arXiv:2611.32456v1 [cs.SC] 24 Nov 2026

有限域上格罗布纳基计算的求解次数与复杂度

Irene Di Muzio*和 Igor Semaev†

挪威卑尔根大学信息学系

摘要

有限域上的多元多项式方程组求解是代数密码分析中的核心问题，通常采用格罗布纳基算法。格罗布纳基计算的复杂度取决于所用算法，并由求解次数决定；求解次数定义为计算过程中所处理多项式的最高次数。因此，对这一量进行估算至关重要，相关文献中已根据正则度给出了若干界。

本文研究了 Buchberger 判据对消除冗余对的影响，并证明，结合线性代数与 Buchberger 原始算法的格罗布纳基算法，其求解次数不超过由相关多项式的首项形式所定义的正则度。这一结果为在格罗布纳基算法的复杂度估计中使用正则度提供了严格依据，也支持了代数密码分析中的一项常见假设。

我们通过确定必须处理的对数上界，进一步完善了复杂度分析。这些上界优于已发表的复杂度估计，在某些参数范围内的改进尤为显著。

关键词： Gröbner基、求解次数、正则次数、Buchberger 判据、代数密码分析、复杂度。

*irene.muzio@uib.no
†igor.semaev@uib.no

1 引言

开发高效方法来求解有限域上的多变量多项式方程组，是计算代数中的一个重要问题，并在密码学中有诸多应用。求解多项式方程组的一种经典方法是格罗布纳基计算。在 Buchberger 提出首个算法后 [1], , Lazard 建立了格罗布纳基计算与对多项式倍式构造的矩阵进行高斯消元之间的联系 [2]。更高效的格罗布纳基算法利用了这一联系，尤其是 F4 [3], F5 [4], 以及相关方法 XL [5], 和它们的所有变体。

我们研究在 $\mathbb{F}_q$ 上为多项式方程组构造格罗布纳基的复杂度

$$f_1, \ldots, f_m, x_1^q - x_1, \ldots, x_n^q - x_n. \tag{1}$$

设 $R^h = \mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^q, \ldots\ldots, x_n^q \rangle$。用 $l_q(n, d)$ 表示 R^h 中次数为 d 的单项式个数，用 $L_q(n, D) = \sum_{d=0}^{D} l_q(n, d)$ 表示次数至多为 D 的单项式个数。设 I^h 是由 $f_1, \ldots\ldots, f_m$ 的首项形式生成的 R^h 的理想，并令 V_d 表示其次数为 d 的齐次元素子空间。满足 V_d 包含 R^h 中所有次数为 d 的形式的最小正整数 d，称为方程组 (1) 的正则度，记作 d_{reg} [6]。对于 $d = d_{\mathrm{reg}}$，空间 V_d 由 R^h 中所有次数为 d 的单项式生成，因此 $\dim V_d = l_q(n, d)$。

注意，这一定义的正则度将域方程纳入了考量，尤其是通过对 R^h 的定义。因此，以这种方式定义的正则度小于在不考虑域方程的情况下对 $f_1, \ldots, f_m$ 在 $\mathbb{F}_q[x_1, \ldots, x_n]$ 中定义的正则度，前提是后者有定义。尽管如此，我们的结果同样适用于不含域方程的多项式系统，只需在普通多项式环中执行相同的构造，并使用相应的单项式数量即可。

令 d_{solv} 表示所考虑算法的求解次数，即计算过程中所处理多项式的最高次数。求解次数决定了格罗布纳基算法的计算成本，它取决于所采用的算法，通常难以直接估计。因此，求解次数的界通常用正则度来表示。正则度得到了广泛研究，尤其是对于半正则多项式系统 [7]。特别地，代数密码分析中通常用于 F4 和 F5 的复杂度估计具有 $O\left(\binom{n+d_{\mathrm{reg}}}{d_{\mathrm{reg}}}^{\omega}\right)$ 的形式，并将正则度作为求解次数的替代指标。对于齐次正则

和半正则序列 [7], ，这是合理的；而对于非齐次方程组，这通常只是一种假设。XL 的分析方式类似，以其自身的运算次数 [8], 为依据，其目标是计算一个解，而不是计算格罗布纳基。

人们提出了多种方法，将求解次数与多项式系统求解中出现的其他参数联系起来。Caminata 和 Gorla 建立了涉及 Castelnuovo-Mumford 正则性的界，并研究了求解次数、最后下降次数和正则度之间的联系 [9, 10]。

