arXiv:2302.08891v1 [cs.SC] 17 Feb 2023

有限域上的消去理想与二元结式

Gilles Villard

法国国家科学研究中心、里昂大学、法国国家信息与自动化研究所、里昂高等师范学院、里昂第一大学、LIP实验室 UMR5668，法国

摘要。本文提出一种新算法，用于计算与两个多项式 a 和 b 相关的 Sylvester 矩阵（关于 x 或 y）的最高次数不变因子，其中 a 和 b 属于 $\mathbb{F}_q$[x,y]，且没有非平凡公因子。该算法采用蒙特卡洛型随机化方法，所需位操作次数为 $O((de)^{1+\epsilon}\log(q)^{1+o(1)})$，其中 d 和 e 分别界定输入多项式关于 x 和 y 的次数。因此，以下计算也具有相同的复杂度估计：当多项式系统 a = b = 0 没有无穷远根时，计算消去理想 ⟨a,b⟩ ∩ $\mathbb{F}_q$[x]（或 $\mathbb{F}_q$[y]）的一个生成元；当 a 和 b 足够一般，尤其是 Sylvester 矩阵只有一个非平凡不变因子时，计算 a 和 b 的结式。我们的方法将该问题归约为在商代数 $\mathbb{F}_q$[x,y]/⟨a,b⟩中求最小多项式的问题。通过提出一种基于结构化多项式矩阵除法的新方法来处理商代数中的元素，我们得以改进目前已知的最佳复杂度界。

1 引言

给定两个多项式 a、$b \in \mathbb{K}[x, y]$, 其中 $\mathbb{K}$ 是交换域，它们关于 y(a,b) 的结式 Res 是相应 Sylvester 矩阵 y 的行列式 S_y 在 $\mathbb{K}[x]$ [22，上的第 6]。一般情况下，按照输入 / 输出规模以准线性时间计算该行列式仍超出我们的能力范围。/。

本文考虑一个较宽松的问题：在有限域 $\mathbb{K} = \mathbb{F}_q$（含有 q 个元素）上，计算S_y的最后一个（次数最高的）不变因子。我们考虑a 和b 关于x的次数至多为d，关于y的次数至多为e，且属于 $\mathbb{F}_q[x, y]$, ，并且没有非平凡公因子。对于任意 $\epsilon > 0$，存在一种随机蒙特卡洛算法，可通过准线性数量的$O((de)^{1+\epsilon}\log(q)^{1+o(1)})$ 次位操作解决该问题。

S 的最后一个不变因子$_y$ 是结式的一个特定因子。如果多项式系统$a = b = 0$ 相对于y（y-首项系数是a 和b 互素），则它给出关于仿射解的核心信息。事实上，它是消去理想 $\langle a, b\rangle \cap \mathbb{K}[x]$ [16, 第 2]的一个生成元。特别地，我们还知道，当a 和b 足够一般时（第7节），这个不变因子就是结式。（一般性是在 Zariski 意义下考虑的：如果某个性质在参数空间的一个超曲面之外都成立，则称该性质具有一般性。）

我们在有限域上的方法受到以下工作的启发，并在此基础上更进一步：Poteaux 和 Schost 针对三角集和根理想提出的变序算法 [53]；van der Hoeven 和 Lecerf 提出的算法，该算法按照总次数计算一般多项式的结式 [28]。在二元情形下，这两项工作首次以关于输入/输出规模的期望准线性时间给出了解法（[53]处理一般多元情形）。它们属于同一条漫长的研究脉络，旨在将消元问题归约为线性代数 [42；16，第 2.4 和 3 节。6], ，尤其是归约为商代数中最小多项式的计算 [44, 59]。我们所沿的正是这条道路。

最小多项式的作用。令 I = ⟨a, b⟩ 为由 a 和 b 在 $\mathbb{K}$[x, y], 中生成的（零维）理想，并令$\mathbb{A}$ = $\mathbb{K}$[x, y]/I 为关联商代数。我们在第 2 节中指出，在不存在无穷远根 [43]的条件下，Sylvester 矩阵 S$_y$ 的最后一个不变因子可计算为商代数 $\mathbb{A}$中乘以 x 的乘法的最小多项式 μ。我们采用的正是这种方法。稍作修改后的多项式满足无穷远处行为的条件，因此仍可用于计算目标不变因子（第 5 节）。

为了提高效率，最小多项式问题本身被归约为幂投影问题 [35, 见第 6] （更完整的参考文献列表将在本引言后面给出）。给定 ℓ 中对偶空间里的一个线性形式 $\mathbb{A}$ 在 $\mathbb{K}$上， $\mathbb{A}$ 中的最小多项式可计算为线性生成序列 $\{\ell(x^i \bmod I)\}_{i\geq 0}$ 在 $\mathbb{K}$上的最小多项式。应用随机线性形式会保留 $\mathbb{A}$ [64] （第6节）中所寻求的递推关系。正如 Shoup [57], 所观察到的，幂投影问题与模合成问题互为对偶 [11]。我们最终依赖于 Kedlaya

以及 Umans的方法来处理后两个问题 [40]，并在有限域上以准线性时间完成。正如我们即将看到的，这得益于我们为模理想上的算术运算提出的一种新算法。

第一个结果。 上述策略的瓶颈之一是在 $\mathbb{A}$ [25] 中执行算术运算，即使只需计算两个多项式的乘法，或计算需要对理想 I 取模的 x 的幂。在这里，我们的贡献主要体现于此。在 [53], 中考虑了三角集这一特殊情形。也就是说，在我们的语境中，a 或 b 中至少有一个是单变量多项式。另一方面， [53] 的一般结式算法依赖于 Gr¨obner 基技术，以及对 I 取模的 [26] 标准形算法。

相反，我们使用多项式矩阵除法 [32, 第 6 节3]。将 $\mathbb{K}[x, y]$ 中的多项式 f 看作一个元素属于 $\mathbb{K}[x]$, 的向量，我们通过 Sylvester 矩阵 S_y 进行除法来降低其 x 次数；还需指出，如果维数不匹配，我们可能需要根据 a 和 b 的倍数构造一个 Sylvester 矩阵（第 3 节）。根据 Sylvester 矩阵的定义，该除法所得的余式给出了陪集 f +I 中的一个新多项式。交换 x 与 y 的角色后进行类似的除法，便得到一个对 I 取模的标准形算法，但需要满足一个与无穷远根有关的正则性假设（引理 2.3 和命题 3.1）。该算法对任意域都是代数的˜且确定性的。如果 f 的 x 次数至多为 δ、y 次数至多为 η, 则该算法使用 $O((d+\delta)(e+\eta))$ 次算术运算（命题 3.1）。Sylvester 矩阵是一种类托普利兹矩阵 [6]。我们的成本界基于快速结构化矩阵运算，相关内容将在第3.1节讨论。特别地，当 a 和 b 的首项系数足够一般时，标准形算法允许在 $\mathbb{K}[x, y]/\langle a, b\rangle$ 中进行乘法，仅需 O(de) 次运算（引理 2.3）。对于总次数情形，对于满足 deg a ≥ deg b 的一般多项式 a、b，在预先计算理想的简洁 Gr¨obner 基表示后，该算法 [26] 的代价为˜O((deg a)(deg b))；预计算使用 ˜O((deg a)^2) 次运算。因此，就各自的假设而言，这两种算法是互补的（第3.3节）。

将 Kedlaya 和 Umans 的技术推广到幂投影。一旦标准形算法可用，也就是说，能够在 $\mathbb{A}$ 中进行算术运算，就可以采用 Shoup [57, 59] 提出的通用策略来计算模幂投影，并通过对偶性将其与 Kedlaya 和 Umans 用于模复合的算法 [40] 结合起来（后者处理的是 $\mathbb{F}_q[x]$ 中的一元理想 I）。这一方法已在 [53] 和 [28], 中推广，所采用的理想 I 的形状分别如上所述。我们沿用同样的思路，将新的除法算法纳入这一整体流程：（i）将 $f \in \mathbb{F}_q[x]$ 对 I 取模，这可视为根据 f(g(x)) mod I 进行模复合，其中 g = x；模复合依赖于多元多点求值，参见 [40, 定理 3.1]；（ii）利用转置原理 [12, 定理 13.20],得到幂投影（第 3.4 节）。由于 a 和 b 关于 y 的结式次数至多为 2de，因此只需能够计算（i）当 deg f < 4de 时的 f 模 I，以及（ii）$\{\ell(x^i \bmod I)\}_{0\le i<4de}$，即可推出该数列的最小多项式（它是结式的一个因子）。我们将在第 4 节证明，使用位操作，在有限域上可以在目标成本范围内完成（i）和（ii）。

最后一个不变因子与消去理想 $\langle a, b\rangle \cap \mathbb{F}_q[x]$。存在无穷远根时，我们会随机变换 a 和 b，得到另外两个多项式；这两个多项式满足计算标准形所需的正则性条件，同时仍可用于求得原来的最后一个不变因子。第 5 节将介绍这一方法。第 6 节将根据模幂投影的复杂度界，给出计算最后一个不变因子的一般复杂度界。根据 Lazard 关于二元理想的结构定理 [43], , 后一个多项式是乘以 x 在 $\mathbb{A}$ 中的最小多项式 μ 的倍数；若系统 a = b = 0 没有无穷远根，则这两个多项式相同（引理 2.1）。在此条件下，至此所做的工作使我们能够在第 7 节计算 μ，也就是消去理想 $I \cap \mathbb{F}_q[x]$ 的一个生成元。

与以往工作的比较。给定任意一个域，二元结式可以通过 $O(de^2)$ 次算术运算计算得到 [22, 第 11]章。

在有限域上， [28] 的方法可实现准线性比特复杂度；对于关于总次数的一般多项式，以及任意 $\epsilon > 0$, 这给出了复杂度界 $O(((\deg a)(\deg b)\log q)^{1+\epsilon}) + \tilde{O}((\deg a)^2 \log q)$, 其中 deg a ≥ deg b。（软 O 记号 $\tilde{O}(c)$ 表示一个额外的对数因子 $O(c\log^k c)$, 其中 k 为正数。）我们的算法尤其涵盖了这种情况。一般性保证不存在无穷远根，且只有一个不变因子（见第 7 节），因此我们得到了可比的渐近界。通过分别考虑各变量的次数条件，我们可以处理更广泛的问题，且所需假设更弱。对于 x 次数为 d、y 次数为 e 的多项式，当 Sylvester 矩阵 S_y 具有唯一的非平凡不变因子时，我们可以在准线性时间内计算结式。

现在，概括而言，在所有情况下，只要不存在无穷远根，我们的方法就能计算消去理想的一个生成元 $I \cap \mathbb{F}_q[x]$。这将在第 7 节中讨论。据我们所知，在相同假设下，此前没有任何方法能在有限域上达到准线性复杂度。这个问题的复杂度确实与结式和双变量字典序 Gr¨obner 基的复杂度相关 [17]。特别是，对于 a 和 b 的总次数至多为 d，我们得到界 $O(d^{2+\epsilon}\log(q)^{1+o(1)})$，而此前的估计为 $\tilde{O}(d^3\log q)$ [45]。

我们采用位复杂度。使用代数计算模型求解二元结式问题是一个更困难的问题。据我们所知，目前还无法达到准线性复杂度界。我们可以参考 [46； 63, 52]以及其中找到的相关指引。还需要指出的是， [47]中针对具有整数系数的二元多项式系统给出了准线性时间算法。

