》。载于 STOC，第416–425页。ACM，2022年。

[VSBR83] Leslie G. Valiant、Sven Skyum、Stuart J. Berkowitz 和 CharlesRackoff。《使用少量处理器快速并行计算多项式》。《SIAM计算杂志》，12(4):641–644，1983年。[YK68] SV Yablonskii 和 VP Kozyrev。《控制论中的数学问题》。载于苏联科学院复杂问题“控制论”科学委员会信息资料，19:3–15，1968年。

A Bonet-Buss 深度缩减

本节中，我们给出定理 10 的证明。这基本上与 Bonet 和 Buss [BB94], 的工作中的证明相同；但由于该论文中的结果仅针对布尔公式陈述，我们在此给出证明以求完整。

我们证明，存在一个足够大的绝对常数 $C > 0$，使得任何由规模为 s 的公式 F 计算的多项式 P，也可以由规模至多为 $s^{1+\varepsilon}$、深度至多为 $2^{O(1/\varepsilon)} \cdot \log s$ 且扇入为 2 的公式 F' 计算。此外，如果 F 是齐次／单调／非交换的，那么 F' 也具有相同性质。后一结论可直接由构造得出。

这里我们假设 F 中的每个门一开始的扇入都是 2。我们可以在开始时对 F 作此修改，代价是增加深度，但不增加规模。

我们通过对公式的规模 s 进行归纳法来证明该结论。设 $T(s)$ 和 $D(s)$ 分别表示由此得到的最大规模和深度，并假设 F' 的规模至多为 F。令 $s.$，其中 $k = 2^{C/\varepsilon}$ 是我们将在下文选定的绝对常数。我们始终假设 $C > 0$，这不失一般性。

公式的基础情形是 $s \leqslant k$，此时结论显然成立，因为任何规模为 s 的公式，其深度至多为 s，而在此情形下该值至多为 $2^{C/\varepsilon}$.。

现在，假设 $s > k.$。在这种情况下，我们找到一个门 α，使得以 α 为根的子公式 F_α 的规模至少为 $s - s/k,$，而 α 的子节点 β 和 γ 不满足这一性质。容易看出，具有这一性质的 α 是唯一的。令 $*$ 表示标记 $\alpha.$ 的运算（即 $+$ 或 $\times$）。

我们用一个新的变量 y 替换 F 中的 α，得到公式 F_y。注意， F_y 的规模至多为 $s_1 = \frac{2s}{k}.$。由于 F_y 中 y 至多出现一次，我们可以写成

$$F_y = A \cdot y \cdot B + C$$

其中， A 是沿着通往输出的路径，在 F 中所有从左侧与 y 相乘的子公式的乘积；类似地， B 是所有从右侧与 y 相乘的子公式的乘积；而 C 是将 y 设为 0 时 F_y 计算出的多项式。显然， A、 B 和 C 的公式分别为 F_A、 F_B 和 F_C，其规模至多为 s_1。最后，我们得到公式 F'，如图 1 所示。

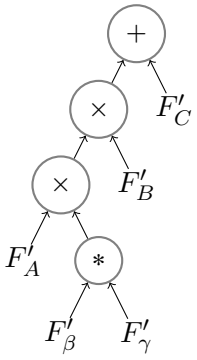

图 1：构造 F'

这里， F'_A、 F'_B、 F'_C、 F'_β 和 F'_γ 是通过对 F_A、 F_B、 F_C、 F_β、 F_γ 递归地应用相同过程得到的公式。

我们可以通过归纳法界定深度约简公式的规模和深度。我们有

$$D(s) \leqslant D(s - s/k) + O(1)$$

由此很容易得出整体深度上界为 $O(k\log s) = 2^{O(1/\varepsilon)} \cdot \log s$，其中常数 C 可任意选取。

对于规模，我们有如下递推关系。

$$T(s) \leqslant \max_{\substack{s_\beta, s_\gamma, s_1: \\ s_\beta, s_\gamma \leqslant s(1-1/k) \\ s_1 \leqslant 2s/k \\ s_\beta + s_\gamma + s_1 \leqslant s}} T(s_\beta) + T(s_\gamma) + 3T(s_1)$$

其中，s_β 和s_γ 分别是 F_β 和 F_γ 的规模。现在我们使用归纳法对 $T(s)$进行如下界定。（为简洁起见，我们省略了关于s_β、s_γ 和 s_1 的条件。）

$$\begin{aligned} T(s) &\leqslant \max_{s_\beta, s_\gamma, s_1} s_\beta^{1+\varepsilon} + s_\gamma^{1+\varepsilon} + 3s_1^{1+\varepsilon} \\ &\leqslant \left(s\left(1-\frac{1}{k}\right)\right)^{1+\varepsilon} + \left(\frac{s}{k}\right)^{1+\varepsilon} + 3\left(\frac{2s}{k}\right)^{1+\varepsilon} \end{aligned}$$

其中我们用到了这样一个事实： $s_1 \leqslant 2s/k$ ；还用到了这样一个事实：利用映射$x \mapsto x^{1+\varepsilon}$的凸性，函数 $s_\beta^{1+\varepsilon} + s_\gamma^{1+\varepsilon}$在$\max\{s_\beta, s_\gamma\} = s - s/k$,时取最大值，这意味着$\min\{s_\beta, s_\gamma\} \leqslant s/k$.

继续计算可得

$$T(s) \leqslant s^{1+\varepsilon}\left(\left(1-\frac{1}{k}\right) + \frac{1}{k^{1+\varepsilon}} + 3\frac{4}{k^{1+\varepsilon}}\right) \leqslant s^{1+\varepsilon} \cdot \left(1 - \frac{1}{k} + \frac{C'}{k^{1+\varepsilon}}\right)$$

对于某个足够大的绝对常数 C'。取足够大的绝对常数 C，令 $k = 2^{C/\varepsilon}$，即可得到 $T(s) \leqslant s^{1+\varepsilon}$，从而证明归纳命题。