采用另一种方法，Semaev 和 Tenti 证明了在有限域上使用基于 Buchberger 的算法时的界 $d_{\mathrm{solv}} \leq 2d_{\mathrm{reg}} - 2$ ，而无需假设半正则性或一般性 [11]。随后，Salizzoni 在适当的次数假设下 [12] 建立了界 $d_{\mathrm{solv}} \leq d_{\mathrm{reg}} + 1$。

本文沿用 Semaev 和 Tenti 的方法，在正则度处构造一个中间多项式系统。利用该系统的结构，我们证明 Buchberger 第二准则可以放宽：只要第三个首项单项式整除它们的最小公倍式，就可以舍弃一个临界对；一般而言，这一条件并不足够。由此可得，所得算法满足更强的界 $d_{\mathrm{solv}} \leq d_{\mathrm{reg}}$ 。在 [12, 例 3.9], 中，我们证明界 $d_{\mathrm{solv}} \leq d_{\mathrm{reg}} + 1$ 是紧的。不过，一般来说，任何格罗布纳基算法的实现都可以像式 (5) 所示，在计算 S-多项式时省略恒等抵消的首项。特别是在本例中，这样就无需显式构造次数为 $d_{\mathrm{reg}} + 1$ 的多项式倍式。

相比之下， [12] 中的界是通过控制多项式表示的次数得到的，而我们的方法直接作用于临界对层面：引理 1 和 2 对算法如何处理临界对进行了清晰的描述。这不仅使我们能够证明次数界，还能确定需要处理的临界对，并推导出其数量的精细上界，如引理 3 所示。

Kouba、Neiger 和 Safey El Din 还利用 F4 Tracer [13]中基于 Syzygy 的版本的 Buchberger 判据，研究了冗余临界对的消除。他们的分析针对一般的零维系统，并且依赖若干假设，其中包括关于 grevlex 初始理想的猜想性质。相比之下，我们的组合分析仅使用正则次数处中间生成集的指定首项单项式，不要求一般性、猜想性质或任何特定的单项式序。

我们工作的次数界改进，以及需要处理的数对数量减少，显著降低了构造格罗布纳基的复杂度。令 $N = L_q(n, \ d_{\mathrm{reg}})$。

定理 1 表明，当 $d_{\mathrm{reg}} = o(n)$ 且 q 固定时，计算格罗布纳基的复杂度为 $O(N^{3+o(1)})$ 次 $\mathbb{F}_q$ 运算。对于其余情形 $d_{\mathrm{reg}} = \Omega(n)$，我们建立了一个一般的复杂度界 $O(N^4)$，并且在某些参数范围内，如定理 2 所示，将复杂度指数级地改进至 $O(c^n N^4)$，其中某个常数为 $c < 1$。这改进了 [11] 中 Semaev-Tenti 算法的复杂度。我们还在第2.4节回顾了 [11] 的过程，该过程用于计算方程组的一个解，或证明其无解。此过程可直接应用于由我们的算法构造的格罗布纳基；当 $q.$ 固定时，它需要额外进行 $O(nN^3)$ 次运算

在 [12] 中，已证明计算格罗布纳基的复杂度界为 $O(M^4 + Mk^{\omega-1})$，其中 k 是输入多项式的数量，且 $M = \binom{n+d_{\mathrm{reg}}+1}{d_{\mathrm{reg}}+1}$。与这些估计相比，我们的界受益于比 [12], 中更少的单项式数量，因为 $N \leq \binom{n+d_{\mathrm{reg}}}{d_{\mathrm{reg}}} < M$，并且在某些参数范围内实现了显著更低的渐近复杂度。

上述关于 F4、F5 和 XL 的复杂度估计依赖于一个未经证明的假设，即这些算法的求解次数不超过正则度。本文对所研究的算法严格证明了这一事实。我们的方法专为求解基域有限域上多项式方程组的零点而设计。因此，正则度的定义取决于域多项式，通常会得到比一般情形更小的正则度数值和复杂度。

本文中的复杂度界仅取决于多项式的首项形式，而与其低次项无关。对于当前算法，界 $d_{\mathrm{solv}} \leq d_{\mathrm{reg}}$ 实际上是等式，因为中间生成集是在次数 d_{reg} 处仅根据首项形式构造的，忽略了输入多项式的线性组合的首项形式相消时产生的低次关系。利用这些关系，可以在相同或更低的次数处得到格罗布纳基，而 d_{reg} 仍是一个上界。

