arXiv:2303.06001v1 [cs.CC] 10 Mar 2023

非交换多项式因式分解的多元到二元归约

V. Arvind* Pushkar S Joglekar†

摘要

基于 Bergman 的一个定理 [5]，我们证明，多元非交换多项式的因式分解可在确定性多项式时间内归约为二元非交换多项式的因式分解。更具体地说，我们证明如下结论：

1. 在白盒设定下，给定域 $\mathbb{F}$（有限域或有理数域）上的一个 n 元非交换多项式 $f \in \mathbb{F}\langle X\rangle$，其表示为算术电路（或代数分支程序），计算 f 的完全因式分解可在确定性多项式时间内归约为一个非交换二元多项式 $g \in \mathbb{F}\langle x, y\rangle$ 的白盒因式分解；该归约将 f 转换为表示 g 的电路（或表示 g 的代数分支程序），并且给定 g 的完全因式分解后，该归约可在多项式时间内恢复 f 的完全因式分解。我们还在黑盒设定下得到了类似的确定性多项式时间归约。

2. 此外，我们证明，在有理数域上，4×4 矩阵的二元线性矩阵因式分解至少与分解无平方因子整数一样困难。这表明，即使在二元情形下，在有理数域上将非交换多项式因式分解归约为线性矩阵因式分解（如 [1] 中所做的那样）也不太可能成功。与此相反，有理数域上 3×3 矩阵的多元线性矩阵因式分解可在多项式时间内完成。

1 引言

本文的主要目标是证明，在自由非交换环 $\mathbb{F}\langle x_1, x_2, \ldots, x_n\rangle$ 上的多元多项式分解可在多项式时间内归约为二元环 $\mathbb{F}\langle x, y\rangle$ 上的二元非交换多项式分解。对于交换多项式分解，Kaltofen 关于交换多项式环 $\mathbb{F}[y_1, y_2, \ldots, y_n]$ [9, 10] 上多元多项式分解的开创性工作已经给出了这一结果。然而，在非交换多项式的情形下，这个问题一直悬而未决。最近，[1] 针对输入以非交换公式给出的有限域上的非交换多项式分解问题，提出了一种随机多项式时间算法。[1] 广义而言，[1] 的算法通过 Higman 线性化（[8] [6] [7]）将问题归约为线性矩阵分解问题；事实证明，该问题在有限域上存在随机多项式时间算法。

*数学科学研究所，印度金奈；金奈数学研究所，印度西鲁塞里、凯兰巴卡姆，电子邮箱：arvind@imsc.res.in

†印度浦那毗湿瓦卡玛理工学院，电子邮箱：joglekar.pushkar@gmail.com[1]齐次非交换多项式的因式分解较为容易，因为它可以归约为一类特殊交换多项式的因式分解。详情见 [4]。

问题 1.1 (线性矩阵分解问题)。 域上的线性矩阵分解问题$\mathbb{F}$ 以一个线性矩阵作为输入： $L = A_0 + \sum_{i=1}^{n} A_i x_i$，其中 A_i 是 $d \times d$ 标量矩阵（定义在 $\mathbb{F}$上），x_i和 $1 \le i \le n$ 是非交换变量；出于技术原因，假设 A_0 可逆。该问题要求计算 L 的一个因式分解，将其表示为不可约线性矩阵的乘积。

矩阵分解（尤其是线性矩阵因式分解）的研究，是 Cohn 关于一般自由理想环上分解理论的重要组成部分。 [6] [5]。

回到 [1], 中描述的多项式分解算法，该算法将多项式分解归约为线性矩阵因式分解，而后者又可归约为计算一组 n 矩阵的公共不变子空间这一问题。对于有限域，利用基于代数分解的 Artin-Wedderburn 定理的 Ronyai 算法 [12]，可以高效地解决公共不变子空间问题。然而，当 $\mathbb{F}$ 是有理数域时，这种方法会遇到严重困难。主要困难在于，给定一个有理数域上的单矩阵代数[2] $\mathcal{A}$，我们不知道如何设计高效算法来判定 $\mathcal{A}$ 是除代数，还是含有零因子。这正是我们希望将多元多项式分解归约为二元分解的动机之一。因为，对一个由公式给出的二元非交换多项式进行 Higman 线性化，将得到一个二元线性矩阵。人们可能会希望，二元线性矩阵的因式分解在计算上比 n 元线性矩阵的因式分解更简单。遗憾的是，事实并非如此。正如我们将看到的，即使对于维数为 4 的二元线性矩阵，因式分解问题也至少与分解无平方因子整数一样困难。

从多元到二元我们先介绍一些形式化预备知识。设 $\mathbb{F}$ 是任意一个域，$X = \{x_1, x_2, \ldots, x_n\}$ 是一组 n 自由非交换变量。令 X^* 表示字母表 X 上的所有自由字（即单项式）构成的集合，其中字的拼接是幺半群运算，空字 ϵ 是单位元。

自由非交换环 $\mathbb{F}\langle X\rangle$由所有有限个 $\mathbb{F}$系数的单项式线性组合构成，其中变量取自X^*；环加法 $+$ 是逐系数相加，环乘法 $*$ 则是通常的卷积积。更准确地说，令 $f, g \in \mathbb{F}\langle X\rangle$，并令 $f(m) \in \mathbb{F}$ 表示多项式 f中单项式 m 的系数。那么，我们可以写成 $f = \sum^{m} f(m)m$ 和 $g = \sum^{m} g(m)m$；对于乘积多项式 fg 中的每个单项式 m，有

$$fg(m) = \sum_{m_1 m_2 = m} f(m_1)g(m_2).$$

单项式 $m \in X^*$ 的次数是该单项式 m的长度，而多项式 $f \in \mathbb{F}\langle X\rangle$的次数 $\deg f$ 是 f中系数非零的最高次单项式的次数。对于多项式 $f, g \in \mathbb{F}\langle X\rangle$，显然有 $\deg(fg) = \deg f + \deg g$。

多项式 $f \in \mathbb{F}\langle X\rangle$ 的非平凡因式分解 是将 f表示为多项式 g、$h \in \mathbb{F}\langle X\rangle$ 的乘积 $f = gh$，且满足 $\deg g > 0$和 $\deg h > 0$。若多项式 $f \in \mathbb{F}\langle X\rangle$ 没有非平凡因式分解，则称其为不可约；否则称其为可约。例如，$\mathbb{F}\langle X\rangle$ 中所有次数为 1 的多项式都是不可约的。显然，通过反复进行因式分解，$\mathbb{F}\langle X\rangle$ 中的每个多项式都可以表示为不可约多项式的乘积。

已知，多元多项式的非交换多项式恒等式测试（多项式恒等式测试）问题可轻易归约为二元多项式的非交换多项式恒等式测试：该归约由以下映射给出

[2]也就是说，该代数没有非平凡的双边理想。

通过代换

$$x_i \to xy^i, 1 \le i \le n,$$

它将一个计算多项式 $f(x_1, x_2, \ldots\ldots, x_n)$ 的给定算术电路（或公式或代数分支程序）变换为二元多项式 $g(x, y) = f(xy, xy^2, \ldots\ldots, xy^n)$。由于该代换映射保证 f 的每个单项式都映射为 $g(x, y)$ 中一个不同的单项式，因此很容易推出：f 是零多项式，当且仅当 $g(x, y)$ 是零多项式。

事实上，可以证明 [6, Excercise 2.5, Problem 14] 该代换映射给出了从环 $\mathbb{F}\langle x_1, x_2, \ldots, x_n\rangle$ 到 $\mathbb{F}\langle x, y\rangle$ 的单射同态。不幸的是，这个映射不能保持因式分解。例如，多项式 $f = x_3x_1 + x_4x_2 + x_4x_1 + x_5x_2 \in \mathbb{F}\langle X\rangle$ 显然不可约，但 f 在上述映射下的像可非平凡地分解为 $(xy^2 + xy^3)(yxy + y^2xy^2)$。因此，我们无法使用该代换映射，将非交换多元多项式分解归约为二元多项式分解。

Bergman 的 1-惰性嵌入 然而，基于 Bergman 的一个定理 [5, Chapter 4], ，我们可以构造一个多项式时间归约，将由算术电路（分别地，非交换代数分支程序（ABP））表示的 $\mathbb{F}\langle x_1, x_2, \ldots, x_n\rangle$ 中的多元非交换多项式因式分解，归约为由算术电路（分别地，ABP）表示的 $\mathbb{F}\langle x, y\rangle$ 中的二元非交换多项式因式分解。对于有限域和有理数，该归约都具有多项式时间复杂度。在有理数的情形下，我们需要确保所有相关数的比特复杂度均有多项式上界。此外，我们还证明，实质上相同的归约也适用于黑盒设置。

更准确地说，Bergman 定理 [5, 第 4 章，定理 5.2] 证明了一个将可数秩自由代数嵌入秩为 2 的自由代数中的 1-惰性嵌入。嵌入映射的 1-惰性性质将在下文定义。我们将定义限定于自由非交换多项式环。