最小多项式与幂投影。我们在此给出一些其他参考文献，我们所采用的结果主要继承自这些文献。将数值矩阵方法应用于有限域环境，最初是为了解决稀疏线性系统这一问题 [13, 64]。这些方法通过对相关矩阵的幂进行投影来计算其最小多项式，Wiedemann 方法 [64]便证明了这一点。这里需要联系的是：利用迹映射 [61, 54] 以及一般投影 [57, 39, 59]，通过幂投影计算商代数中的最小多项式。（实际上，我们在商代数中有一个乘法自同态。）

在 [57] 中，我们观察到幂投影问题与模复合问题之间的对偶性。

在多项式系统求解的背景下，相关文献十分丰富。我们可以参考 [1, 55, 24]，中迹映射的应用，或 [10] 中任意线性形式的应用。 [48] 将结构化矩阵和对偶性应用于多元多项式问题。 [59, 35]，研究了多元幂投影，尤其关注最小多项式； [8], 则利用这些方法计算特殊结式， [51] 将其用于三角集的变量顺序变换。通过在 [19, 18]，中对乘法矩阵进行幂投影，换序与线性代数之间的联系也能发挥作用；尤其是，这有助于利用稀疏性 [20], ，进而回到 Wiedemann 算法。

按照 [43], ，Sylvester 矩阵 S_y （或 S_x）是一个多项式矩阵，我们将其作为多项式矩阵来处理。这可以理解为在一个 $\mathbb{K}[y]$-模中运算，而非在一个 $\mathbb{K}$-向量空间中运算，以表示商代数 $\mathbb{A}$ [31,第 3 节。10], 并实现其元素上的运算。 [4] 也采用了类似思路，用于 Gröbner 基算法的换序。

在线性代数中，对于隐式表示矩阵，一个尚未解决的问题是：能否用与计算最小多项式基本相同的时间计算特征多项式 [Sec. 3][35]。这尤其适用于稀疏矩阵或结构化矩阵。用与计算 Sylvester 矩阵的最后一个不变因子基本相同的时间计算二元结式，这个问题似乎与 Kaltofen 尚未解决的问题类似。

计算模型。多项式 $\mathbb{K}[x、y]$ 模 $\langle a、b\rangle$ 及其转置的标准形算法，采用代数模型（第 3 节）来描述，例如使用计算树 [12, 第4节。4]。复杂度界对应于在 $\mathbb{K}$ 中执行的算术运算次数。

第 4 节中 Kedlaya 和 Uman 技术的应用，以及第 6 节中最后一个不变因子的计算，均依赖于 RAM 位复杂度模型。我们认为，在 $\mathbb{F}_q$ 中，算术运算可在$\tilde{O}(\log q)$ 时间内完成，并且 RAM 能以相同的代价生成一个在 $\mathbb{F}_q$ 中均匀分布的随机元素。

记号。本文中，我们考虑两个多项式 $a,b \in \mathbb{K}[x,y]$, ，它们关于 x 的次数分别为 d_a 和 d_b ，关于 y 的次数分别为 e_a 和 e_b。我们使用记号 $d = \max\{d_a,d_b\}$ 和 $e = \max\{e_a,e_b\}$。关于 x 和 y 的相应西尔维斯特矩阵分别为 $S_x \in \mathbb{K}[y]^{n_x\times n_x}$ 和 $S_y \in \mathbb{K}[x]^{n_y\times n_y}$，其维数分别为 $n_x = d_a + d_b$ 和 $n_y = e_a + e_b$。a 和 b 关于 x 和 y 的结式 $\mathrm{Res}_x(a, b) \in \mathbb{K}[y]$ 和 $\mathrm{Res}_y(a, b) \in \mathbb{K}[x]$, ，分别是 S_x 和 S_y [22, Chap. 6] 的行列式。我们假设 a 和 b 没有非平凡公因子，因此 S_x 和 S_y 均为非奇异矩阵。我们重点研究与 $\mathrm{Res}_y(a,b) = \det S_y$ 有关的计算（若研究 $\mathrm{Res}_x(a, b)$，结论也不会改变）。

我们使用“x次”或“y首项系数”等表述来指明所涉及的变量；涉及二元多项式时，则在公式中使用 $\deg_x$ 和 $\deg_y$。例如， $\mathbb{K}[x,y]_{<(d,n_y)}$ 中的下标表示x 和y的次数界，而 $\mathbb{K}[x]^{n\times d}$ 表示次数为d的多项式集合。

我们经常需要处理多项式的反转。对于 $k \geq 0$，我们将多项式 $f \in \mathbb{K}[x]$ 关于 k 的反转定义为 $\mathrm{rev}_k(f) = x^k f(1/x)$；默认情况下，如果未指定 k，则反转是相对于该多项式的次数进行的。对于多项式矩阵，这一定义推广为将其视为矩阵多项式，即系数为矩阵的多项式。

$\mathbb{K}[x、y]$ 中的多项式与其系数的（列）向量相对应，所使用的维数将由上下文明确。例如，给定 $f = f_0(x) + f_1(x)y + \ldots f_d(x)y^d$ 以及 $n \geq d+1$，$v_y(f) \in \mathbb{K}[x]^n$ 表示向量 $[0 \ldots 0\, f_d \ldots f_0]^\mathsf{T}$。

2 多项式矩阵、结式与双变量理想

我们将介绍本文后续部分所需的基本概念和结果，探讨两个多项式的结式与它们生成的理想之间的关系。作为一元多项式矩阵，西尔维斯特矩阵 S_y 幺模等价于一个对角矩阵 $\mathrm{diag}(s_1, \ldots, s_n) \in \mathbb{K}[x]^{n_y \times n_y}$ 的史密斯标准形，其中 s_n 是次数最大的那个不变因子。我们无法始终在目标成本范围内计算结式。不过，我们能够计算最后一个不变因子（推论 6.1）。

利用有限生成模的结构理论，可以将这个最后一个不变因子视为有限维 $\mathbb{K}$-向量空间 [31, 第3节。10]上的线性变换的最小多项式。这种形式化方法偶尔被用于高效计算一般矩阵的标准形 [62, 60]。关于西尔维斯特矩阵，并在更广泛的多项式系统求解背景下，这与在商代数上使用乘法映射有关 [42]。

设 $I = \langle a, b\rangle$ 为由 a 和 b 在 $\mathbb{K}[x,y]$, 中生成的（零维）理想，而 $\mathbb{A} = \mathbb{K}[x,y]/I$ 为相应的商代数。我们尤其依赖以下结果，它们是 Lazard 定理 [43]的直接推论。

引理 2.1 ([43, 定理 4]). S_y 的最后一个不变因子是乘以 x 在 $\mathbb{A}$中的乘法所对应的最小多项式的倍数；若 a 和 b 关于 y 的首项系数在 $\mathbb{K}[x]$ 中互素，则这两个多项式相同。

证明。 最后一个不变因子是埃尔米特标准形的最后一个对角项 $h \in \mathbb{K}[x]$ 的倍数；该标准形为下三角形，并通过幺模列变换得到。多项式 h 属于 $I \cap \mathbb{K}[x]$ （S_y 的列的线性组合可视为 a 和 b的线性组合），由此得到第一个断言。当首项系数互素时， [43, 定理 4] 中的整除性质 (i) 表明，可以通过幺模（行）变换将S_y 的埃尔米特标准形化为 Smith 标准形，且不改变对角线。根据 [43, 定理 4], 中的 (ii)，最后一个不变因子因此是 I 的一个约化 Gr¨obner 基元素；作为 $\mathbb{K}[x]$ 的多项式，它生成消去理想 $I \cap \mathbb{K}[x]$。□

引理 2.1 中对 a 和 a 与 b 的首项系数所作的2.1系统$a = b = 0$ 相对于y没有无穷远根ffi，其条件的依据是 [16, 第 3]。一般而言，结式和最后一个不变因子可能同时包含来自仿射簇和无穷远处行为的项2.1 。若要仍能将不变因子计算化为最小多项式问题，则对输入多项式进行随机修改后，引理5）中的假设仍然成立（见第

特别是，当 2.1 的 Smith 标准形中只有一个非平凡不变因子，且没有无穷远根时，可以根据引理S_y 推导出结式。这对应于理想I 具有形状基 [23, 2]的某些情形。

引理 2.2（[43, 定理 4]）。关于 y 的首项系数ffi数 a 和 b 在 $\mathbb{K}[x]$ 中互素，并且存在两个多项式μ， $\lambda \in \mathbb{K}[x]$，使得 $I = \langle \mu(x),\ y - \lambda(x)\rangle$ 当且仅当，除去 $\mathbb{K}$ 中的一个非零元素因子后，结式 $res_y(a,\ b)$ 是 $\mathbb{A}$ 中乘以 x 的最小多项式μ。

证明。 根据 [43, 定理 4],，在假设 $I = \langle \mu(x)$、$y - \lambda(x)\rangle$ 成立且二者互素的情况下，我们知道 S_y 的埃尔米特标准形有唯一一个非平凡的对角项，即 μ。因此，除埃尔米特标准形中将其归一化为首一多项式外，后者也是 S_y的行列式。

反过来，$S \in \mathbb{K}$[的埃尔米特标准形] 对角线上的最后一个元素属于 I_y。因此，根据假设，h 必须是 μ 和结式的倍数。由此可得，$h = \mathrm{Res}_y(a,b) = \mu$，且埃尔米特标准形的所有其他对角项均为 1。这证明 a 和 b 关于 y 的首项系数互素；否则，埃尔米特标准形的第一个对角项将是 $\mathbb{K}[x]$ 的非恒定多项式。由 (ii) [43, Thm. 4] 可得结论。 □

关于结式与关联理想之间的联系，读者尤其可以参阅 [15], 其中给出了引理2.2的一个一般多变量版本。

例 *2.1.* 即使存在无穷远根，Sylvester 矩阵也可能只有一个非平凡不变因子（我们的算法将计算该因子）。取 $\mathbb{K} = \mathbb{F}_2$，令 $a = (x+1)\,y + x^2$ 和 $(x+1)\,y^2 + y$。我们有 $I = \langle x^2, y\rangle$，而 S_y 的 Hermite 标准形为

$$S_y U = \begin{bmatrix} x+1 & 0 & 0 \\ 1 & x+1 & 0 \\ 0 & x^2 & x^2\,(x+1) \end{bmatrix},$$

其中 U 是幺模矩阵。引理 2.1和 2.2 中使用的论证均不适用：无法在不改变对角线的情况下，通过幺模行变换将埃尔米特标准形化为 Smith 标准形（正如引理 2.1的证明中所用的方法），而且该标准形也并非平凡形式（引理 2.2的证明）。S_y 的最后一个不变因子为 $\mathrm{Res}_y(a,b) = x^2\,(x+1)^3$. □

现在，我们利用多项式矩阵的列约化性来刻画无穷远根的存在性 [32,第 6.3 节，第384], 页；这一性质将在后续章节中用到。设 S 是一个 $\mathbb{K}[x]^{n\times n}$ 中的矩阵，其第 j 列的次数为 d_j。我们称 S 的（列）首（矩阵）系数为 $\mathbb{K}^{n\times n}$ 中的矩阵，其第（i, j）个元素是 次数为 d_j 的i, j位置元素在 S中的系数矩阵。我们讨论非奇异单变量多项式矩阵，并称这类矩阵为列约化的，如果其首系数矩阵可逆。