在开展本研究的过程中，Di Muzio 最初研究了 Buchberger 算法的 Gebauer-Möller 实现 [14], ，并对该实现应用于 $\mathbb{F}_2$上的一类方程组时的界 $d_{\mathrm{solv}} \leq d_{\mathrm{reg}} + 1$ 给出了组合证明。随后，Semaev 发现，将消除冗余对的判据纳入 Semaev-Tenti 算法，可将该界改进为 d_{reg}，并证明了这一结果适用于 $\mathbb{F}_2$。这一方法还使得可以直接根据正则度给出复杂度估计。随后，Di Muzio 将该结果推广到任意有限域 $\mathbb{F}_q$，如第2节所述，并在第3节进行了复杂度分析。

2 改进的求解次数界

我们首先在第2.1节回顾 Semaev 和 Tenti 的构造，该构造给出了一个生成方程组，其首项具有预先指定的结构。接着，在第2.2节，我们说明如何将 Buchberger 判据用于消除该类方程组中的冗余对，从而以正则度为界限定求解次数。最后，在第2.4节，我们回顾如何在构造出格罗布纳基后计算解（如果解存在）。

2.1 多项式系统的初步构造

设 $R = \mathbb{F}_q[x_1, \ldots, x_n]$ 是有限域 $\mathbb{F}_q$ 上以 n 个变量为元的多项式环。对于由非负整数组成的 n 元组 $\alpha = (\alpha_1, \ldots\ldots, \alpha_n)$，记相应的单项式为 $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$，其总次数为 $|\alpha| = \sum_{i=1}^{n} \alpha_i$。在 R 上固定一个总次数单项式序。

设 I 是由 (1) 中的多项式生成的 R 中的理想。如 [11], 所示，可以构造 I 的一个中间生成集 B，使其具有以下两个性质。首先，B 中每个多项式的次数至多为 d_{reg}。其次，恰有 $l_q(n, d_{\text{reg}})$ 个多项式，其首项单项式遍历 R^h 中所有次数为 d_{reg} 的单项式，且其余项的次数严格更小。

当 $q > d_{\text{reg}}$ 时，域多项式 $x_i^q - x_i$ 可化简为次数小于 d_{reg} 的多项式。当 $q \le d_{\text{reg}}$ 时，基 B 显式包含这些域多项式。也就是说

$$B = \{f_\rho, f_\sigma\}_{\rho,\sigma} \cup \begin{cases} \{x_1^q - x_1, \ldots, x_n^q - x_n\}, & q \le d_{\text{reg}}, \\ \varnothing, & q > d_{\text{reg}}. \end{cases} \tag{2}$$

出现在 $\{f_\rho, f_\sigma\}_{\rho,\sigma}$ 中多项式里的每个单项式项 x^α，其中$\alpha = (\alpha_1, \ldots, \alpha_n)$，都满足 $0 \le \alpha_i < q$ 对所有 i 均成立，并且

- $f_\rho = x^\rho + g_\rho$，其中 $x^\rho, |\rho| = d_{\text{reg}}$ 是 f_ρ 的首项单项式，且 $\deg(g_\rho) < |\rho|$;
- $f_\sigma = x^\sigma + g_\sigma$，其中 $x^\sigma, |\sigma| < d_{\text{reg}}$ 是 f_σ 的首项单项式，且 $\deg(g_\sigma) \le |\sigma|$。

2.2 Buchberger 判据的应用

对于当前基中的每一对多项式 f_α，f_β，Buchberger 算法会计算 S-多项式 $S(f_\alpha, f_\beta)$ 并对其进行约化。每个非零余式都会加入基中。当所有此类

约化结果均为零时，算法终止。将 Buchberger 算法应用于 (2)，当 $q > d_{\mathrm{reg}}$ 或 $q \le d_{\mathrm{reg}}$ 时，可得到相同形式的基。

对于基中的每一对多项式 f_α，f_β，定义单项式 $x^\delta = \mathrm{lcm}(x^\alpha, x^\beta)$，其中 $\delta = \delta(\alpha, \beta) = (\delta_1, \ldots, \delta_n)$ 且 $\delta_i = \max(\alpha_i, \beta_i)$。

Buchberger 判据允许在计算过程中依据以下规则舍弃某些对 f_α，f_β。

(C1) 首项单项式 x^α 和 x^β 互素。

(C2) 存在第三个首项单项式 x^γ，其整除 x^δ，并且以下两对 (f_α, f_γ) 和 (f_γ, f_β) 均已得到处理：要么通过约化 S-多项式进行处理，要么依据 Buchberger 判据将其舍弃。