定义 *1.2*（*1*-惰性嵌入）。 [5] 设 $X = \{x_1, x_2, \ldots\}$ 是一个可数无限集，其中的元素为自由非交换变量；$Y = \{x, y\}$ 是两个自由非交换变量。将 $\mathbb{F}\langle X\rangle$ 嵌入到$\mathbb{F}\langle Y\rangle$ 中的 *1*-惰性嵌入是一个单射同态 $\varphi: \mathbb{F}\langle X\rangle \to \mathbb{F}\langle Y\rangle$，使得对于每个多项式 $f \in \mathbb{F}\langle X\rangle$，若其像$\varphi(f)$ 在 $\mathbb{F}\langle Y\rangle$ 中有非平凡因式分解

$$\varphi(f) = g_1 \cdot g_2,$$

那么它们的原像 $\varphi^{-1}(g_1)$ 和 $\varphi^{-1}(g_2)$ 存在，并且由于 φ 是同态，它给出了 f 在环 $\mathbb{F}\langle X\rangle$中的一个非平凡因式分解 $f = \varphi^{-1}(g_1)\,\varphi^{-1}(g_2)$ 。

注释 *1.3.* 根据上述定义，对于所有因式分解 $\varphi(f) = g_1g_2$，多项式 g_1 和g_2 都在 φ 的值域内。我们注意到，*Cohn* 的工作 *[6, 5]* 讨论了针对一般非交换整环 R_1 和 R_2的 *1*-惰性嵌入 $\varphi: R_1 \to R_2$。在一般情形下，定义只要求存在某个单位元 $u \in R_2$，使得 g_1u 和 $u^{-1}g_2$ 属于映射 φ 的值域；这意味着因式分解$\varphi(f) = (g_1u)(u^{-1}g_2)$ 在 φ 的值域内成立。由于 $\mathbb{F}\langle X\rangle$ 中的单位元只有 $\mathbb{F}$ 的元素，对于多项式$f \in \mathbb{F}\langle X\rangle$，其像 $\varphi(f)$ 的因子全都属于 *1*-惰性嵌入 φ 的值域 $\varphi(\mathbb{F}\langle X\rangle)$。

定义 1.4. 非交换多项式 $f \in \mathbb{F}\langle X\rangle$ 的完全因式分解 是将其因式分解为$f = f_1 \cdot f_2 \cdots f_r$，即不可约多项式 $f_i \in \mathbb{F}\langle X\rangle$的乘积。

给定一个关于 f 的代数分支程序（分别地，算术电路），我们可以高效地得到一个关于 $\varphi(f)$ 的代数分支程序（分别地，算术电路），然后我们利用这一思路

在代数分支程序或电路上运行替换自动机（例如参见 [4], [2], [3]），根据 $\varphi(f)$ 的完全因式分解，构造出 f 的完全因式分解。下一节中，我们将详细阐述并扩展 Bergman 嵌入定理 [5]，并说明如何得到其有效的算法版本，以便根据 $\varphi(f)$ 的因子重构 f 的因子。

2 Bergman 嵌入

我们在 $\{x, y\}^*$ 中的单项式上定义如下全序。

定义 2.1. 对于 $m_1, m_2 \in \{x, y\}^*, m_1 \neq m_2$，若满足以下任一条件，我们称 $m_1 \prec m_2$：

- $m_1 = m_2$。
- 次数(m_1) <次数(m_2)。
- $\deg(m_1) = \deg(m_2)$ 并且若 $m_1 \neq m_2$，那么在它们不同的最左位置 i，有 $m_1[i] = y$ 和 $m_2[i] = x$。

上述序就是通常的二进制串字典序，其中将 y 视为 0，将 x 视为 1。对于任意多项式 g, $\mathrm{Mon}(g)$ 表示 g 中所有具有非零系数的单项式组成的集合。

当 $m_1 \prec m_2$ 时，我们称单项式 m_1 小于单项式 m_2。等价地， m_2 大于 m_1。多项式 $g \in \mathbb{F}\mathrm{h}x$, $y\mathrm{i}$ 的首项单项式是 $\mathrm{Mon}(g)$ 中满足 $w \prec m$ （对所有 $w \in \mathrm{Mon}(g)$）的单项式 $m \in$ （记作 $\mathrm{lm}(g)$）。也就是说， g 的首项单项式是 $\mathrm{Mon}(g)$ 中最大的单项式。

定义 2.2. 对于单项式 $m \in \{x, y\}^*$，令 $d_x(m)$ （分别地， $d_y(m)$）表示 m中 x （分别地， y）出现的次数。单项式 m 的不平衡 $i(m)$定义为

$$i(m) = d_x(m) - d_y(m).$$

令 B 为所有满足以下条件的多项式构成的代数：其中每个多项式的每个单项式的不平衡均为 0。

令 T 为所有满足以下条件的单项式 m 构成的集合：要么 $m = \epsilon$，要么 $i(m) = 0$，并且对于 m 的任意前缀 m'，若满足 $m' \neq \epsilon$，则 $m' \neq m$、 $i(m') > 0$。我们称这些单项式为极小平衡单项式。显然，在 T 中的所有非空单项式里，最左边的符号是 x。我们按字典序 $\prec$ 排列 T 中的非空单项式，并将序列中的第 i^{th} 个单项式记为u_i。令 u_i 为这样一个单项式：在 u_i中将每个 x 替换为 y，并将每个 y 替换为 x。令$T = \{\overline{u_i} \mid i \geq 1\}$。显然， T 和 T中的单项式共同生成代数 B。

令 C 为由$\{u_i + \overline{u_i} \mid i \geq 1\}$生成的代数。显然， C 是 B的子代数。

由于每个 u_i 和 $\overline{u_i}$ 都是平衡的，显然， C 中多项式的任意单项式的不平衡度都是 0。令 $X = \{x_1, x_2, \ldots\ldots, x_n\}$ 和 $X_\infty = \{x_1, x_2, \ldots\ldots\}$ 为一个可数无限集的不定元。

我们注意到 $B \setminus C$ 中的多项式具有一个关键性质。

引理 2.3。

- 任意多项式 m 的首项单项式具有如下形式： $m = u_{i_1} u_{i_2} \cdots u_{i_l}$，其中每个 $u_{i_j} \in T$。也就是说，m 不以任何 $\overline{u} \in T$为子词。

- 每个多项式 $f \in B \setminus C$ 都可以表示为 $f = g + h$，其中 $g \in C$ 且 $h \in B$。此外，若 $h \neq 0$，则 h 的首项单项式以某个 $\overline{u} \in T$ 为子词。

证明。根据代数 B（因此也根据 C）的定义，对于 $g \in B$ 以及任意单项式 $m \in \mathrm{supp}(g)$，我们有 $m \in (T \cup \overline{T})^*$。此外，每个 $g \in C$ 都是形如 $\prod_{k=1}^{\ell}(u_{i_k} + \overline{u_{i_k}})$ 的乘积的线性组合。因此，若 $\deg(g) = d$ 且 $\mathrm{supp}(g)$ 含有一个次数为 d 的单项式 $g_{j_1} g_{j_2} \ldots g_{j_\ell}$，其中 $g_{j_k} \in \{u_{j_k}, \overline{u_{j_k}}\}$ 对于 $k \in [l\,]$,成立，那么 $\mathrm{supp}(g)$ 也含有次数为 d 的单项式 $u_{j_1} u_{j_2} \ldots u_{j_\ell}$。根据定义 $\prec$，单项式 $u_{j_1} u_{j_2} \ldots u_{j_\ell}$ 比（关于序 $\prec$）所有含有某个 $\overline{u} \in T$ 作为子词的单项式都大。因此，任意多项式 $g \in C$ 的首项单项式都具有所声称的形式。

接下来，令 $f \in B \setminus C$。若 f 的首项单项式含有子词 $\overline{u} \in T$，则断言由 $\overline{f} = 0 + f$ 和 $0 \in C$ 得证。设 f 的首项单项式为 $m = u_{j_1} u_{j_2} \ldots u_{j_\ell}$，对所有 k 均有 $u_{j_k} \in T$。若 m 在 f 中的系数为 α，令

$$f_1 = f - \alpha(u_{j_1} + \overline{u_{j_1}})(u_{j_2} + \overline{u_{j_2}}) \ldots (u_{j_\ell} + \overline{u_{j_\ell}}). \tag{1}$$

如果 m_1 是 f_1 的首项单项式，那么显然 $m_1 \prec m$。此外，$f_1 \in B \setminus C$，因为 $f - f_1 \in C$。因此，只需证明对于某个满足所述性质的 $g_1 \in C$ 和 $h_1 \in B$，有 $f_1 = g_1 + h_1$。我们可以将公式 1 中的消去步骤应用于 f_1，得到 f_2，依此类推。在第 i^{th} 步，我们会得到一个新的多项式 f_i，其首项单项式小于 f和每个 $f_j, j < i$的首项单项式。由于 $\prec$-序在单项式上是良序，这个过程将会终止，从而得到所需的 f的表示式 $f = g + h$，其中 $g \in C$，且h 的首项包含子词 u，其中 $u \in T$。这就证明了第二部分。□