引理 2.3. S_x 列约化，当且仅当，a 和 b 的 y 首项系数互素，并且在 $\mathbb{K}[x]$ 中，后两个多项式至少有一个的次数分别为 d_a 或 d_b。

证明。 设 $s,t \in \mathbb{K}[x]$ 分别为 a、b 的 y-首项系数，其次数分别为 d_s 和 d_t。S_x 的首项系数矩阵的各列由 $\mathbb{K}^{d_a+d_b}$ 中的向量给出，这些向量对应于

$$x^{d_b-1}s, x^{d_b-2}s, \ldots, s, x^{d_a-1}t, x^{d_a-2}t, \ldots, t.$$

若S_x 列约化，则其首项系数矩阵的第一行非零，且$d_s = d_a$ 或$d_t = d_b$。不妨设$d_s = d_a$ （至多相差一个列置换）。因此，S_x 的首项系数为

$$x^{d_b-1}s, x^{d_b-2}s, \ldots, x^{d_t}s, x^{d_t-1}s, x^{d_t-2}s, \ldots, s, x^{d_s-1}t, x^{d_s-2}t, \ldots, t, \tag{1}$$

并且我们 看到其秩与由s和t 对应的 Sylvester 矩阵的秩相同，因为后者为

$$x^{d_t-1}s, x^{d_t-2}s, \ldots, s, x^{d_s-1}t, x^{d_s-2}t, \ldots, t.$$

反过来，由等式（1）中向量的线性无关性可得S_x的列约化性。 □

3 二元多项式除法

本节提出一种针对理想 I = ⟨a,b⟩ 的二元多项式标准形算法。该算法依赖于矩阵多项式除法。我们将 $\mathbb{K}$[x,y] 中的二元多项式交替视为关于 $\mathbb{K}$[x] 和 $\mathbb{K}$[y], 的单变量多项式向量；将这样的向量除以 S_y 或 S_x，实际上等价于将相应多项式模该理想化简。西尔维斯特矩阵是 Toeplitz 类矩阵。我们首先在第 3.1 节回顾如何在考虑其结构 [6, 50] 的情况下对这类矩阵进行运算。随后在第 3.2 节研究多项式向量除以 S_y 或 S_x 的带余除法。为了定义标准形并高效地执行除法，我们采用关于首项系数矩阵的正则性假设：假设 S_x 和 S_y 是列约化的。对于计算最后一个不变因子而言，这一假设最终不会造成实质影响（第 5 节）。

在第3.3节中，我们介绍标准形算法。对于 a 和 b 的次数以及矩阵的维数，我们沿用前文的记号；特别地，d 是关于 x 的最高次数，且 S_y is $n_y \times n^{y}$。给定一个 ˆ ˆ 多项式 f ∈ $\mathbb{K}$[x, y],，我们将说明如何计算唯一的多项式 f ∈ $\mathbb{K}$[x, y]$_{<(d,n_y)}$，记作 f =ˆ f rem I，使得 f − f ∈ I（命题 3.1）。借助多项式矩阵除法所提供的适当性，便可保证唯一性。该构造是一个 $\mathbb{K}$-线性映射，将 f 映射为 f，其 y-系数由下式给出

向量的各个分量$v_y(\hat{f}) \in \mathbb{K}[x]_{<d}^{n_y}$使得$S_y^{-1}v_y(\hat{f})$是严格真有理的（当$x$趋于无穷时趋于零），见式（2）。这使我们能够用标准形表示$\mathbb{A}$中的元素。用于计算相应幂投影的转置算法将在第3.4节中推导。

设$\deg_x a = d_a$、$\deg_x b = d_b$、$\deg_y a = e_a$，且$\deg_y b = e_b$，则商代数$\mathbb{A}$的维数至多为$d_a e_b + d_b e_a$。为了表示其中的元素，将该商代数嵌入维数为$\mathbb{K}[x]_{<d}^{n_y}$的空间

$$dn_y = \max\{d_a, d_b\}(e_a + e_b)$$

因此其维数可能略大（示例3.1）。

3.1 结构化矩阵运算

标准形算法利用了西尔维斯特矩阵具有结构这一事实。我们所面对的结构类别是类托普利茨多项式矩阵，通常通过位移秩[33]的概念来处理。该概念使我们能够以紧凑的矩阵表示来表示矩阵，从而高效地执行矩阵运算高效[6, 50]。

给定多项式a和b，S_x和S_y可用$\mathbb{K}$中的$O(de)$个元素表示。除法算法需要求解相关线性方程组，并使用含有截断幂级数项的矩阵求逆。我们认为，多项式西尔维斯特矩阵及其逆矩阵均用其紧凑的类托普利茨表示[6]表示。例如，可通过将域[34], 上定义的ΣLU形式扩展到多项式或截断幂级数[52,（见第3]节）来实现这一点。

将一个次数为d、大小为n×n的多项式Sylvester矩阵与一个次数至多为l的多项式向量相乘（在$\mathbb{K}[x]$上），可在$\mathbb{K}$[6]中用O(n(d+l))次算术运算完成。当矩阵逆存在时，使用矩阵模x^l的逆进行同类乘法，也具有这一复杂度界。若$T \in \mathbb{K}^{n\times n}$是一个非奇异的Sylvester矩阵，且$v \in \mathbb{K}^n$，则线性方程组$T^{-1}v$可用$\tilde{O}(n)$次算术运算求解。这是结合Sylvester矩阵的求逆公式[41], 与矩阵Padé逼近[3]得到的（另见[6, 第2章，第9]节及[63, 第5]节）。这一方法在第3.2节中应用于模x^l的截断幂级数。设$S \in \mathbb{K}[x]^{n\times n}$ d是一个多项式Sylvester矩阵，满足det S (0) $\neq$ 0，并考虑一个次数至多为l的向量$v \in \mathbb{K}[x]^n$。线性方程组$S^{-1}v$可模x^l用$\tilde{O}(n(d+l))$次算术运算求解。根据[63, 命题5.1],，模x^l的矩阵逆本身也可在相同的复杂度界内计算（并采用紧凑表示）。

3.2 矩阵与二元多项式除法

考虑$\mathbb{K}[S\,x]^{n\times n}$，其为次数为$d$的非奇异矩阵。对于任意向量$v \in \mathbb{K}[x]^n$，由[32, 定理6.3-15，第389]页可知，存在唯一的w、$\hat{v} \in \mathbb{K}[x]^n$，使得

$$v = S\,w + \hat{v}, \tag{2}$$

且$S^{-1}\hat{v}$是严格真有理的。由[32, 定理6.3-10，第383]页，我们进一步得到，多项式余式向量$\hat{v}$的次数小于d；但需要注意的是，唯一性是由真有理性而非后一个次数性质保证的（例3.1）。

以下内容将同时应用于S_x和S_y，因此我们在表述中采用一般记号S。我们针对（标量）带余多项式除法，提出一种结构化矩阵多项式版本的Cook-Sieveking-Kung算法，读者可参阅[22, 第9节。1]。

引理3.1. 设$S \in \mathbb{K}[x]^{n\times n}$是一个次数为$d$的*Sylvester*矩阵，并假设$S$是列约化的。考虑一个次数至多为$l$的向量$v \in \mathbb{K}[x]^n$。按照公式（2）对$v$除以$S$所得的唯一余式$\hat{v}$可以通过使用$O(n(d+l))$次算术运算在$\mathbb{K}$中计算。

证明。考虑与两个多项式$a,b \in K[x,y]$相关联的S，如前所述，使得$S = S_y$，并且我们有e_1列的次数为d_1，以及e_2列的次数为d_2。经过行和列置换后，不妨假设$d = \max\{d_1,d_2\} = d_1$。

我们首先处理$d = d_1 = d_2$的情形。S的所有列具有相同的次数，因此由于S是列约化的，它也是行约化的（对各行使用引理2.3之前给出的定义）。

如果 l < d，那么取 v̂ = v。根据 [32, 定理 6.3-11，第 385] 页，由于行约化性，我们知道 S⁻¹v 是严格真有理的。如果 l ≥ d，则可将 [22, 第 9.1 节，公式（2）] 重新表述为矩阵上的多项式除法。由于 S 具有非奇异首项系数矩阵，根据可预测次数性质 [32, 定理 6.3-13，第 387] 页，我们知道商向量 w 的次数为 deg v − d，因此至多为 l − d。利用矩阵多项式的反转，公式（2）可改写为

$$\mathrm{rev}_l(v) = \mathrm{rev}_d(S) \cdot \mathrm{rev}_{l-d}(w) + x^{l-d+1}\mathrm{rev}_{d-1}(\hat{v}),$$

因此我们有

$$\mathrm{rev}_{l-d}(w) \equiv \mathrm{rev}_d(S)^{-1}\mathrm{rev}_l(v) \bmod x^{l-d+1}. \tag{3}$$

注意，由约化性假设可知，$\mathrm{rev}_d(S)$ 的 0 次系数矩阵是非奇异的，因此后一个矩阵模 x^{l-d+1} 可逆。一旦已知 $w' = \mathrm{rev}_{l-d}(w)$，进而已知 $w = \mathrm{rev}_{l-d}(w')$，便可利用 $\hat{v} = v - Sw$ 推导出 v̂。与前文一样，根据约化性可知 S⁻¹v 是严格真有理函数。利用快速结构化矩阵运算（第3.1节），可根据式（3）计算 $\mathrm{rev}_{l-d}(w)$，并在所述成本界内得到 v̂。

当 $d = d_1 > d_2$, 时，首先平衡各列的次数。给定 $\delta = d_1 - d_2 > 0$，取 $D = \mathrm{diag}(x^\delta, \ldots, x^\delta, 1, \ldots, 1)$，其中有 e_1 个元素为 x^δ。矩阵 $T = SD^{-1}$ 的所有列次数均为 d_2。此处及下文中，有理函数的次数定义为分子次数与分母次数之差。列约化性和行约化性也相应地作扩展。

若 $l < d_2$，我们令 $v' = v$；否则，我们可以计算一个次数至多为 $l - d_2$ 的多项式向量 w′，并令 $v' = v - Tw'$，使其次数小于 d_2，且 $T^{-1}v'$ 严格真有理。将所有内容乘以 x^δ，从而化为多项式矩阵除法后，利用公式（2）即可完成此计算，时间复杂度为 $\tilde{O}(n(d+l))$。这与上面的 $d_1 = d_2$ 情形类似，因为 T 是列约化的。

然后，将w' 的前e_1 个条目除以x^δ，可写成$w' = Dw + z$，其中z 的次数小于 δ，且只有它的前e_1 个条目可能非零。向量w 的次数仍至多为$l - d_2$, ，我们可在$O(n(d+l))$时间内得到$\tilde{v}$，其中

$$\hat{v} = v - Sw = v - SD^{-1}(w' - z) = v' + SD^{-1}z.$$

为完成证明，我们检查 S⁻¹v 是否为严格真有理。该向量为 S⁻¹v = S⁻¹v′ + D⁻¹z = D⁻¹T⁻¹v′ + D⁻¹z。根据构造，T⁻¹v′是严格真有理，因此 D⁻¹T⁻¹v′也如此；z 的前 e_1个分量（其余分量为零）的次数至多为 $\delta - 1$，因此 D⁻¹z 是严格真有理。□