在这两种情况下，对 f_α，f_β 均称为冗余对，因此无需约化 $S(f_\alpha, f_\beta)$。

接下来的引理考察特定基 (2) 中 Buchberger 第二准则 (C2) 的组合结构，并将其转化为一种直接根据指数元组识别冗余对的策略。

引理 1. 考虑来自(2)中第一组的一个对 f_α, f_β，其中 $\alpha \neq \beta$。假设满足以下条件之一：

(i) $|\alpha| = |\beta| = d_{\mathrm{reg}}$ 和 $|\delta| \ge d_{\mathrm{reg}} + 2$;

(ii) $|\alpha| < d_{\mathrm{reg}}$ 或 $|\beta| < d_{\mathrm{reg}}$，以及 $|\delta| \ge d_{\mathrm{reg}} + 1$。

那么存在一个 n-元组 $\gamma \neq \alpha, \beta$，使得

1. $|\gamma| = d_{\mathrm{reg}}$ 和 $x^\gamma \mid x^\delta$，*2.* $\delta(\alpha, \gamma) = d_{\mathrm{reg}} + 1$ 和 $\delta(\beta, \gamma) = \delta(\alpha, \beta) - 1$。若 $|\beta| < d_{\mathrm{reg}}$，则后者在情形（*ii*）下成立。

证明。定义

$$K = \{k \in \{1, \ldots, n\} : \alpha_k < \beta_k\},$$

并选取 j 使得 $\alpha_j > \beta_j$。这样的指标 K 和 j 存在；否则一个单项式将整除另一个，这将推出 $|\delta| \le d_{\mathrm{reg}}$，与假设矛盾。

情形（i）。任取 $k \in K$，并通过设定定义 γ

$$\gamma_k = \alpha_k + 1, \qquad \gamma_j = \alpha_j - 1,$$

当 $\gamma_i = \alpha_i$ 对每个 $i \neq j$，k 都成立时。这就得到 $|\gamma| = |\alpha| = d_{\mathrm{reg}}$，并且对任意 i，$\gamma_i \le \delta_i$，因此 $x^\gamma \mid x^\delta$。显然，$\gamma \neq \alpha$。假设 $|\delta| \ge d_{\mathrm{reg}} + 2$ 确保

$\gamma \neq \beta$。这就证明了引理的第一个陈述。第二个陈述显然成立。

情形（ii）。由对称性，不妨设 $|\beta| < d_{\text{reg}}$。选取整数 γ_k，使得对于 $k \in K$

$$\alpha_k \leq \gamma_k \leq \beta_k, \qquad \sum_{k\in K}(\gamma_k - \alpha_k) = d_{\text{reg}} - |\alpha| + 1. \tag{3}$$

令 $\gamma_j = \alpha_j - 1$，并对 $i \notin K$ 和 $i \neq j$ 令 $\gamma_i = \alpha_i$。于是

$$|\gamma| = \sum_{k\in K}\gamma_k + \sum_{i\notin K}\alpha_i - 1 = \sum_{k\in K}(\gamma_k - \alpha_k) + |\alpha| - 1 = d_{\text{reg}},$$

并且逐分量地，$\gamma_i \leq \delta_i$。这样的 γ_k 的存在性由

$$|\delta| = |\alpha| + \sum_{k\in K}(\beta_k - \alpha_k) \geq d_{\text{reg}} + 1,$$

这由关于 $|\delta|$ 的假设成立。因此，$\sum_K (\beta_k - \alpha_k) \geq d_{\text{reg}} - |\alpha| + 1$，其中 $\beta_k - \alpha_k \geq 0$。所以，可以选取 γ_k，使得（3）成立。

此外，根据构造，$\gamma \neq \alpha$；并且由于 $|\gamma| = d_{\text{reg}}$，而 $|\beta| < d_{\text{reg}}$，所以 $\gamma \neq \beta$。这证明了引理的第一个结论。第二个结论显然成立。

□

引理 2。设 $f_\alpha = x_j^q - x_j$ 是（2）中的一个域多项式，并设 f_β 属于（2）中的第一个集合，且 $\beta_j > 0$。假设以下条件之一成立：

(i) $|\beta| = d_{\text{reg}}$ 和 $|\delta| \geq d_{\text{reg}} + 2$,

(ii) $|\beta| < d_{\text{reg}}$ 和 $|\delta| \geq d_{\text{reg}} + 1$。

那么存在一个 n-元组 $\gamma = (\gamma_1, \ldots, \gamma_n)$ $0 \leq \gamma_i < q$ 和 $\gamma \neq \alpha, \beta$，使得

1. $|\gamma| = d_{\text{reg}}$ *and* $x^\gamma \mid x^\delta$,
2. $\delta(\alpha, \gamma) = d_{\text{reg}} + 1$ *and* $\delta(\beta, \gamma) = \delta(\alpha, \beta) - 1$.