引理 2.4。存在一个从环 $\mathbb{F}\langle X_\infty \rangle$ 到$\mathbb{F}\langle x, y \rangle$的单射同态（即同态嵌入）。

证明。考虑函数 $\varphi : \mathbb{F}\mathrm{h}X_\infty\mathrm{i} \mapsto \mathbb{F}\mathrm{h}x,\ y\mathrm{i}$，定义如下：

- 对所有 $x_i \in X_\infty$，令 $\varphi(x_i) = u_i + \overline{u_i}$。
- 通过乘法将 φ 扩展到所有单项式。也就是说，$\varphi(x_{i_1} x_{i_2} \ldots x_{i_k}) = \prod_{j=1}^{k} \varphi(x_{i_j})$。
- 此外，利用线性性将 φ 扩展到环 $\mathbb{F}\mathrm{h}X_\infty\mathrm{i}$：$\varphi(\sum_{i=1}^{t} \alpha_i m_i) = \sum_{i=1}^{t} \alpha_i \varphi(m_i)$，其中 $m_i \in X_\infty^*$ 为单项式，$\alpha_i \in \mathbb{F}$ 为标量，$i = 1$从 t 到 t。

为证明 φ是同态，我们首先注意到，根据线性性，对于 $f, g \in \mathbb{F}\mathrm{h}X_\infty\mathrm{i}$，有 $\varphi(f+g) = \varphi(f) + \varphi(g)$。为验证 $\varphi(fg) = \varphi(f)\varphi(g)$，令 $f = \sum^m f_m m$，且 $g = \sum^m g_m m$，其中$f_m, g_m \in \mathbb{F}$ 分别是单项式 m 在 f 和 g中的系数。于是

$$\begin{aligned}
\varphi(fg) &= \varphi\left((\sum_m f_m m)(\sum_w g_w w)\right) \\
&= \varphi\left(\sum_{m,w} f_m g_w m w\right) \\
&= \sum_{m,w} f_m g_w \varphi(mw) \quad \text{(by linearity of } \varphi\text{)} \\
&= \left(\sum_m f_m \varphi(m)\right)\left(\sum_w f_w \varphi(w)\right) \\
&= \varphi(f)\varphi(g).
\end{aligned}$$

为了证明 φ 是单射，只需证明对于 $f \neq 0$， $\varphi(f) \neq 0$。假设 $m \in \text{supp}(f)$。那么根据 φ的定义，我们注意到 $\varphi(m) \neq 0$。因此，如果 m 是supp(f)中的唯一单项式，就可得出 $\varphi(f) \neq 0$。

否则，令 et $m' \in \text{supp}(f)$ 和 $m' \neq m$。令 u 为 m 和 m' 的最大公共前缀。 n

$$m = ux_iv \text{ and } m' = ux_jw,$$

对于单项式 $u, v, w \in X_\infty^*$ 和 $x_i \neq x_j$。注意到 $\varphi(x_i) = u_i + \overline{u}_i$ 且 $\varphi(x_j) = u_j + \overline{u}_j$，我们有 e

$$\varphi(m) = \varphi(u)(u_i + \overline{u}_i)\varphi(v) \text{ and } \varphi(m') = \varphi(u)(u_j + \overline{u}_j)\varphi(w).$$

根据 φ 的定义，显然 $\varphi(u)$ 是 $\mathbb{F}\langle\langle x, y\rangle\rangle$ 中的齐次多项式。令 $\deg(\varphi(u)) = D$。假设 $\mathrm{l} = |u_i| = |\overline{u}_i|$ 且 $\mathrm{l}' = |u_j| = |\overline{u}_j|$。不失一般性，可以假设 $u_i \prec u_j$。因此 $\mathrm{l} \leq \mathrm{l}'$。由于 u_i 和 u_j 是最小平衡的，u_i 不可能是 u_j 的前缀。因此，对于 $\text{supp}(\varphi(m_1))$ 和 $\text{supp}(\varphi(m_2))$ 中的任意单项式 w_1、w_2，w_1 和 w_2 在从位置 $D+1$ 开始的长度为 l 的子词上会不同。由此可得 $\text{supp}(\varphi(m)) \cap (\varphi(m')) = \emptyset$。因此，$\varphi(f) \neq 0$，这意味着 φ 是单射。□

接下来，我们将讨论代数 C 中多项式因式分解的一项重要性质。为了使论述自成一体，我们给出完整的证明，细节比 Cohn 的书 [5] 中更多。

定理 2.5 (Bergman)。 *[5, 第 4 章，定理 5。2]* 设 $f \in C$。对于任意因式分解 $f = g \cdot h$，多项式 g 和 h 均属于 C。

证明。首先，我们证明 g 的所有单项式具有相同的不平衡。同样，h 的所有单项式也具有相同的不平衡。设 a_{min} 和 a_{max} 分别是 g 的单项式不平衡的最小值和最大值。设 b_{min} 和 b_{max} 分别是 h 的单项式不平衡的最小值和最大值。设 m_{min} 是 g 中不平衡为 a_{min} 的所有单项式里，关于 $\prec$最小的单项式；设 m_{max} 是 g 中不平衡为 a_{max} 的所有单项式里，关于 $\prec$最大的单项式。类似地，设 w_{min}、w_{max} 是多项式 h 中分别对应于 b_{min} 和 b_{max} 的单项式。现在考虑单项式 $u = m_{max}w_{max}$。它在 $f = g.\mathrm{h}$ 中非零，且不平衡为 $a_{max} + b_{max}$。类似地，单项式 $v = m_{min}w_{min}$ 在 f 中非零，且不平衡为 $a_{min} + b_{min}$。由于 $f \in C \subset B$， f 的每个单项式的不平衡都为 0。因此， $a_{max} + b_{max} = 0$ 和 $a_{min} + b_{min} = 0$。于是 $a_{max} = -b_{max} \leq -b_{min} = a_{min}$，这意味着 $a_{min} = a_{max} = a$ 和 $b_{min} = b_{max} = -a$。因此， g 的所有单项式的不平衡均为 a，而 h 的所有单项式的不平衡均为 $-a$。

设 m 为 f的首项单项式。显然， m 是 f的一个最高次数单项式。此外，m 在 f的最高次数单项式中最大。设 $m = m_1m_2$ 满足 $m_1 \in \text{supp}(g)$ 且$m_2 \in \text{supp}(\mathrm{h})$。我们有 $i(m_1) = a$， $i(m_2) = -a$。由于 $f \in C$，将 m 中每个 x 都替换为 y，并将每个 y 替换为 x 所得的单项式 $\bar{m}$ 也属于 $\text{supp}(f)$。此外，$\bar{m}$ 是 f的最高次数单项式中最小的。这就意味着单项式 $\bar{m}_1$ （在 m_1中交换 x和 y 所得）属于 supp(g)。同理，单项式 $\bar{m}_2$（在 m_2中交换 x和 y所得）属于 supp(h)。我们有 $i(\bar{m}_1) = -a$ 且 $i(\bar{m}_2) = a$。现在， g 的所有单项式具有相同的不平衡，且 $m_1, \bar{m}_1 \in \text{supp}(g)$。这就意味着 $a = -a = 0$。因此，supp(g) ∪ supp(h) 中的所有单项式的不平衡均为零，这意味着 $g, \mathrm{h} \in B$。

由引理 2.3 应用于 g 和h，可得

1. $g = g$ - $_{-1} + g_2, h = h_1 + h2, g_1, h_1 \in C, \text{lm}(g_2)$ 包含 $\bar{u} \in T$， 且 $\text{lm}(h_2)$ 包含 $\bar{v} \in T$，

2. 因此，$\mathrm{lm}(g_2h_1)$ 的 $\deg(g_2)$ 前缀包含子词 $\bar{u}$，而 $\mathrm{lm}(g_1h_2)$ 的 $\deg(h_2)$ 后缀包含子词 $\bar{v}$。

3. 最后，g_2 的次数前缀和 $_2h$ 的次数后缀都包含子词 $\bar{u}$ 和 $_v$，它们均来自 $\mathrm{lm}(g_2 \cdot h_2)$。

因此，首项单项式 $\mathrm{lm}(g_2 \cdot h_1)$,$\mathrm{lm}(g_1 \cdot h_2)$ 和 $\mathrm{lm}(g_2 \cdot h_2)$ 彼此无法抵消。因此，$g_2 \cdot h_1 + g_1 \cdot h_2 + g_2 \cdot h_2$ 的首项单项式包含来自 T 的子词 $\bar{}$，除非 $g_2 = 0$ 和 $h_2 = 0$ 都成立。因此，

$$\begin{aligned} g_2 \cdot h_1 + g_1 \cdot h_2 + g_2 \cdot h_2 &= gh - g_1 \cdot h_1 \in C \text{ and} \\ f &= g \cdot h, g_1, h_1 \in C. \end{aligned}$$