3.3 双变量理想模标准形

给定一个多项式 $f \in \mathbb{K}[x, y]$ 其 y-次数小于维数 n_y 的 S_y，我们可以将引理 3.1 应用于向量 $v_y(f) \in \mathbb{K}[x]^{n_y}$ 中 的系数 f。方程（2）变为

$$v_y(f) = S_y w + v_y(\hat{f})$$

关于向量，根据 Sylvester 矩阵的定义，我们有

$$\hat{f} = f - ua - vb \in f + I$$

$\hat{}$ 对某些 $u, v \in \mathbb{K}[x, y],$, f的 x-次数小于 d。借助命题 3.1，我们证明，由于余式的唯一性，这使我们能够定义模 $\langle a, b\rangle$的标准形。对于 y-次数一般的情形，f通过先对 S_x 进行除法（其元素属于 $\mathbb{K}[y]$），以降低 y 的次数。整个构造给出一个 $\mathbb{K}$- 线性映射

$$\begin{aligned} \varphi : \mathbb{K}[x, y] &\to \mathbb{K}[x, y]_{<(d, n_y)} \\ f &\mapsto \hat{f} = f \bmod I \end{aligned} \tag{4}$$

使得 $f - \varphi(f) \in I$，并且如果 $g \in I$，则 $\varphi(g) = 0$。因此，映射 φ 适合用标准形表示 $\mathbb{A}$ 中的元素。

例 3.1。令 $\mathbb{K}=\mathbb{Q}$，考虑 $a=x^2y+y$ 和 $b=xy^2+x$；我们有 $d=d_a=2$ 和 $n_y=e_a+e_b=1+2=3$。若 $f=x$，则 f 和 $f-b=-xy^2$ 均属于 $\mathbb{K}[x,y]_{<(2,3)}$，因此映射 φ 可能不是满射。公式（2）中的除法得到

$$v_y(f)=\begin{bmatrix}0\\0\\x\end{bmatrix}=S_y w+v_y(\hat{f})=\begin{bmatrix}x^2+1 & 0 & x\\ 0 & x^2+1 & 0\\ 0 & 0 & x\end{bmatrix}\begin{bmatrix}0\\0\\1\end{bmatrix}+\begin{bmatrix}-x\\0\\0\end{bmatrix},$$

以及 $\hat{f}=f-b$ 因为我们可以验证 $S^{-1}v_y(\hat{f})$ 是严格真有理的，而 $S^{-1}v_y(f)$ 则不是。值得注意的是，商代数 $\mathbb{K}[x,y]/\langle a,b\rangle$ 的维数为 5，小于 $\mathbb{K}[x,y]_{<(2,3)}$ 的维数。□

若 $\eta=\deg_y f\ge n_y$ 且 $\delta=\deg_x f$ 小于 S_x 的维数 n_x，那么我们可以直接利用 S_x进行除法。否则，正如引理 3.2 所示，我们首先将 S_x 扩展为一个更大的适当 Sylvester 矩阵 T_x，其维数为 $\delta+1$。通过线性化，我们将向量 $v_x(f)\in\mathbb{K}[y]^{\delta+1}$ 与 f 关联起来，其 y 次数为 η。随后利用 T_x进行除法；T_x 的 y 次数是 S_x 的次数 e。由此可计算出 f'，其 y 次数小于 $e<n_y$，且满足 $f-f'\in I$。

引理 3.2. 假设关于 x 构造的 a 和 b 的 *Sylvester* 矩阵 S_x 是列约化的。考虑$\tilde{f}\in\mathbb{K}[x,y]$，其 x 次数至多为 δ，y 次数至多为 $\eta\ge n_y$。通过在 $\mathbb{K}$ 中进行 $O((n_x+\delta)\eta)$ 次算术运算，我们可以计算出一个多项式 $f'\in\mathbb{K}[x,y]$,，其 x 次数至多为 $\max\{n_x-1,\delta\}$，y 次数小于 $e<n_y$，且满足 $f-f'\in I$。

证明。如果 δ 小于 n_x，我们只需取 $T_x=S_x$。否则，令 $m=\delta-n_x+1$，并将 a、b 的 y 首项系数记为 s、$t\in\mathbb{K}[x]$。由于 S_x 是列约化的，根据引理 2.3，我们知道 $\gcd(s,t)=1$。s 或 t 中至少有一个不能被 x 整除；不妨设为 s，并令 T_x 为关于 $\mathbb{K}[y]$, 的、由 a 和 $x^m b$ 关于 x 构造的 Sylvester 矩阵。s 和 $x^m t$ 对应的 Sylvester 矩阵是非奇异的，因此根据引理 2.3，T_x 也是列约化的：若 $\deg s=d_a$ 或 $\deg t=d_b$，则 $\deg s=d_a$ 或 $\deg t+m=d_b+m$。

矩阵 T_x的维数为 $\max\{n_x,\delta+1\}$，次数为 $e=\max\{e_a,e_b\}$（关于 y）。将 $v_x(f)$ 除以 T_x 所得的余式为 f'，满足 $f-f'\in I$，其 y 次数小于 T_x的 y 次数，且其 x 次数小于 T_x的维数。根据引理 3.1，计算成本上界为：使用维数为 $n=\max\{n_x,\delta+1\}$、次数为 e 的矩阵，以及次数为 $l=\eta\ge e$ 的向量。□

引理 3.2 允许先约化 y 次数，而现在对 x 次数的约化也能确保得到标准形。

命题 3.1. 假设与 a 和 b 相关联的西尔维斯特矩阵 S_x 和 S^y 均为列约化矩阵，并考虑 $f\in\mathbb{K}[x,y]$。式(4) 中的 $\mathbb{K}$-线性映射定义良好：为 f 选取 $\mathbb{K}[x,y]_{<(d,n_y)}$中的唯一多项式，使得 $f-\hat{f}\in I$，且 $S_y^{-1}v_y(\hat{f})$ 严格真有理。若 f 的 x 次数至多为 δ，y 次数至多为 η，则可使用 $O((d+\delta)(e+\eta))$ 次 $\mathbb{K}$中的算术运算，计算 $f+I$ 在 $\mathbb{A}$ 中的这一标准形。

证明。我们先证明对每个 f 都存在这样的 f，然后证明若 $g=0$ 属于 I，则 $\hat{g}=0$。利用引理 3.2 除以 S_x 后，得到 $f'\in\mathbb{K}[x,y]$，其 y 次数小于 $e<n_y=e_a+e_b$，且满足 $f-f'\in I$。接着由引理 3.1，也就是除以 S_y，得到 $\hat{f}\in\mathbb{K}[x,y]_{<(d,n_y)}$，使得 $f'-\hat{f}\in I$，因此 $f-\hat{f}\in I$。根据构造，$S_y^{-1}v_y(\hat{f})$ 是严格真有理的。对于 $g\in I$，首先得到某个 g'，其 y 次数小于 $e<n_y$。由于 S_y 是列约化的，由引理 2.3 可知，a 和 b 的 y 首项系数互素，因此利用 [43, 引理 7]，存在多项式 $r,s\in\mathbb{K}[x,y]$，使得

$$g'-ra-sb=0,\ \deg_y r<e_b,\ \text{and}\ \deg_y s<e_a.$$

由唯一性可知，我们必有 $\hat{g}=0$，因为根据上述恒等式，这个值是合适的。

映射 $\varphi(f)$ 良好的，并给出了一个标准形。对于陪集 $f+I$ 中的 f_1,f_2，我们确实有$\varphi(f_1-f_2)=0$，因此根据除法的 $\mathbb{K}$-线性，$\varphi(f_1)=\varphi(f_2)$。

~根据引理 3.2，第一次用 S_x 进行除法的代价为 $O((d+\delta)(e+\eta))$，这里我们利用了 S_x 的维数为 $n_x\le 2d$、次数为 e。这接下来需要用 S_y对一个次数至多为 $\max\{n_x-1,\delta\}$ 的向量进行除法；S_y的维数为 $n_y<2e$~，次数为 d。根据引理 3.1，这还需进行 $O(e(d+\delta))$ 次运算。□

例 3.2。我们继续考虑例 3.1 中的 $a = x^2y + y$ 和 $b = xy^2 + x$；S_x 和 S_y 的维数均为 $n_x = n_y = 3$。对于 $f = y^3 + x^3y^2 + 1$，我们首先利用 S_x 降低 y 次数。由于 $\delta = \deg_x f \geq n_x$，我们无法直接使用 S_x，其为 3×3。按照引理 3.2 的证明，我们增大维数，并考虑 $T_x \in \mathbb{K}[y]^{4\times4}$，即关于 x、与 a 和 xb 相关的 Sylvester 矩阵。因此，第一次除法为：

$$v_x(f) = \begin{bmatrix} y^2 \\ 0 \\ 0 \\ y^3+1 \end{bmatrix} = T_x w_1 + v_x(f') = \begin{bmatrix} y & 0 & y^2+1 & 0 \\ 0 & y & 0 & y^2+1 \\ y & 0 & 0 & 0 \\ 0 & y & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ y^2 \\ 1 \\ -y \end{bmatrix} + \begin{bmatrix} -1 \\ y \\ 0 \\ 1 \end{bmatrix}.$$

新多项式为 $f' = -x^3 + yx^2 + 1$，其 y 次数为 $1 < n_y$，因此现在可以通过 $S_y \in \mathbb{K}[x]^{3\times3}$ 进行除法，以降低 x 次数：

$$v_y(f') = \begin{bmatrix} 0 \\ x^2 \\ -x^3+1 \end{bmatrix} = S_y w_2 + v_y(\hat{f}) = \begin{bmatrix} x^2+1 & 0 & x \\ 0 & x^2+1 & 0 \\ 0 & 0 & x \end{bmatrix} \begin{bmatrix} x \\ 1 \\ -x^2 \end{bmatrix} + \begin{bmatrix} -x \\ -1 \\ 1 \end{bmatrix}$$

并得到标准形 $\hat{f} = -xy^2 - y + 1 \in \mathbb{K}[x, y]_{<(2,3)}$。 □

命题 3.1 的假设对于能够降低 x 的次数至关重要，同时也确保了标准形。下面的例子描述了相对于 y 存在无穷远根的情形。

例 3.3. 取 $\mathbb{K} = \mathbb{F}_7$，令 $a = (x+3)y + x^2 + 5x + 5$，$b = (x+3)(x+4)y + x^2 + 4x + 2$。那么，商代数中 x 的最小多项式为 $x + 2$，但无法通过 y 次数小于 $e_a = e_b = 1$ 的 a 和 b 的组合得到，也就是说，无法使用 S_y 的列的组合得到。向量 $[0\ x + 2]^T$ 是其通过 $S_y \in \mathbb{K}[x]^{2\times2}$ 除法所得的自身余式，因此 $x + 2$ 虽然属于理想，却未被化为零。不过，在第 5 节的随机调理作用下，我们能够正确计算结式（见第 7 节）。