证明。我们采用与前一个证明类似的构造。事实上，(i) 和 (ii) 中均成立 $|\delta| = q + \sum_{k\neq j}\beta_k \geq d_{\text{reg}} + 1$。因此，$\sum_{k\neq j}\beta_k \geq d_{\text{reg}} - q + 1$。

令 $\gamma_j = q - 1$，并选择 γ 的其余坐标，使得

$$0 \leq \gamma_k \leq \beta_k \text{ for } k \neq j, \qquad \sum_{k\neq j}\gamma_k = d_{\text{reg}} - q + 1.$$

于是 $|\gamma| = d_{\mathrm{reg}}$，每个坐标都满足 $0 \le \gamma_i < q$ 和 $x^\gamma \mid x^\delta$。显然，$\gamma \neq \alpha$。

在情形（i）中，$|\delta| \ge d_{\mathrm{reg}} + 2$ 蕴含 $\beta_j \le q-2$，因此有 $\gamma_j = q-1 > \beta_j$ 和$\gamma \neq \beta$。在情形（ii）中，$\gamma \neq \beta$ 由 $|\gamma| = d_{\mathrm{reg}} > |\beta|$推出。这就证明了引理的第一条陈述。第二条陈述显然成立。 □

注 1. 引理 *1* 和 *2* 中构造的目的，是在(2)中找到一个多项式 f_γ 。因此，关于 $|\delta|$ 的界不能进一步改进。事实上，这些假设确保可以找到一个次数为 d_{reg} 的元组 γ；此外，根据构造，x^γ 是(2)中某个多项式的首项单项式。对于更小的 $|\delta|$值，可以构造次数为 $< d_{\mathrm{reg}}$的元组 γ，但无法保证 x^γ 会作为方程组中的首项单项式出现。

正如 Buchberger [15], 所观察到的，第三个首项单项式整除最小公倍式的存在性通常不足以舍弃一个临界对。然而，生成集 (2) 的特殊结构使我们能够证明，辅助对可以递归地约化为由我们的算法选取的对，具体如下。

命题 1. 满足引理 *1* 或引理 *2* 的条件 *(i)* 或 *(ii)* 的对 (f_α, f_β) 是冗余的。

证明。考虑这样的一个对 (f_α, f_β)，并令 $\delta = \delta(\alpha, \beta)$。根据前述引理，存在第三个元组 γ，使得 $|\gamma| = d_{\mathrm{reg}}$ 且 $x^\gamma | x^\delta$。在所有情形下，我们都有

$$|\delta(\gamma, \alpha)| = d_{\mathrm{reg}} + 1, \qquad |\delta(\gamma, \beta)| = \delta(\alpha, \beta) - 1. \tag{4}$$

接下来，我们将证明可根据判据 (C2) 丢弃 (f_α, f_β)。我们对 $|\delta(\alpha, \beta)|$ 进行归纳，以证明辅助对 (f_γ, f_α) 和 (f_γ, f_β) 不满足这些引理的条件（因此应予处理），或者它们自身可依据判据 (C2) 丢弃，也可能需要借助更多辅助对。我们考虑两种情况。

1. 令 $|\delta(\alpha, \beta)| = d_{\mathrm{reg}} + 1$。首先假设 f_α, f_β 均不是域多项式。若 $|\alpha| = |\beta| = d_{\mathrm{reg}}$，则该对不满足引理 1 的条件 (i)。

   因此，$|\alpha|$，$|\beta|$ 中至少有一个必须小于 d_{reg}。由对称性，$|\beta| < d_{\mathrm{reg}}$。由于根据（4），$\delta(\gamma, \beta) = d_{\mathrm{reg}}$，因此数对 (f_γ, f_β) 不满足这些引理的条件。

   考虑（f_γ，f_α）。我们有 $|\gamma| = d_{\mathrm{reg}}$和 $|\delta（\gamma, \alpha）| = d_{\mathrm{reg}} + 1$。如果$|\alpha| = d_{\mathrm{reg}}$，那么（$f_\gamma$，$f_\alpha$）的首项单项式次数为 d_{reg} 和