根据引理 2.3，对于任意多项式 $\mathfrak{f} \in C$，其首项单项式 $\mathrm{lm}(\mathfrak{f})$ 都不能含有来自 T 的子词 $\bar{}$。这就迫使 $g_2 = 0$ 和 $h_2 = 0$，从而推出 $g, h \in C$。□

下面的定理是定理 2.5 的推论，它表明嵌入 φ 是一个 1-惰性嵌入（见定义 1.2）。也就是说，它保持因式分解。

定理 *2.6.* 设 $f \in \mathbb{F}\langle X\rangle$，其中 $X = \{x_1, \ldots, x_n\}$。假设 $f' = \varphi(f) = g' \cdot h'$ 是 $\varphi(f)$ 在环 $\mathbb{F}\langle x, y\rangle$ 中的一个非平凡因式分解。那么存在多项式 $g, h \in \mathbb{F}\langle X\rangle$, $g, h \notin \mathbb{F}$，使得 $g' = \varphi(g)$, $h' = \varphi(h)$ 且 $f = g \cdot h$。

证明. 根据构造，同态 φ 将 $\mathbb{F}\langle X_\infty\rangle$ 单射映射到 $\mathbb{F}\langle x, y\rangle$ 中。由于 $\mathbb{F}\langle X\rangle \subset \mathbb{F}\langle X_\infty\rangle$，$\varphi$ 将 $f \in \mathbb{F}\langle X\rangle$ 映射为某个 $f' = \varphi(f) \in C$。假设 $f' = g' \cdot h'$ 是 f' 在 $\mathbb{F}\langle x, y\rangle$ 中的一个非平凡因式分解。根据定理 2.5，$f' \in C$ 两个因子 $g', h' \in C$。由于 $g' \in C$，它是以下形式乘积的 $\mathbb{F}$-线性组合：$(u_{t_1} + \overline{u_{t_1}})(u_{t_2} + \overline{u_{t_2}}) \ldots (u_{t_\ell} + \overline{u_{t_\ell}})$。根据 φ 的定义，

$$(u_{t_1} + \overline{u_{t_1}})(u_{t_2} + \overline{u_{t_2}}) \ldots (u_{t_\ell} + \overline{u_{t_\ell}}) = \varphi(x_{t_1} x_{t_2} \ldots x_{t_\ell}).$$

因此，由线性性可知，对于某个非平凡多项式 $g \in \mathbb{F}\langle X_\infty\rangle$，有 $g' = \varphi(g)$；类似地，存在一个非平凡多项式 $h \in \mathbb{F}\langle X_\infty\rangle$，使得 $h' = \varphi(h)$。由于 φ 是同态，我们有

$$\varphi(f) = f' = g' \cdot h' = \varphi(g) \cdot \varphi(h) = \varphi(g \cdot h).$$

由于 φ 是单射，我们有 $f = g \cdot h$。为了完成证明，我们需要说明 $g, h \in \mathbb{F}\langle X\rangle$。令 $\mathrm{Var}(g)$ 表示变量集合 x_i，其中的变量出现在 g的某个非零单项式中。我们要证明 $\mathrm{Var}(g) \subseteq X$。假设 $\mathrm{Var}(g)$ 包含某个 $x_i \notin X$。在所有包含x_i的 g 单项式中，令 m 为最大单项式（按 $\prec$-序）。那么，单项式 $m \cdot \mathrm{lm}(h)$ 包含变量 x_i，并且在 $f = gh$ 中的系数非零。这与 $f \in \mathbb{F}\langle X\rangle$ 矛盾，因为 X 不包含 x_i。因此，$\mathrm{Var}(g) \subseteq X$。类似地，$\mathrm{Var}(h) \subseteq X$。□

3 多元到二元归约

本节将应用 Bergman 定理，证明多变量非交换多项式因式分解在白盒和黑盒两种情形下都可归约为二元非交换多项式因式分解。

我们首先介绍一些简单的工具，借助这些工具可以从 Bergman 定理（定理 2.5）得到一种高效的归约。

令 $X = \{x_1、\ x_2、\ \ldots\ldots、\ x_n\}$ 和 $v_1、\ v_2、\ \ldots\ldots、\ v_n$ 为 $\{x、\ y\}^*$ 中任意互不相同的极小平衡单项式。我们定义函数 $\varphi: \mathbb{F}\langle X\rangle \to \mathbb{F}\langle x、\ y\rangle$：

- $\varphi(x_i) = v_i + \overline{v_i}$ 对所有 i 均成立。
- φ 通过乘法扩展到单项式，即 $\varphi(x_{i_1} x_{i_2} \ldots\ldots x_{i_k}) = \prod_{j=1}^{k} \varphi(x_{i_j})$。
- φ 通过线性性扩展到 $\mathbb{F}\langle X\rangle$。

注 3.1. 上述定义与 *Bergman* 定理证明中的定义基本相同，不同之处在于，这里 X 是一个有限变量集，而 $v_i、\ 1 \le i \le n$ 是任意互不相同的极小平衡单项式。

沿着定理 2.5 和定理 2.6 的相同思路，我们可以证明以下结论。这个直接的证明方法是在定理 2.6 的证明中应用定理 2.5 之前和之后，适当地重命名变量 $x_1、\ \ldots\ldots、\ x_n$。

引理 *3.2.* 令 $X = \{x_1, \ldots, x_n\}$，$f \in \mathbb{F}\langle X\rangle$。假设 $v_1, v_2, \ldots, v_n$ 是 $\{x, y\}^*$ 中任意互不相同的极小平衡单项式。如果 $f' = \varphi(f) = g' \cdot h'$ 是 f' 在 $\mathbb{F}\langle x, y\rangle$ 中的非平凡因式分解，那么存在多项式 $g, h \in \mathbb{F}\langle X\rangle$，使得 $g' = \varphi(g), h' = \varphi(h)$ 且 $f = g \cdot h$。

为了得到多项式时间可计算归约，方便起见，可选择 $v_1, v_2, \ldots, v_n$，使每个 v_i 的长度都相同。下一个引理保证 $l = O(\log n)$ 就足够了。

引理 3.3. 在 $\{x, y\}^*$ 中，长度为 $2l$ 的极小平衡单项式至少有 n 个，其中 $for l \ge max(\lceil \log 4n \rceil, 7)$。此外，字典序最小的 n 个长度为$2l$ 的极小平衡单项式可在关于 n 的多项式时间内计算。

证明。 首先，我们考虑长度为 $2l$ 且$l \ge 2$的极小平衡单项式的数量。任意极小平衡单项式的第一个符号都是 x。若它大于 2，第二个符号也必定是 x（如果是 y，那么平衡单项式 xy 就会是该极小平衡单项式的真前缀，这与极小性矛盾。）我们考虑以下形式的单项式

$$v = xx \cdot w \cdot yy,$$

其中 w 是一个 Dyck 单项式[3]。也就是说，w 是一个平衡单项式，并且其每个前缀 w 中 y 的数量都不超过 x 的数量。注意，$w \in \{x,\ y\}^{2\ell-4}$。由此可知，$v$ 的任何非平凡前缀中，x 的数量都严格多于 y。因此，任何这样的单项式都是长度为 $2l$的极小平衡单项式。长度为 $2l-4$ 的 Dyck 单项式数量为 $C_{\ell-2}$（即 $(l-2)^{th}$ 卡特兰数）。利用标准估计可得

$$C_k \sim \frac{4^k}{k^{3/2}\sqrt{\pi}},$$

这意味着 C_k 是 $2^{\Omega(k)}$。具体而言，$C_k > 2^k$ 对于 $k \ge 5$。如果 $n < 2^{\ell-2}$ 且$l \ge 7$，那么至少有 n 个长度为 $2l$ 的极小平衡单项式，其中$l = \max(\lceil \log 4n \rceil, 7)$。

显然，我们可以通过枚举在 poly(n) 时间内计算 $v_i,\ 1 \le i \le n$。 □

[3]本质上是一个平衡括号串，其中 x 和 y 分别作为左括号和右括号

3.1 白盒归约

我们首先介绍输入多项式 $f \in \mathbb{F}\langle X\rangle$ 由非交换算术电路给出时，白盒情形下的归约。

引理 3.4。 设 $X = \{x_1, \ldots, x_n\}$ 和 $f \in \mathbb{F}\langle X\rangle$ 是由大小为 s 的算术电路 C 给出的非交换多项式。则存在一个确定性多项式时间算法，输出一个计算多项式 $\varphi(f) \in \mathbb{F}\langle x, y\rangle$ 的算术电路，其中定义映射 φ 的极小平衡单项式 $v_i, 1 \le i \le n$ 如引理 *3.3* 所述。