由于 $\mathbb{K}[x, y]$ 中的乘法可以在准线性时间 [22, Sec.8.4], 内计算，~命题 3.1 允许在 $\mathbb{K}[x, y]/\langle a, b\rangle$ 中使用 O(de) 次算术运算进行乘法。当两个西尔维斯特矩阵都是列约化时，该结论成立。根据引理 2.3，这意味着 a 和 b 的 x-首（分别为 y-）系数互素，并且其中一个的次数为最大次数 d_a 或 d_b（分别为 e_a 或 e_b）。在互补情形下，即对于分次字典序而言，理想 $\langle a, b\rangle$ 足够一般，并采用总次数时，[26] 已经针对这类商中的乘法实现了准线性复杂度。尽管该结果仍然对理想保留了特定假设，我们还要提及 [30, Sec. 4.5] 中的乘法复杂度界 ~$O((de)^{1.5})$。

3.4 通过转置标准形进行幂投影

借鉴 Shoup 在商代数中计算最小多项式的一般方法，我们尤其依赖这样一个事实：幂投影问题是模复合问题的转置 [57；35，第 6]节。命题3.1 中的标准形算法处理的是模复合的一种特殊情形，因为f 模I 可以看作 $f(g(x))$ 模 I，其中$g = x$。因此，我们迄今为止所做的工作，经过转置后已经可以得到某些幂投影，本节将对此进行说明。这是第4 节一般算法的核心，用于高效计算更多数量的$O(de)$ 个投影，效率为ffi，适用于 $\mathbb{K} = \mathbb{F}_q$。

考虑将$\varphi_{\delta,\eta}$ 限制在 φ 上的情形，其中 $\mathbb{K}$-向量空间为 $\mathcal{U} = \mathbb{K}[x,y]_{\leq(\delta,\eta)}$，并将 $\mathbb{K}[x,y]_{<(d,n_y)}$ 作为一个 $\mathbb{K}$-向量空间记为 $\mathcal{V}$。我们还引入 $\mathcal{U}$ 和 $\mathcal{V}$ 上 $\mathbb{K}$-线性形式的对偶空间 $\widehat{\mathcal{U}}$ 和 $\widehat{\mathcal{V}}$。$\varphi_{\delta,\eta}$ 的转置是如下的 $\mathbb{K}$-线性映射

$$\begin{aligned} \varphi^{\mathsf{T}}_{\delta,\eta} : \widehat{\mathcal{V}} &\to \widehat{\mathcal{U}} \\ \ell &\mapsto \ell \circ \varphi_{\delta,\eta}. \end{aligned} \tag{5}$$

我们将 $\mathcal{U}$ 中的多项式视为单项式基 $\mathcal{B} = \{1, x, \ldots, x^\delta, y, xy, \ldots, x^\delta y^\eta\}$ 上的向量。$\widehat{\mathcal{U}}$ 中关于 $\mathcal{B}$ 的对偶基的线性形式由 $\mathbb{K}^{(\delta+1)(\eta+1)}$ 中的向量表示。$\mathcal{V}$ 和 $\widehat{\mathcal{V}}$ 中的元素在 $\mathbb{K}^{dn_y}$ 中被视为

基 $\{y^{n_y-1}, y^{n_y-1}x, \ldots, y^{n_y-1}x^{d-1}, y^{n_y-2}, y^{n_y-2}x, \ldots, x^{d-1}\}$ 的 $\mathcal{V}$(按照 Sylvester 矩阵 S_y 的定义)。由式（5），$\varphi^{\mathsf{T}}_{\delta,\eta}(\ell)$ 的各项即为双变量幂投影

$$(\ell \circ \varphi_{\delta,\eta})(x^i y^j) \text{ for } 0 \le i \le \delta \text{ and } 0 \le j \le \eta. \tag{6}$$

我们通过应用转置原理 [7, 21; 57]来计算这些投影。该原理指出，如果一个 a$\mathbb{K}$-线性映射 $\phi\colon \mathcal{E}_1 \to \mathcal{E}_2$ 可以用长度为 l 的线性直线程序计算，那么其转置映射可以用长度为 $l + \dim \mathcal{E}_2$(若 ϕ 是同构，则为 l) [12, Thm. 13.20] 的程序计算。我们采用一种常用策略来实现该原理 [9]。命题 3.2 可直接由命题 3.1 得出，例如，仿照 [8, Sec. 4] 中关于 $\mathbb{K}[x, y]/\langle f(x), g(y)\rangle$ 或 [51, 53] 模三角集的结果即可。变化仅涉及理想的表示方式。

命题 3.2。假设与 a 和 b 相关联的西尔维斯特矩阵 S_x 和 S_y 是列约化的。给定两个整数 δ，$\eta \ge 0$ 和 $\ell \in \widehat{\mathcal{V}}$，可以使用 $\tilde{O}((d+\delta)(e+\eta))$ 次 $\mathbb{K}$中的算术运算计算 $\varphi^{\mathsf{T}}_{\delta,\eta}(\ell)$。

证明。关于 $\varphi^{\mathsf{T}}_{\delta,\eta}$ 的结论将由对命题 3.1 中针对$\varphi_{\delta,\eta}$的算法应用转置原理得出，其中部分步骤写成 $\mathbb{K}$-线性直线程序。

计算 $\varphi_{\delta,\eta}$ 归结为两次应用引理 3.1，因此只需研究矩阵带余除法算法的转置。关于该算法，注意到若预先计算了式（3）中的矩阵逆，那么之后涉及的就只有输入向量各项中的 $\mathbb{K}$-线性形式。此外，这些线性形式可以通过-线性直线计算求得。因此，引理 3.1 中的除法算法可以表述如下：按照引理 3.1中所述的时间，利用第 3.1 节的复杂度界，预先计算式（3）中反向 Sylvester 矩阵在截断幂级数上的逆。随后，在相同的成本界内执行涉及输入向量的线性运算，包括结构化矩阵向量乘积 [6], 。转置除法算法如下：它将预先计算的逆作为参数，并通过对其余线性直线程序部分应用转置原理得到。对于转置除法，这给出的复杂度界与引理 3.1 中所述相同；对于转置 $\varphi^{\mathsf{T}}_{\delta,\eta}$，则得到命题 3.1 中的复杂度界。□

我们直接使用转置原理。不过，转置算法也可以像 [9] 中单变量情形的处理那样，通过线性递推序列扩展的对偶性 [56], 以及 [51, 53]中多变量三角集的处理那样，表述得更加明确。

4 Kedlaya 和 Umans 技术的应用

在x 对 $\mathbb{A}$ 的乘法所对应的最小多项式，需要计算$O(de)$次幂的x 的投影（第6节）。因此，命题3.2 不足以实现准线性复杂度。这促使我们应用 Kedlaya 和 Umans 的技术 [40], 及其在 [53, 28], 中的扩展，以便实现有限域上的高效模复合（推论ffiicient modular composition over afinitefield(Corollary 4.1)andpowerprojection by transposition (Corollary 4.2）。

给定三个多项式 f、g、h $\in \mathbb{K}[x]$，其中 deg(f) <n 且 deg(g) <n，n =deg(h)，模复合问题是计算 f(g) mod h [11]。（更根本地说，这个问题是在一个环上定义的。）在这种情形下，从一开始我们就能受益于这样一个事实：对于此类多项式，可以用 O(n) 次算术运算计算带余除法˜ [22, 第 9 节1]。二元情形的难点之一，是要能够从类似的起点出发，也就是说，高效地计算模 I 的带余除法。一旦做到这一点，就可以按照 [40] 中的方法处理模复合和幂投影。 [53]（多变量情形）和 [28]（特殊情形 g = x）已经分别实现了这一点，其理想 I 的形状正是我们前面提到的那些。我们采用同样的方法，将新的除法（标准形）算法整合到整个过程中。因此，我们不再重复定理 4.1 及其推论的全部证明细节，而是请读者参阅相关论文。至于命题 3.2，我们的改动在于理想的表示方式，这由此导出了推论 4.2 中新的模双变量投影算法。

第一个主要步骤是将模复合的除法问题，化约为输入次数较小的除法以及一个多点求值问题 [40, Pb.2.1]。更具体地说，定理 4.1 表明

计算 f $\in \mathbb{K}[x]_{<\delta}$ 模 I 的标准形问题，当 $2 \le d_\epsilon < \delta$ 时，可化约为 x 次数和 y 次数分别小于 $d_\epsilon d \log \delta$ 和 $d_\epsilon e \log \delta$ 的多项式的标准形问题，以及多点求值问题。这里请记住记号 $d = \max\{\deg_x a, \deg_x b\}$ 和 $e = \max\{\deg_y a, \deg_y b\}$。Sylvester 矩阵 S_y 是 $n_y \times n_y$ 阶的，定义在 $\mathbb{K}$ 上。

定理 *4.1*（[40, 定理 *3*.1], 在 [53, 28] 中的推广）。设 $f \in \mathbb{K}[x]$ 的次数小于 δ，且 $2 \le d_\epsilon < \delta$ 为任意整数。假设与 a 和 b 相关联的西尔维斯特矩阵 S_x 和 S_y 均为列约化，并且$|\mathbb{K}| > l(d_\epsilon - 1)\, max\{d - 1, n_y - 1\}$，其中 $l = \lceil log_{d_\epsilon}(\delta) \rceil$。若 $\delta = O(de)$，则可使用 $\tilde{}O(d_\epsilon^2 de)$ 次算术运算计算 $f(x)\ rem\ I$，此外还需对一个含 l 个变量、各变量次数小于 d_ϵ的多项式，在 $\mathbb{K}$ 上的 $O(l^2 d_\epsilon^2 de)$ 个点处进行一次多元多点求值。

证明。 以下六个步骤即为 [40, 定理 3.1] 的证明步骤。

1. 首先，我们使用逆克罗内克代换 [40, Dfn. 2.3], , 将 f 映射为一个有 l 个变量、且每个变量的次数都小于 d_ϵ的多项式。这个从 $\mathbb{K}$-线性映射 $\mathbb{K}[x]_{<\delta}$ 到 $\mathbb{K}[z_0, \ldots, z_{l-1}]_{<(d_\epsilon, \ldots, d_\epsilon)}$ 定义如下。对于 $0 \le k < \delta$，单项式 x^k 被映射为 $z_0^{k_0} z_1^{k_1} \ldots z^{k_{l-1}} l_{-1}$，其中 $k_0, k_1, \ldots, k_{l-1}$ 是 k 在 d_ϵ进制展开中的系数。将此映射线性扩展到 $\mathbb{K}[x]_{<\delta}$，并以这种方式将 f 映射为多项式$\phi \in \mathbb{K}[z_0, \ldots, z_{l-1}]_{<(d_\epsilon, \ldots, d_\epsilon)}$。该映射在 $\mathbb{K}[x]_{<\delta}$ 上是单射，并可利用单项式基在线性时间内计算。 2. 接着，我们计算多项式 $\chi_i = x^{d_\epsilon^i} \text{ rem } I \text{ in } \mathbb{K}[x, y]_{<(d, n_y)}$，其中 $i = 0, \ldots, l - 1$。这相当于对 d_ϵ 进行 l 次模 I 的幂运算。根据命题 3.1，通过连续进行二元多项式乘法 [22, Sec. 8.4], , 并在每次乘法后对理想取余˜，可在 O(de) 时间内完成。一个关键性质是 $f(x) \text{ rem } I = \phi(\chi_0, \ldots, \chi_{l-1}) \text{ rem } I$。因此，我们可以先通过求值-插值计算 $\phi(\chi_0, \ldots, \chi_{l-1})$，然后再对理想取余。我们知道，$\phi(\chi_0, \ldots, \chi_{l-1})$ 的次数在 x 中至多为 $\delta' = l(d_\epsilon - 1)(d - 1)$，在 y 中至多为 $\eta' = l(d_\epsilon - 1)(n_y - 1)$。 3. 我们从 $\mathbb{K}$中选取子集 K_1 和 K_2，其基数分别为 $\delta' + 1$ 和 $\eta' + 1$。通过二元多点求值，我们计算所有的值 $\mu_{i,j,k} = \chi_i(\lambda j, \lambda_k) \in \mathbb{K}$，其中 $i = 0, \ldots, l - 1$，且 $(\lambda j, \lambda_k) \in K_1 \times K_2$。逐个变量进行单变量求值 [22, Sec. 10.1], , 所需运算次数为 $\tilde{}O(l\delta'\eta')$，因此为 $\tilde{}O(d_\epsilon^2 de)$ 次运算 $(n_y \le 2e)$。 4. 接下来计算所有的值 $\phi(\mu_{1,j,k}, \ldots, \mu_{l,j,k})$；这是对一个有 l 个变量、各变量次数均小于 d_ϵ的多项式，在 $\mathbb{K}^l$中的 $(\delta' + 1)(\eta' + 1)$ 个点上进行多点求值。 5. 随后，根据刚才在 $K_1 \times K_2$, 处得到的值，通过二元插值恢复 $\phi(\chi_0, \ldots, \chi_{l-1})$；与上文的二元多点求值类似，这需要 $\tilde{}O(d_\epsilon^2 de)$ 次运算。˜6. 最后，$f(x) \text{ rem } I = \phi(\chi_0, \ldots, \chi_{l-1}) \text{ rem } I$。根据命题 3.1，我们知道这需要 $O(\delta'\eta')$ 次运算，即 $\tilde{}O(d_\epsilon^2 de)$。□