证明。 对于 $1 \le i \le n$，我们注意到，两个单项式 $v_i + \overline{v_i}$ 之和可以由大小为 $O(\log n)$ 的非交换算术公式 F_i 计算。令 C' 为从电路 C 得到的算术电路，其中将输入变量 x_i 替换为公式 F_i。显然， C' 计算 $\varphi(f)$，且其大小有多项式上界。□

引理 *3.5*。对于 $f \in \mathbb{F}\langle X\rangle$，假设 $\varphi(f) = f'1 \cdot f'2 \cdots f'r$ 是 $\varphi(f)$ 在 $\mathbb{F}\langle x, y\rangle$ 中分解为不可约因子 $f'_i \in \mathbb{F}\langle x, y\rangle$ 的完全因式分解。那么存在不可约多项式 $f_1, f_2, \ldots, f_r \in \mathbb{F}\langle X\rangle$，使得$f = f_1 f_2 \ldots f_r$，并且对于每个 i，都有 $\varphi(f_i) = f'_i$。

证明。 由反复应用引理 3.2 可知，若

$$\varphi(f) = f'_1 \cdot f'_2 \cdots f'_r,$$

是不可约因子的因式分解 $f'_i \in \mathbb{F}\langle x, y\rangle$，那么存在多项式 $f_1, f_2, \ldots\ldots, f_r \in \mathbb{F}\langle X\rangle$，使得 $f = f_1 f_2 \ldots\ldots f_r$ 且 $\varphi(f_i) = f'_i$ 对每个 i 都成立。我们断言，每个 f_i 都是不可约的。因为，若 $f_i = g \cdot h$ 是 f_i 在 $\mathbb{F}\langle X\rangle$ 中的非平凡因式分解，那么显然 $f'_i = \varphi(f_i) = \varphi(g)\varphi(h)$ 是 f'_i 的非平凡因式分解，这与其不可约性矛盾。□

设 C'_i 是一个大小为 s'_i、用于 f'_i 的算术电路，针对 $i \in [r]$。我们将为每个 $i \in [r]$ 高效地构造一个大小为$poly(s'_i, n)$、用于 f_i 的电路；这是我们多元到二元归约的关键部分。

下一个引理描述了白盒归约中的关键算法。

引理 3.6. 给定一个计算多项式 $\varphi(g) \in \mathbb{F}\langle x, y\rangle$的非交换算术电路 C，其中 $g \in \mathbb{F}\langle X\rangle$ 是次数为 d 的多项式， $X = \{x_1, x_2, \ldots, x_n\}$，存在一种确定性多项式时间算法，其运行时间为 $\mathrm{poly}(d, \mathrm{size}(C), n)$，可计算出一个计算多项式 g 的非交换算术电路 C'。此外，若 $\varphi(g)$ 由代数分支程序给出，则该算法会计算出一个计算 g 的代数分支程序。

证明。 证明基于这样一个想法：在一个自动机（具体而言，是一个代换自动机）上求值一个非交换算术电路；该自动机见 [4]（相关应用示例参见 [2],[3]）。

设 $g' = \varphi(g)$。设 $g = \sum_m \alpha_m m$，其中 $m \in X^*$，且 α_m 是 g中 m 的系数。如前所述，映射 φ 具有如下性质：对于 X^*中的单项式 $m \ne m'$，$\mathrm{Mon}(\varphi(m)) \cap \mathrm{Mon}(\varphi(m')) = \emptyset$。此外，如果 $m = x_{i_1} x_{i_2} \ldots x_{i_\ell}$ 在 g 中的系数 α_m 非零，那么 g' 就有一个系数为 α_m 的单项式 $m' = v_{i_1} v_{i_2} \ldots v_{i_\ell}$。因此，要从给定的、用于表示 g' 的电路 C' 中求得表示 g 的算术电路，我们的目标是对由电路 C'给出的多项式 g' 执行如下变换：

去掉 g' 中包含所有 $j \in [n]$ 的单项式，$\overline{v_j} \in T$ 适用于此情形。

- 对于每个剩余单项式 m'，在 m' 中每当出现单项式 v_i 作为子串时，就用 x_i 替换它，以得到 g'。

我们将通过在适当选取的矩阵代换 $x \leftarrow M_x$ 和 $y \leftarrow M_y$下求值电路 C' 来完成这一变换，其中 M_x 和 M_y 将是维数受多项式界定的 N阶矩阵。由此得到的求值结果 $C'(M_x, M_y)$ 将是一个 $N \times N$ 阶矩阵。该矩阵的一个指定条目将包含多项式 g。显然，如果我们能够高效计算所声称的矩阵 M_x 和 M_y，就能得到一个计算多项式 g的算术电路 C。这些矩阵 M_x和 M_y 将作为替换自动机的转移矩阵获得，该自动机将在多项式 g'上执行上述变换步骤。

我们回顾一下当前语境中的替换自动机。有限替换自动机 $\mathcal{A}$ 是一个确定性有限自动机 $\mathcal{A}$，并配有一个代换映射

$$\delta : Q \times \{x, y\} \to Q \times (X \cup \mathbb{F})$$

其中 Q是状态集合，而 $X = \{x_1, x_2, \ldots, x_n\}$ 是非交换变量。对于 i、$j \in Q$、$a \in \{x, y\}$、$u \in X \cup \mathbb{F}$，若 $\delta(i, a) = (j, u)$，这表示当自动机 $\mathcal{A}$处于状态 i并读取 a时，它将 a 替换为 u，并转移到状态 j。对于每个 $a \in \{x, y\}$，我们可以定义 $|Q| \times |Q|$ 转移矩阵 M_a，使得当且仅当 $\delta(i, a) = (j, u)$ 时，$M_a(i, j) = u$；否则为 0。

将 δ 与投影 $\delta_1 : Q \times \{x, y\} \to Q$ 以及 $\delta_2 : Q \times \{x, y\} \to X \cup \mathbb{F}$ 相关联，它们定义为 $\delta_1(i, a) = j$ 和 $\delta_2(i, a) = u$，若 $\delta(i, a) = (j, u)$。函数 δ_1 和 δ_2 自然地扩展到单项式：对于 $w \in \{x, y\}^*$，$\delta_1(i, w) = j$ 表示自动机 $\mathcal{A}$ 在读取w时从状态 i 转移到状态 j。令 $\tilde{w}_\ell$表示 w 长度为 ℓ 的前缀，w_ℓ表示从左数起 w的第 ℓ^{th} 个符号。$\delta_2(i, w) = p$ 表示

$$p = \prod_{\ell=0}^{|w|-1} \delta_2(\delta_1(i, \tilde{w}_\ell), w_{\ell+1}).$$

注意，$\delta_2(i, w)$具有 $\beta \cdot w'$的形式，其中 $\beta \in \mathbb{F}$，$w' \in X^*$。对于 $\alpha \in \mathbb{F}$，定义 $\delta_2(i, \alpha \cdot w)$ 为 $\alpha \cdot \delta_2(i, w)$。

令 $g'(x, y) = \sum_m \alpha_m m \in \mathbb{F}\langle x, y\rangle$。则，$s$，$t)^{th}$项是 $|Q| \times |Q|$矩阵 $g'(M_x, M_y)$ 的一个多项式 $g \in \mathbb{F}\langle X\rangle$，使得

$$g = \sum_{m \in W_t} \alpha_m \delta_2(s, m),$$

其中 W_t 是所有将自动机 $\mathcal{A}$ 从状态 s 带到状态 t的单项式的集合。

显然，如果 g' 具有大小为 s 的算术电路，那么我们就能在确定性时间 $\mathrm{poly}(s, n, |Q|)$ 内，为 g构造一个大小为 $\mathrm{poly}(s, n, |Q|)$ 的算术电路。

回到归约，考虑用于 $g' = \varphi(g) \in \mathbb{F}\langle x, y\rangle$ 的输入电路 C。我们将构造一个替换自动机 $\mathcal{A}$，使得多项式 g 是矩阵$g'(M_x, M_y)$ 的 $(s, t)^{th}$ 项。

替换自动机的描述如前所述，每个 v_i 都具有 xxw_iyy 的形式，其中 w_i 是一个 Dyck 单项式。令 $v'_i = xw_iy$，其中 $i \in [n]$。我们可以轻松地设计一个具有 $O(mn)$ 个状态的确定性有限自动机 A'，使得 A' 所接受的语言恰好是有限集 $\{v'_1, v'_2, \ldots\ldots, v'_n\}$，其中 m 是 v_i 的长度，其中 $i \in [n]$。令 δ' 表示转移函数，Q' 表示 A' 的状态集，其中 q_1 是初始状态，q_{f_i} 是与之关联的终态

对字符串 v_i'（其中 $i \in [n]$）的接受。A' 具有树结构，根节点为 q_1，叶节点为 q_{f_i}（其中 $i \in [n]$），且任意从根节点到叶节点的路径长度都恰好为 $2l - 2$。现在我们定义替换自动机 $\mathcal{A}$。其状态集为 $Q = Q' \cup \{q_0, q_f, q_r\}$。转移函数 δ：$Q \times \{x, y\} \to Q \times (X \cup \mathbb{F})$ 定义如下：