根据 [40, 定理 7。1] 并且 [53, 28], 借助快速多点求值 [40, 推论 4。5], 现在我们可以界定将单变量多项式模理想约简的代价。

推论 4.1。 设 $\mathbb{K}$ 为一个有限域 $\mathbb{F}_q$。假设与 a 和 b 相关联的西尔维斯特矩阵 S_x 和 S_y 均为列约化，并考虑次数小于 $\delta = 4de$ 的 $f \in \mathbb{F}_q[x]$。对于任意常数 $\epsilon > 0$，若 $q \ge \delta^{1+\epsilon}$，则 f 模 I 可通过 $O((de)^{1+\epsilon} \log(q)^{1+o(1)})$次位操作计算。

证明。根据 ϵ，我们选取一个足够大的常数整数 c，使 $d_{\frac{\epsilon}{d_\epsilon}} = \lceil \delta^{1/c} \rceil$ 相对于 de 足够小。特别地，我们有 $d_\epsilon < \delta^\epsilon$，且 $l = \lceil \log_{4\ 1} \tilde{}(\delta) \rceil \le c$。取足够大的 δ，可得 $l(d_\epsilon - 1) \max\{d, n_y - 1\} \le q$，因此可以应用定理。。我们知道，f 模 I 可通过 $O(d_\epsilon^2 de)$ 次运算在 $\mathbb{F}_q$ 中计算，即 $O(de)^{1+\epsilon}$，再加上相应多点求值的代价。接着利用以下事实：对于任意常数 $\gamma > 0$，存在一种算法，可在 $\mathbb{F}_q[z_0, 、 \ldots 、 z_{l-1}]_{<(d_\epsilon, \ldots, 、 d_\epsilon)}$ 中对一个多项式求值，在 $\mathbb{F}_q^l$ 中的 n 个点上使用 $(d_\epsilon^l + n)^{1+\gamma} \log(q)^{1+o(1)}$ 次位操作；前提是各变量次数 d_ϵ 足够大，且变量个数 l 至多为 $d_\epsilon^{o(1)}$ [40, 推论 4.5]。考虑定理 4.1 中的求值参数以及 $l \le c$，对于每个 $\gamma > 0$，多点求值的代价为 $O((\delta + d_\epsilon^2 de)^{1+\gamma} \log(q)^{1+o(1)})$，由此可得所声称的复杂度界。□

如前所述，与 [40]的表述相比，我们的表述更为简化。类似于推论 q 中的复杂度界，对 4.1 的依赖关系被明确写出，并用 [53] 中的多对数函数表示。对 [28] 的研究使用一个缓慢增长的显式函数来表示多点求值问题的变量个数。在 [27, 5] 中可以找到多点求值的更精确界和改进算法，而 [29]

用于有限域上的多元模组合成。由于我们还依赖于对偶问题的一种解法，而后面提到的参考文献并未讨论这一问题，因此我们的工作基本上仍以 [40]为基础。

与第 3.4 节中的做法类似，我们现在对推论 4.1 的算法取转置。我们的推理依据是 [40, 定理 7。7], [53, 定理 3。3] 以及 [28, 命题 1] 关于模幂投影的内容。我们采用式（ φ （4）中的记号来表示正规形映射。

推论 4.2。 设 $\mathbb{K}$ 是一个有限域 $\mathbb{F}_q$。假设与 a 和 b 相关联的西尔维斯特矩阵 S_x 和 S_y 均为列约化。设 ℓ 是 $\mathbb{F}_q[x, y]_{<(d,n_y)}$ 的对偶空间中的一个线性形式。对于任意常数 $\epsilon > 0$，若 $q \geq \delta^{1+\epsilon}$ 满足 $\delta = 4de$，则投影 $(\ell \circ \varphi)(x^i)$ 对 $0 \leq i < \delta$ 可通过 $O((de)^{1+\epsilon} \log(q)^{1+o(1)})$ 次位操作计算得到。

证明。由式 (6)，我们需要计算 $\varphi^{\mathsf{T}}_{\delta-1,0}(\ell)$。将转置原理（第 3.4 节）按相反顺序应用于推论 4.1 的标准形算法中的各个代数步骤，即可得出这一结论。多点求值所涉及的算法中的非代数部分，则通过 [40, Thm. 7.6] 处理。算法的各个步骤见定理 4.1 [40, Thm. 3.1] 的证明。其中，需考虑依赖输入 f 的四个步骤，即步骤 1、4、5 和 6；我们将它们视为 $\mathbb{F}_q$-线性映射。最后一步（步骤 6）是模 I 约化，其转置由命题 3.2 得出。步骤 5 是二元插值，通过先对 x 再对 y 插值来计算。对此进行转置时，使用两次转置的单变量插值 [36, 9]。步骤 4 是使用 [40,Cor. 4.5] 进行多元求值。当环境维数等于求值点的数量时，转置由 [40, Thm. 7.6] 给出，也就是说，该线性映射可以表示为一个方阵。对于我们所处的一般情形，即求值点数量更多的情形，则如 [40, Thm. 7.7] 的证明所述，使用方阵情形的多个实例来处理，其代价符合所声称的上界。最后，步骤 1 中逆克罗内克代换的转置是一个投影，所需时间为线性时间。根据转置原理和 [40, Thm. 7.6], , 由这些转置得到的算法能够以 $O((de)^{1+\epsilon} \log(q)^{1+o(1)})$ 次位操作计算幂投影，与推论 4.1 中相同。□

5 使用随机平移和反转构造非奇异首项矩阵

为了利用推论4.2 中的幂投影进行最小多项式计算，并求出 S_y 的史密斯标准形的最后一个不变因子，我们需要解决列约化性问题。本节将介绍我们的解决方法。如果输入多项式 a 和 b 得到的 S_x 和 S_y 具有奇异的首项系数，那么我们将构造两个新的多项式 a' 和 b'，以克服这一困难。

引理 5.1（S_x **的调理**）。给定 $\alpha \in \mathbb{K}$，且其不是$\mathrm{Res}_x(a,b)$ 的根（该理想是零维的），我们可以在 $\tilde{O}(de)$ 算术时间内计算出两个多项式 a' 和 b'，它们的次数分别与 a 和 b 的次数相同，使得新的 *Sylvester* 矩阵 S'_x 是列约化的，且 S'_y 的史密斯标准形与 S_y的史密斯标准形相同。

证明。考虑 $a^{(1)}(x, y) = a(x, y + \alpha)$ 和 $b^{(1)}(x, y) = b(x, y + \alpha)$。关于 x 的新 Sylvester 矩阵 $S_x^{(1)}$ 的常数项非奇异，因为 $(\mathrm{Res}_x(a, b))(\alpha) \neq 0$。$S_y^{(1)}$ 的 Smith 标准形与 S_y 的 Smith 标准形相同。事实上，设 $Q_{\alpha,k} \in \mathbb{K}^{k\times k}$ 为自同态的矩阵，该自同态将次数小于 k 的多项式平移 α；$Q_{\alpha,k}$ 是对角线为单位元的下三角矩阵。我们有

$$S_y^{(1)} = Q_{\alpha,e_a+e_b}\, S_y\, \mathrm{diag}(Q^{-1}_{\alpha,e_b}, Q^{-1}_{\alpha,e_a}), \tag{7}$$

因此 $S_y^{(1)}$ 和 S_y 幺模等价。接下来，我们分别将 $a^{(1)}$ 和 $b^{(1)}$ 关于 y 反转，得到反转多项式a' 和 b'，所用次数分别为 e_a 和 e_b。注意，a' 和 b' 必须保持相同的 y 次数，否则 $S_x^{(1)}$ 的常数项就不可能非奇异；出于同样的原因，与 a' 和 b' 相关联的新矩阵 S'_x 是列约化的。另一方面，关于 y 的 Smith 标准形保持不变，因为

$$S'_y = J_{e_a+e_b}\, S_y^{(1)}\, \mathrm{diag}(J_{e_b}, J_{e_a}), \tag{8}$$

其中 J_k 是维数为 k 的反转矩阵。计算成本主要来自至多 $2(d+1)$ 次移位，每次移位作用于次数至多为 e 的多项式，且位于 $\mathbb{K}[y]$, 中，参见例如 [6][第 1 章，习题 3。5]。□

请注意，引理 5.1 保持 S_y 的史密斯标准形，但不一定保持其埃尔米特标准形。由引理 2.3，$a' = b' = 0$ 关于 y 没有无穷远根，因此 S_y 的最后一个不变因子是新商代数中关于 x 的乘法的最小多项式（引理 2.1 ）。后者可能已经改变，并且由于 $a = b = 0$ 可能存在无穷远根，还会多出一个因子。

现在，我们对S_y 的列约化性进行同类型的处理，并需要先对反转多项式矩阵作一项初步观察。矩阵多项式的按列逆序，是指将其各列的元素分别按该列的次数反转后得到的矩阵。

引理 5.2（逆序史密斯标准形）。$A \in \mathbb{K}[x]^{n\times n}$ 按列反转后所得矩阵的最后一个不变因子，是将 A 的最后一个不变因子反转并化为首一多项式后，再乘以 x 的某个幂所得。

证明。设X 属于 $\mathbb{K}[x]^{n\times n}$ ，其行列式为x 的某个幂，并且A 按列反转所得的R 满足$R = A\ (1/x)X$。令A的史密斯标准形为S_A ，并设幺模矩阵U 和V 满足$AV = US_A$。于是

$$RX^{-1}V(1/x) = U(1/x)S_A(1/x). \tag{9}$$

令S_A^*为对角矩阵，其对角元素是S 的对角元素反转后，再除以其首项系数而化为首一多项式所得。将式（9）两边乘以适当的x的幂，得到

$$RW_1 = W_2S_A^*$$

对于两个矩阵 W_1 和 W_2 ，它们属于 $\mathbb{K}[x]^{n\times n}$ ，且其行列式是x的幂。现在令 S_R^* 为对角矩阵，其对角项为R 的不变因子分别除以它们所含的最高次x 幂。采用与上述类似的变换，我们得到

$$S_R^*W_3 = W_4S_A^*$$

对于两个矩阵 W_3 和 W_4 ，它们属于 $\mathbb{K}[x]^{n\times n}$ ，且其行列式也是 x 的幂。根据史密斯标准形的乘法性 [49, 第 II 章，定理 2.15], ，注意到 S_A^* 和 S_R^* 本身就是史密斯标准形，我们得到$S_R^* = S_A^*$。由于R 的最后一个不变因子是$S^*{}_R$ 的最后一个不变因子乘以x的某个幂，而S_A^* 的最后一个不变因子是A 的最后一个不变因子除以其首项系数后所得的倒序多项式，因此结论成立。 □

引理 5.3（调理 S_x 和 S_y）。给定 α，$\beta \in \mathbb{K}$ 它们分别不是$\mathrm{Res}_x(a,\ b)$ 和 $\mathrm{Res}_y(a,\ b) \in \mathbb{K}[x]$, 的根（该理想是零维的），在算术时间 $\tilde{O}(de)$ 内，我们可以计算出两个多项式 a' 和b'，其次数分别与 a 和 b 的次数相同，并满足：新的西尔维斯特矩阵 S_x' 和 S_y' 是列约化的；$S_{\tilde{y}}$的最后一个不变因子可由 S_y' 的最后一个不变因子通过 $O(de)$次额外的算术运算推得。

证明。应用引理 5.1 后，我们可以假设 a 和 b 满足 S_x 是列约化的，且不会改变 S_y，因此 Res_y(a, b) 也不变。我们使用与引理 5.1 证明中类似的论证。首先，令 $a^{(1)}(x, y) = a(x + \beta, y)$，并令 $b^{(1)}(x, y) = b(x + \beta, y)$。关于 y 的新 Sylvester 矩阵 $S_y^{(1)}$有非奇异常数项，因为 $(\mathrm{Res}_y(a, b))(\beta) \neq 0$。我们将 S_y 的最后一个不变因子记为 $\sigma \in \mathbb{K}[x]$。$S_y^{(1)}$的最后一个不变因子为 $\sigma_\beta = \sigma(x + \beta)$，且满足 $\sigma_\beta(0) \neq 0$。接着，分别按照次数 d_a 和 d_b，考虑 $a^{(1)}$ 和 $b^{(1)}$ 关于 x 的反转多项式 a′ 和 b′ 。由于 $S_y^{(1)}$有非奇异常数项，a′ 和 b′ 保持相同的 x 次数，而与 a′ 和 b′ 相关联的新矩阵 S_y' 是列约化的。

现在我们证明关于 a′ 和 b′ 的结论。我们刚刚已经证明了 y-Sylvester 矩阵的列约化性。对于 x，首次应用引理 5.1 后，Sylvester 矩阵是列约化的。使用该引理证明中的公式 (7) 和 (8)，现在令 β、$S_x^{(1)}$ 和 S_x' 分别取相应值，我们推得 S_x' 仍然是列约化的。最后，我们根据 S_y' 的最后一个不变因子，计算 S_y 的最后一个不变因子 σ。Sylvester 矩阵 S_y' 是 $S_y^{(1)}$ 的反转。令 σ_β' 为 σ_β 的反转多项式。由引理 5.2 可得，S_y' 的最后一个不变因子为 $cx^l\sigma_\beta'$，其中 $l \geq 0$ 是某个整数，且 $c \in \mathbb{K}$ 非零。由于 $\sigma_\beta(0) \neq 0$，$cx^l\sigma_\beta'$ 的反转为 $c\sigma_\beta$。通过平移 $-\beta$ 并将多项式化为首一多项式，可得 σ。

除了引理 5.1 中的开销外，我们基本上还需要对次数至多为 $e + 1$ 的多项式执行至多 $2(d$ 次 $\mathbb{K}[x]$, 平移，此外还要对一个次数为 $O(de)$ 的多项式进行最后一次平移，参见例如 [6][第 1 章，题 3。5]。□

6 不变因子计算

对于适当的随机线性形式 ℓ，商代数 $\mathbb{K}[x,y]/\langle a,b\rangle$ 中乘以 x 的最小多项式 μ，以高概率也是线性生成序列 $(\ell\circ\varphi)(x^i)_{i\geq 0}$ 的最小多项式 [58, 第 4 节；39，引理 6]。本质上，这种最小多项式方法是对 Wiedemann [64]，方法的转述，只不过使用乘法矩阵而非稀疏矩阵 [57]。因此，本节首先利用我们先前得到的幂投影复杂度界（推论 4.2）来界定最小多项式问题的复杂度。由于 μ 的次数至多为 2de，因此可由幂投影序列的前 4de 项计算得到。然而，只有当所涉及的西尔维斯特矩阵是列约化时，这一点才成立。经过随机平移和反转（第 5 节）后，我们将说明如何从一个略作修改的商代数中乘以 x 的最小多项式推导出 S_y 的最后一个不变因子。

定理 6.1。考虑两个多项式 a、$b \in \mathbb{F}_q[x, y]_{\leq(d,e)}$，并假设相应的西尔维斯特矩阵 S_x 和 S_y 均为列约化。对于任意常数 $\epsilon > 0$，若 $q \geq \delta^{1+\epsilon}$ 满足 $\delta = 4de$，则存在一种随机蒙特卡洛算法，使用 $O((de)^{1+\epsilon}\log(q)^{1+o(1)})$ 位操作，计算 $\mathbb{F}_q[x、y]/\langle a、b\rangle$ 中乘以 x 的最小多项式。该算法返回最小多项式的一个因子，并且以至少 $1-2de/q \geq 1/2$ 的概率返回与其相等的因子。

证明。按照推论 4.2，针对一个随机线性映射 ℓ计算模幂投影。序列 $\{(\ell\circ\varphi)(x^i)\}_{i\geq 0}$ 是线性生成的；其最小多项式 μ′ 是 $\mathbb{A}$ 中乘以 x 的最小多项式 μ 的一个因子。由于 deg μ ≤ 2de，可以利用该序列的前 4de 项，通过 Algo 12.9]，以 O(de) 次额外操作在 $\mathbb{K}$ 中计算 μ′。只需证明 μ′ = μ 以高概率成立即可得出结论。按照式 (4) 中 φ的构造，可以定义乘法映射

$$\begin{aligned}\psi : \mathbb{F}_q[x,y]_{<(d,n_y)} &\to \mathbb{F}_q[x,y]_{<(d,n_y)}\\ f &\mapsto xf \bmod I.\end{aligned} \tag{10}$$

对于 $\mathbb{F}_q[x, y]_{<(d,n_y)}$ 作为 $\mathbb{F}_q$-向量空间的一组适当的基，我们认为 ψ 由矩阵 $M \in \mathbb{F}_q^{(dn_y)\times(dn_y)}$ 表示，而 1 由向量 $u \in \mathbb{F}_q^{dn_y}$ 表示。根据我们在第 3.4 节中所见，我们还用 $\mathbb{F}_q^{dn_y}$ 中的向量表示 $\mathbb{F}_q[x, y]_{<(d,n_y)}$ 对偶空间中的线性形式。由此，μ 是 u 关于 M 的最小多项式。因此，对于由 $v \in \mathbb{F}_q^{dn_y}$ 表示的随机线性形式 ℓ，线性生成序列 $\{(\ell\circ\varphi)(x^i)\}_{i\geq 0} = \{v^T M^i u\}_{k\geq 0}$ 的最小多项式至少以 $1-\deg\mu/q$ [37, Lem. 2; 38, Lem. 1] 的概率为 μ。□

推论 6.1。考虑两个互素多项式 a，$b \in \mathbb{F}_q[x, y]_{\leq(d,e)}$。对于任意常数 $\epsilon > 0$，都存在一种随机化蒙特卡洛算法，可计算与 a 和 b 相关的 *Sylvester* 矩阵关于 x 或 y 的最后一个不变因子，所需位操作数为 $O((de)^{1+\epsilon}\log(q)^{1+o(1)})$。该算法会返回目标不变因子（概率至少为1/2），或其某个因子，或“失败”。

证明。当 $q \geq (12de)^{1+\epsilon}$ 时，我们随机选取 α 和 β，它们属于 $\mathbb{F}_q$，然后检查引理 5.3~ 中的 S'_x 和 S'_y 是否列约化。该检查需要 O(d+e) 次运算，参见引理 2.1 和例如 [22, Thm. 11.10]。由于 $\mathrm{Res}_y(a, b) \in \mathbb{F}_q[x]$ 和 $\mathrm{Res}_x(a, b) \in \mathbb{F}_q[y]$ 的次数至多为 2de，成功概率至少为 $1-4de/q$。若西尔维斯特矩阵是列约化的，则根据定理 6.1，我们接着计算与 S'_y（或 S'_x）相关的商代数中乘以 x（或 y）的乘法所对应的最小多项式。引理 2.1 告诉我们，实际上我们以至少 $1-2de/q$ 的概率计算出了 S'_y（或 S'_x）的最后一个不变因子。再次应用引理 5.3，我们最终得到 S_y（或 S_x）的最后一个不变因子。如果 q 太小，我们就构造一个 $\mathbb{F}_q$ 的扩域，其基数至少为 $(12de)^{1+\epsilon}$，也就是说，其次数为 O(log(de))。这可以通过预期 $O((\log(de)^2+\log(de)\log(q))$ 次位操作完成 [57] (关于这一点，也请参见 [14] 和 [22, Sec. 14.9])。然后我们在这个扩域中进行运算；由此产生的开销只是对数因子，不会改变目标复杂度界，并且可以调整成功概率。□

7 消去理想与结式

当方程组 $a = b = 0$ 关于y没有无穷远根时，根据引理 2.1 和推论 6.1，我们可以得到一种蒙特卡洛算法，用于计算乘以 x的乘法的最小多项式；它是消去理想 $\langle a,b\rangle \cap \mathbb{F}_q[x]$的生成元。

同样，在关于 y没有无穷远根的情况下，引理 2.2 指出，如果理想还具有形状基 $I = \langle \mu(x), y - \lambda(x) \rangle$ [23, 2]，那么a 和 b 的结式是已知的。注意，引理 ˜ 2.2 中额外的非零常数可以通过在 $O(de)$ 次运算内使用关于 $\mathbb{F}_q$ x 的求值来计算。