1. $\delta(q_0, x) = (q_1, 1)$；$\delta(q_0, y) = (q_r, 0)$。2. 对于 $q \in Q' \setminus \{q_{f_i} | 1 \le i \le n\}$。以及 $a \in \{x, y\}$，令 $\delta(q, a) = (\delta'(q, a), 1)$。3. $\delta(q_{f_i}, x) = (q_r, 0)$；对于每个 $i \in [n]$，$\delta(q_{f_i}, y) = (q_f, x_i)$。4. $\delta(q_f, x) = (q_1, 1)$，且 $\delta(q_f, y) = (q_r, 0)$。5. 对于 $a \in \{x, y\}$，$\delta(q_r, a) = (q_r, 0)$。

$\mathcal{A}$ 的终态是 q_f。对于单项式 $w \in \{x, y\}^*$，从状态 q_0 开始，只要自动机 $\mathcal{A}$ 与 v_i 的前缀匹配，就会将所有变量替换为 1，其中 $i \in [n]$ 由上文 1、2 中的转移给出。当单项式与某个 i 的 v_i 匹配时（读取符号 y 时就会发生这种情况，因为每个字符串 v_i 都以 y 结尾），$\mathcal{A}$ 会将 y 替换为 x_i，并转移到状态 q_f。如果读到的是 x 而不是 y，那么 $\mathcal{A}$ 就会进入拒绝状态 q_r（由上文 3 中的转移给出）。因此，如果 $\mathcal{A}$ 在 w 中找到子串 v_i，就会将其替换为 x_i。每当 $\mathcal{A}$ 处于状态 q_f 时，这意味着目前读到的单项式形式为 $v_{i_1} v_{i_2} \ldots\ldots v_{i_t}$，并且已将其替换为 $x_{i_1} x_{i_2} \ldots\ldots x_{i_t}$。如果处于状态 q_f 时遇到符号 y，这意味着下一个子串不可能与极小平衡单项式匹配（因为这类单项式以 x 开头），于是自动机转入拒绝状态 q_r。如果处于状态 q_f 时读到变量 x，自动机就会转移到状态 q_1，并重新开始搜索与某个 v_i 匹配的新子串（上文 4 中的转移）。

总之，$\mathcal{A}$ 将所有形如 $v_{i_1} v_{i_2} \ldots v_{i_t}$ 的单项式替换为 $x_{i_1} x_{i_2} \ldots x_{i_t}$。如果单项式中含有 v_i，或者它不是形如 $v_{i_1} v_{i_2} \ldots v_{i_t}$，那么 $\mathcal{A}$ 会通过恰当地将某个 y 置为零来消去该单项式，或者进入拒绝状态 q_r。[4]

因此，矩阵 $|Q| \times |Q|(M_x, M_y)$ 的 (q_0, q_f) 项是多项式 g，其中 $g' = \varphi(g)$ 和 M_x, M_y 是替换自动机 $\mathcal{A}$ 的转移矩阵。由此完成证明。

最后，如果 $\varphi(g)$ 由代数分支程序 P 给出，那么很容易看出，利用替换自动机 $\mathcal{A}$ 进行上述构造，可得到 $P(M_x, M_y)$，它是一个代数分支程序。□

本节的主要定理陈述如下，它总结了本节的讨论。

定理 3.7。在白盒设定下，将多元非交换多项式分解为不可约因子的因式分解问题，可在确定性多项式时间内归约到将二元非交换多项式分解为不可约因子的因式分解问题。更准确地说，给定由算术电路（分别地，代数分支程序）表示的 $f \in \mathbb{F}\langle X \rangle$ 作为输入，计算完全因式分解 $f = f_1 \cdot f_2 \cdots f_r$ 的问题（其中每个 f_i 都以算术电路（分别地，代数分支程序）的形式输出），可在确定性多项式时间内归约到对 $\mathbb{F}\langle x, y \rangle$ 中的二元多项式求解同一问题。

证明。我们描述该归约：

[4]我们可以省去拒绝状态 q_r，因为将 y 的某个出现恰当地设为 0 也足够。为便于说明，我们设置了通向拒绝状态 q_r 的转移。

1. 输入 $f \in \mathbb{F}\langle X\rangle$（以电路或代数分支程序表示）。 2. 根据引理 3.3 的算法，将 f转换为 $f' = \varphi(f) \in \mathbb{F}\langle x, y\rangle$ 的电路（分别为代数分支程序）。 3. 对 $f' = f'_1 \cdot f'_2 \cdots f'_r$ 计算完全因式分解，其中每个 $f'_i \in \mathbb{F}\langle x, y\rangle$ 都是不可约的，并以电路（分别为代数分支程序）的形式计算得到。 4. 应用引理 3.6 的算法，得到 $f = f_1 \cdot f_2 \cdots f_r$ 的完全因式分解，其中每个 f_i 都是不可约的，并以电路（分别为代数分支程序）的形式输出。

归约的正确性及其多项式时间界由引理 3.2、3.3 和 3.6 得出。□

注 3.8. 我们注意到，当 $\mathbb{F}$ 是域 $\mathbb{Q}$（有理数域）时，需要考虑所涉及有理数的位复杂度，并论证该归约仍可在多项式时间内计算。这里需要注意的要点是，该归约保证因子 f_i 的大小相对于 g_i、$1 \le i \le r$ 的大小呈多项式有界，其中 g_i 的大小包括算术电路（或代数分支程序）对 g_i 的描述中可能涉及的任何有理数的大小。

注 *3.9.* 我们在此指出，环 $\mathbb{F}\langle X\rangle$ 不是唯一分解整环。也就是说，多项式$f \in \mathbb{F}\langle X\rangle$ 通常可能有多个不可约因式分解 *[6]*。一个标准例子是多项式 $x + xyx$，它既可分解为 $x(1 + yx)$，也可分解为 $(1 + xy)x$，其中 x、y、$1 + yx$、$1 + xy$ 均不可约。由于映射 φ 是单射同态，$\varphi(f)$ 的因式分解与 f 的因式分解之间存在一一对应。更具体地说，我们的归约以任意一个完全因式分解$\varphi(f) = f'_1 f'_2 \ldots f'_r$ 为输入，并计算出 f 的相应完全因式分解 $f = f_1 f_2 \ldots f_r$。

注 3.10。 我们注意到，嵌入 φ 不会保留多项式 f的稀疏度[5]。更确切地说，如果 f这个 n元、次数为 d 的多项式的稀疏度为 s，那么二元多项式 $\varphi(f)$的稀疏度为 $O(2^d s)$。因此，利用这个嵌入映射，我们无法将稀疏 n元、次数为 d的多项式因式分解归约为稀疏二元多项式因式分解，其中 s、d 可以计入运行时间。这个问题仍未解决。

3.2 黑盒归约

黑盒情形下的归约基本相同。需要指出的一点是，引理 3.6 的对应结论在黑盒设置下成立，这一点很容易看出。我们在下面陈述该结论。先回顾一下非交换设置中的黑盒是什么意思。

定义 3.11。 一个通过黑盒 给出的非交换多项式 $f \in \mathbb{F}\langle X\rangle$，本质上意味着我们可以在任意矩阵代入 $x_i \leftarrow M_i$、$M_i \in \mathbb{F}^{N\times N}$处对 f 求值，而每次求值的代价为矩阵维数 N。

在黑盒设置中，假设我们有一个高效算法，可以对次数为 D 的多项式 $g \in \mathbb{F}\langle x, y\rangle$ 进行二元非交换多项式因式分解；该算法以 g 的黑盒作为输入，并在 poly(D) 时间内输出某个 g 因式分解中不可约因子的黑盒。于是，给定一个次数为 D n 的多元多项式 $f \in \mathbb{F}\langle X\rangle$ 的黑盒作为输入，我们要求该归约将其转换为二元多项式 $g \in \mathbb{F}\langle x, y\rangle$ 的黑盒，并且根据 g 的不可约因子的输出黑盒，归约必须能够高效地恢复 f 中对应不可约因子的黑盒。

[5]多项式 f 的稀疏度是 Mon(f) 中单项式的数量。

引理 3.12。 给定多项式 $\varphi(g) \in \mathbb{F}\{x, y\}$ 的黑盒作为输入，其中 $g \in \mathbb{F}\langle X\rangle$ 是次数为 d 的多项式， $X = \{x_1, x_2, \ldots, x_n\}$；通过在确定性多项式时间内计算针对 x 和 y 的矩阵代换，我们可以得到多项式 $g \in \mathbb{F}\langle X\rangle$ 的黑盒。

证明。 引理 3.6 的证明已蕴含了这一点，因为其中描述的矩阵 M_x 和 M_y 无需以白盒形式作为电路或代数分支程序给出 $\varphi(g)$。因此，通过访问矩阵输出 $\varphi(g)(M_x, M_y)$的 $(q_0, q_f)^{th}$ 项， $\varphi(g)$的黑盒即可得到 g的黑盒。□

因此，我们也在黑盒设置下得到了所述的从多变量因式分解到二元分解的归约。

定理 3.13。 对于由黑盒给出的 $f \in \mathbb{F}\langle X\rangle$ ，计算其完全因式分解的问题，可在确定性多项式时间内归约到黑盒计算 $\mathbb{F}\langle x, y\rangle$中多项式的完全因式分解问题。

证明。 给定 f的黑盒，应用引理 3.3 即可得到 $\varphi(f)$的黑盒。然后，给定一个完全因式分解

$$\varphi(f) = f_1' \cdot f_2' \cdots f_r',$$

其中每个因子 f_i' 均由其对应的黑盒输出，根据引理 3.12，我们可以得到每个 f_i的黑盒。由此得到 f的完全因式分解 $f = f_1 \cdot f_2 \cdots f_r$，其中各因子均由黑盒给出。□

4 在 $\mathbb{Q}$上对 4×4 线性矩阵进行因式分解

我们在第 3 节中证明，多变量非交换多项式因式分解可以高效地归约到二元情形。设 $f \in \mathbb{F}\langle x, y\rangle$是一个由大小为 s的公式给出的二元多项式。按照 [1], 中的做法应用 Higman 线性化 [6], ，我们可以将问题转化为对双变量线性矩阵 $A_0 + A_1 x + A_2 y$进行因式分解，其中矩阵的大小有 $2s$的上界。在 [1]中，当 $\mathbb{F}$ 是有限域时，给定公式的 n元多项式 $f \in \mathbb{F}\langle X\rangle$的因式分解问题分两步得到解决：
(i) 将 f 转化为线性矩阵 L ，并通过将其归约到公共不变子空间问题，将 L分解为不可约因子；
(ii) 从 L的因子中提取 f的因子。此方法不适用于 $\mathbb{F} = \mathbb{Q}$，因为 Ronyai [12] 证明，关于 $\mathbb{Q}$ 上矩阵的公共不变子空间问题至少与无平方因子整数的因式分解一样困难。

本节将说明，即使对于 4×4 双变量线性矩阵，其因式分解仍至少与分解无平方因子整数一样困难。因此，即使对于二元多项式，在 $\mathbb{Q}$ 上进行高效的多项式分解仍然遥不可及。证明基于 Ronyai 前述的结果。

定义 4.1 （广义四元数代数）。 设 $\alpha, \beta \in Q$ 是非零有理数。广义四元数代数 H（α, β）是由元素1、 u、 v、 uv 生成的有理数域上的四维代数，其中 H（α, β）中的乘法规则由 $u^2 = \alpha$、 $v^2 = \beta$和 $uv = -vu$给出。

域 $\mathbb{F}$ 上的单代数 $\mathcal{A}$ 是指没有非平凡双边理想的代数。代数 $\mathcal{A}$ 的中心C 是由 $\mathcal{A}$ 中所有与 $\mathcal{A}$的每个元素都可交换的元素构成的子代数。

Fac命题 4.2。 对于任意非零的 α、 $\beta \in \mathbb{Q}$，代数 $H(\alpha, \beta)$ 是一个中心为 $\mathbb{Q}$ 的单代数 .

此外，根据一般理论 [11, 第 1 章。6] 可知

事实 4.3。 代数 $H(\alpha,\beta)$要么是除代数（这意味着其中没有零因子），要么同构于 $\mathbb{Q}$ 上的 2×2 阶矩阵代数（这意味着它含有零因子）。

四维代数 $H(\alpha,\beta)$ 可以表示为一个由 4×4 上的矩阵构成的代数，这就是正则表示。容易看出，与 1 对应的矩阵是 I_4，而与 u 和 v 对应的矩阵 M_u 和 M_v 是

$$M_u = \begin{bmatrix} 0 & 1 & 0 & 0 \\ \alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & \alpha & 0 \end{bmatrix} \tag{2}$$

$$M_v = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ \beta & 0 & 0 & 0 \\ 0 & -\beta & 0 & 0 \end{bmatrix} \tag{3}$$

接下来我们注意到，因式分解 4×4 双变量线性矩阵至少与在广义四元数代数中寻找零因子一样困难。

定理 4.4。 在输入的四元数代数 $H(\alpha,\beta)$ 中寻找零因子，可多项式时间归约到因式分解 4×4 双变量线性矩阵 $A_0 + A_1x + A_2y$，其中每个数量矩阵 A_i 都属于 $\mathrm{M}_4(\mathbb{Q})$。

证明。 设 $H(\alpha,\beta)$ 为给定的广义四元数代数。那么

$$H(\alpha,\beta) = \{a_o + a_1u + a_2v + a_3uv \mid a_i \in \mathbb{Q}\},$$

其中 $u^2 = \alpha$、 $v^2 = \beta$ 和 $uv = -vu$ 定义了代数乘法。

众所周知（例如参见 Pierce 的著作 [11, 第 1 章。6]），代数 $H(\alpha,\beta)$ 是单 的（即，它没有非平凡的双边理想），其中心为 $\mathbb{Q}$。此外，它要么是一个除代数（这意味着其中没有零因子），要么同构于有理数域 $\mathbb{Q}$ 上的矩阵代数 $\mathrm{M}_2(\mathbb{Q})$，其中 2×2含有零因子。

现在我们来考察线性矩阵 4×4 $I_4 + M_ux + M_vy$ 的因式分解，其中矩阵 M_u和 M_v 由方程 2 和 3 定义。

断言。 线性矩阵 $I_4 + M_ux + M_vy$ 不可约，当且仅当四元数代数是除代数。

断言的证明 证。 假设线性矩阵 $L = I_4 + M_ux + M_vy$ 有一个非平凡的因式分解 n

$$L = I_4 + M_ux + M_vy = FG.$$

这意味着 F 和 G 都不是数量矩阵。根据 Cohn 定理 [6, 定理 5.8。8], , 存在可逆数量矩阵 P 和 Q，属于 $\mathrm{M}_4(\mathbb{Q})$，使得

$$PLQ = \begin{bmatrix} A & 0 \\ D & B \end{bmatrix}. \tag{4}$$

注 4.5。 要应用 *Cohn* 定理，我们需要矩阵 L 是首一的（也就是说，矩阵 $[M_u \mid M_v]$满行秩，矩阵 $[M_u^T \mid M_v^T]^T$ 满列秩）。由于 M_u 和 M_v 都是满秩矩阵，因此 L 具有首一性。

代入 $x = y = 0$，我们观察到

$$PQ = \begin{bmatrix} A_0 & 0 \\ D_0 & B_0 \end{bmatrix},$$

其中 A_0，B_0 和 D_0 是标量矩阵。由于 P 和 Q 可逆，因此 A_0 和B_0 均为可逆矩阵。于是我们有

$$PLP^{-1} = \begin{bmatrix} A & 0 \\ D & B \end{bmatrix} \cdot \begin{bmatrix} A_0 & 0 \\ D_0 & B_0 \end{bmatrix}^{-1} = \begin{bmatrix} A' & 0 \\ D' & B' \end{bmatrix},$$

其中 A'、B' 和 D' 也都是线性矩阵。现在回顾一下，矩阵 I_4、M_u 和 M_v是元素 1、u、$v \in H(\alpha, \beta)$ 关于基 $\{1, u, v, uv\}$ 的矩阵表示，而 $H(\alpha, \beta)$ 是该基。将 P 视为基变换矩阵，上述等式给出了 $H(\alpha, \beta)$ 的一个新基 $\{w_1, w_2, w_3, w_4\}$。令 $\dim(A') = k$。则 $1 \le \dim(A') \le 3$，且向量 w_1、……、w_k张成一个 k 维子空间 $W \subset H(\alpha, \beta)$，它是矩阵$I_4$、$M_u$、$M_v$ 和 M_{uv}的公共不变子空间。换言之，子空间 W 在 u和 v的左乘作用下保持不变。不失一般性，我们可以假设 $w_1 \neq 1$: 若 $k > 1$，显然可以作此假设。若 $k = 1$，注意到 $w_1 = 1$ 不可能，因为子空间 W 在 u 或 v的左乘作用下并不保持不变。于是四个元素 w_1、uw_1、vw_1、uvw_1 全都属于 W，因此它们线性相关。于是存在某个非平凡线性组合

$$\gamma_0 w_1 + \gamma_1 u w_1 + \gamma_2 v w_1 + \gamma_3 u v w_1 = 0.$$

which 表示 $(\gamma_0 + \gamma_1 u + \gamma_2 v + \gamma_3 uv) \times w_1 = 0$。因此，$w_1$ 是 $H(\alpha, \beta$ 中的零因子).