对于结式，我们看到，与 [28], 中使用总次数的情形相比，这带来了较弱的一般性假设。假设理想 ⟨ a, b⟩ 关于字典序 y ≻ x 处于一般位置，因此 $\mathrm{res}_y(a, b) = c\mu$，其中 $c \neq 0 \in \mathbb{F}_q$。在这种情况下，再由引理 2.2 和引理 2.1，我们可以将结式计算为 S_y 的最后一个不变因子，而无需对分次逆字典序 [28]施加额外条件。这使我们还能处理比总次数情形更一般的情况，因为对于所有满足 $\mathrm{Res}_y(a, b) = c\mu$ 的情形，我们都能得到结式。这个条件是充分但非必要的（例 2.1 和 3.3）；当 S_y 只有一个非平凡不变因子时，也可以计算结式。请注意，后一性质可以在 Zariski 意义下形式化，例如，借助没有无穷远根且处于一般位置的理想 [16, 第 3 节5]。更准确地说，存在一个关于 $\mathbb{K}$上 $2(d + 1)(e + 1)$ 个变量的非零多项式 Φ，使得当 Φ在 a 和 b 的系数处不为零时，S_y 的 Smith 标准形只有一个非平凡不变因子。

若事先已知结式的次数，通用结式算法便成为 Las Vegas 型，尤其是在 Sylvester 矩阵 S_y 经过列约化时。后一种情况下，结式的次数确实等于S_y [32, 的列次数之和，见式 (24)，第 385]页。

参考文献

[1] M.-E. Alonso、E. Becker、M.-F. Roy 和 T. W¨ormann。《零维系统的零点、重数与幂等元》。载于《代数几何与应用算法》，第 1–15 页。PM 第 143 卷，Birkha¨user，1996年。 [2] E. Becker、T. Mora、M. G. Marinari 和 C. Traverso。《形状引理的形状》。载于 ISSAC 会议论文集，第 129–133 页。ACM出版社，1994年。[3] B. Beckermann 和 G. Labahn。《快速计算矩阵型 Pad´e 逼近的一种统一方法》。SIAM 矩阵分析与应用杂志，15(3)：804–823，1994年。 [4] J. Berthomieu、V. Neiger 和 M. Safey El Din。《在形状与稳定性假设下更快的 Gröbner 基变序算法》。载于 ISSAC 会议论文集，第 409–418 页。ACM出版社，2022年。 [5] V. Bhargava、S. Ghosh、Z. Guo、M. Kumar 和 C. Umans。《所有有限域上的快速多元多点求值》。载于 FOCS 会议论文集，第 221–232 页。IEEE，2022年。 [6] D. Bini 和 V. Y. Pan。《多项式与矩阵计算》。Birkh¨auser，1994年。 [7] J. L. Bordewijk。《电互易性在电网络中的应用》。博士论文，代尔夫特理工学院，1956年。 [8] A. Bostan、P. Flajolet、B. Salvy 和 E. Schost。《特殊结式的快速计算》。符号计算杂志，41(1)：1–29，2006年。 [9] A. Bostan、G. Lecerf 和 ´E. Schost。《将 Tellegen 原理付诸实践》。载于 ISSAC 会议论文集，第 37–44 页。ACM出版社，2003年。 [10] A. Bostan、B. Salvy 和 ´E. Schost。《利用对偶性求解零维多项式系统的快速算法》。应用代数工程与通信，14：239–272，2003年。 [11] R. P. Brent 和 H. T. Kung。《形式幂级数运算的快速算法》。ACM 杂志，25(4)：581–595，1978年。 [12] P. B¨ urgisser、M. Clausen 和 M. A. Shokrollahi。《代数复杂性理论》，数学科学基础丛书第 315 卷。施普林格，1997年。 [13] D. Coppersmith 、 A. M. Odlzyko 和 R. Schroeppel。《 GF(p) 上的离散对数》。Algorithmica，1(1-4)：1–15，1986年。 [14] J.-M. Couveignes 和 R. Lercier。《有限域上不可约多项式的快速构造》。以色列数学杂志，194 105，2013 1 77( ): – 。[15] D. A. Cox 和 C. D’Andrea。《子结式与形状引理》。arXiv:2112.10306，2021年。 [16] D. A. Cox、J. Little 和 D. O’Shea。《代数几何的应用》。施普林格出版社，纽约，1998年。第二版，2005年。 [17] X. Dahan。《模去一个单变量多项式的二元多项式字典序 Gröbner 基》。符号计算杂志，: – 。[18] J.-C. Faug`ere、P. Gaudry、L. Huot 和 G. Renault。《Gröbner 基的次立方换序：一种概率方法》。载于 ISSAC 会议论文集，第 170–177 页。ACM出版社，2014年。 [19] J.-C. Faug`ere 和 C. Mou。《利用稀疏乘法矩阵对零维 Gröbner 基进行换序的快速算法》。载于 ISSAC 会议论文集，第 115–122 页。ACM出版社，2011年。 [20] J.-C. Faug`ere 和 C. Mou。《稀疏 FGLM 算法》。符号计算杂志，80(3)：538–569，2017年。

[21] C. M. Fiduccia。《矩阵乘法的代数复杂性》。博士论文，布朗大学，1973年。 [22] J. von zur Gathen 和 J. Gerhard。《现代计算机代数》。剑桥大学出版社，1999年。第三版，2013年。 [23] P. Gianni、B. Trager 和 G. Zacharias。《Gröbner 基与多项式理想的初等分解》。符号计算杂志，6(2-3)：149–167，1988年。 [24] L. Gonzalez-Vega、F. Rouillier 和 M.-F. Roy。《多项式系统求解的符号方法》。载于《数学与计算算法：计算机代数小品》，第 34–65 页。施普林格，1999年。 [25] J. van der Hoeven。《多元多项式除法的复杂性》。载于 ACA 2015 会议论文集，第 447–458 页。施普林格，计算机科学讲义 PROMs 198，2017年。[26] J. van der Hoeven 和 R. Larrieu。《一般二元理想的快速 Gröbner 基计算与多项式约化》。应用代数工程与通信，30(6)：509–539，2019年。 [27] J. van der Hoeven 和 G. Lecerf。《重新探讨快速多元多点求值》。复杂性杂志，56，2020年。 [28] J. van der Hoeven 和 G. Lecerf。《一般二元结式的快速计算》。复杂性杂志，62，2021年。 [29] J. van der Hoeven 和 G. Lecerf。《多项式系统求解的复杂性指数》。计算数学基础，21(1)：1–57，2021年。 [30] S. G. Hyun、S. Melczer、 ´E. Schost 和 C. St-Pierre。《单变量与二元 m-初等理想的基变换》。载于 ISSAC 会议论文集，第 227–234 页。ACM出版社，2019年。 [31] N. Jacobson。《基础代数 I》。多佛出版社，2009年。第二版，W.H. Freeman，1985年。 [32] T. Kailath。《线性系统》。普伦蒂斯·霍尔，1980年。 [33] T. Kailath、S. Y. Kung 和 M. Morf。《矩阵与线性方程的位移秩》。应用数学与应用分析杂志，68(2)：395–407，1979年。[34] E. Kaltofen。《类托普利兹奇异线性系统的渐近快速求解》。载于 ISSAC 会议论文集，第 297–304 页。ACM出版社，1994年。[35] E. Kaltofen。《符号计算的挑战：我最喜欢的开放问题》。符号计算杂志，29 919，2000 6 891( ): – 。[36] E. Kaltofen 和 Y. Lakshman。《改进的稀疏多元多项式插值算法》。载于 ISSAC 会议论文集，第 467–474 页。施普林格，计算机科学讲义 358，1988年。 [37] E. Kaltofen 和 V. Y. Pan。《抽象域上线性系统的处理器高效并行求解》。载于 SPAA 会议论文集，第 180–191 页。ACM，1991年。[38] E. Kaltofen 和 D. Saunders。《关于 Wiedemann 求解稀疏线性系统的方法》。载于 AAECC-9，计算机科学讲义第 539 卷，第 29–38 页。施普林格出版社，1991年。 [39] E. Kaltofen 和 V. Shoup。《有限域上多项式因式分解的次二次时间算法》。计算数学，67(233)：1179–1197，1998年。 [40] K. S. Kedlaya 和 C. Umans。《有限特征小的有限域上多项式因式分解的快速确定性算法》。SIAM 计算杂志，40(6)：1767–1802，2011年。[41] G. Labahn。《块类汉克尔矩阵的求逆分量》。线性代数及其应用，177：7–48，1992年。 [42] D. Lazard。《代数方程组的求解》。理论计算机科学，15(1)：77–110，1981年。 [43] D. Lazard。《理想基与初等分解：两个变量的情形》。符号计算杂志，1(3)：261–270，1985年。 [44] D. Lazard。《零维代数系统的求解》。符号计算杂志，13(2)：117–131，1992年。 [45] R. Lebreton、E. Mehrabi 和 ´E. Schost。《二元系统求解的复杂性：非奇异解的情形》。载于 ISSAC 会议论文集，第 251–258 页，2013年。 [46] G. Lecerf。《Lickteig-Roy 子结式算法的复杂性》。HAL报告，法国国家科学研究中心与 ´巴黎综合理工学院，2017年。 [47] E. Mehrabi 和 ´E. Schost。《一种求解整数系数二元多项式系统的软最优蒙特卡洛算法》。复杂性杂志，34：78–128，2016年。 [48] B. Mourrain 和 V. Y. Pan。《多元多项式、对偶性与结构化矩阵》。复杂性杂志，16 180，2000 1 110( ): – 。[49] M. Newman。《整矩阵》。学术出版社，1972年。第一版。[50] V. Y. Pan。《结构化矩阵与多项式：统一的超快速算法》。施普林格，2001年。 [51] C. Pascal 和 ´E. Schost。《二元三角集的换序》。载于 ISSAC 会议论文集，第 277–284 页。ACM出版社，2006年。 [52] C. Pernet、H. Signargout 和 G. Villard。《多项式西尔维斯特矩阵的高阶提升》。Hal-03740320，2022年。 [53] A. Poteaux 和 ´E. Schost。《模三角集的模复合及其应用》。计算复杂性，22(3)：463–516，2013年。[54] J. Rif`a 和 J. Borrell。《改进有限域中不可约多项式与本原多项式计算的时间复杂度》。载于 AAECC 会议论文集，计算机科学讲义 539，第 352–359 页，1991年。 [55] F. Rouillier。《通过有理单变量表示求解零维系统》。应用代数工程与通信计算，9：433–461，1999年。 [56] V. Shoup。《有限特征小的有限域上多项式因式分解的快速确定性算法》。载于 ISSAC 会议论文集，第 14–21 页，1991年。

[57] V. Shoup. 有限域上不可约多项式的快速构造。《符号计算杂志》，17(5):371–391，1994年。 [58] V. Shoup. 一种新的多项式因式分解算法及其实现。《符号计算杂志》，20(4):363–397，1995年。 [59] V. Shoup. 有限域代数扩张中最小多项式的高效计算。载于 ISSAC 论文集，第53–58页。ACM出版社，1999年。[60] A. Storjohann. 矩阵典范形算法。博士论文，科学计算研究所，苏黎世联邦理工学院中心，瑞士苏黎世，2000年11月。¨J. A. Thiong Ly. 关于计算大有限域中元素最小多项式的注记。载于编码理论与应用会议论文集，计算机科学讲义388，第185–192页，1989年。 [61] G. Villard. 将矩阵约化为标准形的快速并行算法。《应用代数与工程、通信和计算》，8(6):511–537，1997年。[62] G. Villard. 关于计算一般二元多项式的结式。载于 ISSAC 论文集，第391–398页。ACM出版社，2018年。[63] D. Wiedemann. 有限域上稀疏线性方程的求解。《IEEE信息论汇刊》，32(1):54–62，1986年。