反过来，如果 $z \in H(\alpha, \beta)$ 是零因子，那么我们可以看出左理想

$$J = \{xz \mid x \in H(\alpha, \beta)\}$$

是 $H(\alpha, \beta)$ 的真子空间，且在 M_u 和 M_v作用下保持不变。然后，应用 Cohn 定理[6, 定理 5.8.8]，，我们可以得到可逆数量矩阵 P 和 Q，使得方程 4 成立，从而得到因式分解

$$PLQ = \begin{bmatrix} A & 0 \\ D & B \end{bmatrix} = \begin{bmatrix} A & 0 \\ 0 & I \end{bmatrix} \cdot \begin{bmatrix} I & 0 \\ D & I \end{bmatrix} \cdot \begin{bmatrix} I & 0 \\ 0 & B \end{bmatrix}.$$

■

为完成归约，请注意，若 $I_4 + M_u x + M_v y$不可约，则 $H(\alpha, \beta)$ 是一个除代数。另一方面，若给定一个非平凡因式分解 $I_4 + M_u x + M_v y = FG$，那么通过分析 Cohn 定理 [6, 定理 5.8.8] 的证明（详情另见 [1]），利用适当的行变换和列变换，我们可以在多项式时间内根据因子 F 和 G计算出可逆数量矩阵 P 和Q。因此，根据上述断言的证明，我们可以高效地计算出 $H(\alpha, \beta)$ 中的一个零因子 w_1。□

由于已知在四元数代数 $H(\alpha, \beta)$ 中寻找零因子至少与无平方因子整数分解 [12] 一样困难，因此我们得到以下结论。

推论 4.6。 对 $\mathbb{Q}$ 上的 4×4 双变量线性矩阵进行因式分解，至少与对无平方因子整数进行因式分解一样困难。

5 在 $\mathbb{Q}$ 上对 3×3 线性矩阵进行因式分解

本节介绍一种确定性多项式时间算法，用于对 $\mathbb{Q}$ 上的 3×3 多变量线性矩阵进行因式分解。我们先从一个关于一般线性矩阵因式分解的简单观察开始。

引理 5.1。 假设 $L = I_d + \sum_{i=1}^{n} A_i x_i$ 是一个线性矩阵，其中每个 A_i、$0 \le i \le d$ 都是 $\mathbb{Q}$ 上的一个 $d\times d$ 矩阵。那么，如果对于任意 i，A_i 的特征多项式在 $\mathbb{Q}$ 上不可约，则 L 不可约。

证明。 因为如果 L 可约，那么存在一个可逆数量矩阵 P，使得 t

$$PLP^{-1} = \begin{bmatrix} A & 0 \\ D & B \end{bmatrix},$$

这意味着

$$PA_iP^{-1} = \begin{bmatrix} A_i' & 0 \\ D_i' & B_i' \end{bmatrix},$$

对于数量矩阵 A_i', B_i' 和 D_i'。因此，A_i 的特征多项式是 A_i' 和 B_i' 的特征多项式之积，从而构成非平凡因式分解。□

定理 5.2。 存在一种确定性多项式时间算法，可对 $\mathbb{Q}$ 上的 3×3 多元线性矩阵进行因式分解。

证明。我们首先考虑形式为 $L = I_3 + \sum_{i=1}^{n} A_i x_i$ 的线性矩阵，其中每个 $A_i \in \mathrm{M}_3(\mathbb{Q})$，且 x_i 是非交换变量。该算法计算出 L 的完全因式分解，将其分解为（至多三个）不可约线性矩阵因子。根据 Cohn 定理 [6, 定理 5.8.8], 要么是不可约的，要么存在一个可逆数量矩阵 P，使得

$$PLP^{-1} = \begin{bmatrix} A & 0 \\ D & B \end{bmatrix}.$$

要么 A，要么 B 是一个数量矩阵。如果 A 是一个数量矩阵，那么与之对应的矩阵 A_i，$1 \le i \le n$ 存在一个由某个向量（例如 v）张成的一维公共不变子空间。更准确地说，行向量 v^T 是每个矩阵 A_i 的特征向量，并且 $v^T A_i = \lambda_i v^T$，其中 $\lambda_i \in \mathbb{Q}$ 是矩阵 A_i 对每个 i 所对应的特征值。同样，如果 B 是一个数量矩阵，那么相应地存在一个由（列）向量 u 张成的一维公共不变子空间，使得 $A_i u = \mu_i u$，其中 μ_i 是 A_i 的特征值。在这两种情况下，都可以通过特征多项式（例如 A_1 的特征多项式）轻松求得公共特征子空间，然后验证它对于其余的 A_i 也成立。由此可得因式分解

$$PLP^{-1} = \begin{bmatrix} A & 0 \\ 0 & I \end{bmatrix} \cdot \begin{bmatrix} I & 0 \\ D & I \end{bmatrix} \cdot \begin{bmatrix} I & 0 \\ 0 & B \end{bmatrix},$$

其中 B 是一个 2×2 线性矩阵。现在问题归结为对线性矩阵 $B = I_2 + \sum_{i=1}^{n} B_i x_i$ 进行因式分解，其中 $B_i \in \mathrm{M}_2(\mathbb{Q})$。下面讨论的一个单情形分析给出了对 B 进行因式分解的多项式时间算法。

1. 如果任意 B_i 的特征多项式在 $\mathbb{Q}$ 上不可约，那么线性矩阵 B 显然不可约。

2. 某个 B_i 有两个不同的特征值 $\lambda \neq \lambda' \in \mathbb{Q}$，那么对应的特征子空间是一维的，分别由其特征向量 $u \neq u'$张成。于是，对于每个 B_j， u 或 u' 必定是一个特征向量（否则 B 不可约），此时我们就得到了B的一个因式分解。

3. 假设每个 B_i 只有一个特征值 λ_i。那么，根据线性代数，经过基变换 B_i可化为以下形式

$$\begin{bmatrix} \lambda_i & 1 \\ 0 & \lambda_i \end{bmatrix}$$

在这种情况下，特征空间为 1 维，其特征向量为 $(10)^T$。我们可以像之前一样，检查该特征空间对每个 B_j 是否不变。否则，经过基变换，每个

$$B_i = \begin{bmatrix} \lambda_i & \\ 0 & \lambda_i \end{bmatrix}$$

这意味着对于每个 i 都有 $B_i = \lambda_i I_2$，而 B 的因式分解为

$$B = \begin{bmatrix} 1 + \sum_{i=1}^{n} \lambda_i x_i & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 + \sum_{i=1}^{n} \lambda_i x_i \end{bmatrix}$$

□

参考文献

[1] Vikraman Arvind 和 Pushkar S. Joglekar。通过 Higman 线性化高效地对非交换多项式进行因式分解。载于 Shachar Lovett（编），第 *37* 届计算复杂性会议（*CCC 2022*），*2022* 年 *7* 月 *20–23* 日，美国宾夕法尼亚州费城，第 234 卷，*LIPIcs*，第 12:1–12:22 页。Schloss Dagstuhl - Leibniz-Zentrum für Informatik，2022 年。

[2] Vikraman Arvind、Pushkar S. Joglekar、Partha Mukhopadhyay 和 S. Raja。非交换电路的随机多项式时间恒等性测试。载于第 *49* 届 *ACM SIGACT* 计算理论研讨会论文集（*STOC 2017*），*2017* 年 *6* 月 *19–23* 日，加拿大魁北克省蒙特利尔，第 831–841 页，2017 年。

[3] Vikraman Arvind、Partha Mukhopadhyay 和 Srikanth Srinivasan。关于非交换与交换多项式恒等性测试的新结果。*Comput.Complex.*，19(4)：521–558，2010。

[4] Vikraman Arvind、Gaurav Rattan 和 Pushkar S. Joglekar。关于非交换多项式分解的复杂性。载于计算机科学数学基础 *2015*——第 *40* 届国际研讨会，*MFCS 2015*，意大利米兰，*2015* 年 *8* 月 *24* 日至 *28* 日，会议论文集，第二部分，第 38–49 页，2015 年。

[5] P. M. Cohn。自由环及其关系。伦敦数学学会专著。Academic Press，1985 年。

[6] P. M. Cohn。《自由理想环与一般环中的局部化》。新数学专著。剑桥大学出版社，2006年。

[7] Ankit Garg、Leonid Gurvits、Rafael Mendes de Oliveira 和 Avi Wigderson。算子缩放：理论与应用。*Found. Comput. Math.*，20(2):223–290，2020年。[8] Graham Higman。群环的单位元。伦敦数学会会刊，s2-46(1):231–248，1940年。[9] Erich Kaltofen。由直线程序给出的多项式的因式分解。*Adv. Comput.Res.*，5:375–412，1989年。[10] Erich Kaltofen 和 Barry M. Trager。利用多项式求值的黑箱进行计算：最大公因式、因式分解以及分子与分母的分离。*J. Symb. Comput.*，9(3):301–320，1990年。[11] Richard S. Pierce。《结合代数》。数学研究生教材。施普林格，1982年。[12] Lajos Rónyai。单代数难以处理。载于 Alfred V. Aho（编），第*19*届年度*ACM*计算理论研讨会论文集，*1987*年，纽约，美国纽约州，第398–408页。ACM，1987年。