$|\delta(\gamma,\ \alpha)| = d_{\mathrm{reg}} + 1$。因此，$(f_\gamma,\ f_\alpha)$ 不满足这些引理的条件。

设 $|\alpha| < d_{\mathrm{reg}}$，对 (f_γ, f_α) 应用引理 1 的构造，我们得到一个元组 γ'，其中 $|\gamma'| = d_{\mathrm{reg}}$ 且

$$\delta(\gamma, \gamma') = d_{\mathrm{reg}} + 1, \qquad \delta(\gamma', \alpha) = d_{\mathrm{reg}}.$$

两个辅助对 $(f_{\gamma'}, f_\gamma)$ 和 $(f_{\gamma'}, f_\alpha)$ 均不满足这些引理的条件。因此，(C2) 允许丢弃 (f_γ, f_α)，从而也丢弃 (f_α, f_β)。

现假设 $f_\alpha = x_j^q - x_j$ 是一个域多项式。由于 $|\delta(\alpha,\beta)| = d_{\mathrm{reg}}+1$，引理 2 的条件 (i) 不能成立。因此该对必须满足条件 (ii)，从而 $|\beta| < d_{\mathrm{reg}}$。引理 2 中 γ 的构造给出 $\gamma_j = q - 1$，以及 $|\gamma| = d_{\mathrm{reg}}$，并且 $\delta(\gamma,\alpha) = d_{\mathrm{reg}} + 1$。因此 (f_γ, f_α) 不满足这些引理的条件。此外，由 (4) 可知 $\delta(\gamma,\beta) = d_{\mathrm{reg}}$。所以，$(f_\gamma, f_\beta)$ 不满足这些引理的条件。

2. 令 $|\delta(\alpha,\beta)| \geq d_{\mathrm{reg}} + 2$。由 (4)，我们有

$$\delta(\gamma,\alpha) < |\delta(\alpha,\beta)|, \qquad \delta(\gamma,\beta) < |\delta(\alpha,\beta)|,$$

因此，两个辅助对 (f_γ, f_α) 和 (f_γ, f_β) 的最小公倍数次数都严格较小。根据归纳假设，每个辅助对要么不满足引理的条件，要么自身可由判据 (C2) 舍弃。因此，判据 (C2) 也适用于 (f_α, f_β)。

□

2.3 新算法

对于一个 n 元组 α，令 $\mathrm{supp}(\alpha) = \{i :\ \alpha_i > 0\}$。

1. 从 (1) 出发，根据 [11]，按照 (2) 构造基 B。
2. 令 $f_\alpha \neq f_\beta$ 属于当前基，且 $\mathrm{supp}(\alpha) \cap \mathrm{supp}(\beta) \neq \varnothing$。假设其中一个

- $|\alpha| = |\beta| = d_{\text{正则度}}$ 与 $|\delta(\alpha,\beta)| = d_{\text{正则度}} + 1$，
- $|\alpha|$ 或 $|\beta| < d_{\text{正则度}}$ 与 $|\delta(\alpha,\ \beta)| \leq d_{\text{正则度}}$，
- $f_\alpha = x_j^q - x$，以及 $|\beta| = d_{\text{正则度}}$，以及 $|\delta(\alpha,\ \beta)| = d_{\text{正则度}} + 1$，
- $f_\alpha = x_j^q - x$，以及 $|\beta| < d_{\text{正则}}$，以及 $|\delta(\alpha,\ \beta)| \leq d_{\text{正则}}$。

然后对当前基取模，化简 $S(f_\alpha,\ f_\beta)$。将余数加入基中并重复此过程。

3. 如果所有余式都为零，则终止。

方程组 (2) 仅包含首项单项式次数为$\leq d_{\mathrm{reg}}$的多项式。每当 S-多项式的余式非零时，其次数为$< d_{\mathrm{reg}}$，并将其加入基中。我们可以假设，在算法的每一步中，基中的多项式都是线性无关的。在整个算法过程中，当$q > d_{\mathrm{reg}}$时，基至多由 $N = L_q(n, d_{\mathrm{reg}})$ 个多项式组成；而当 $q \leq d_{\mathrm{reg}}$ 时，至多由 $N + n$ 个多项式组成。

该算法构造了一个格罗布纳基，且从未产生次数高于 d_{reg} 的多项式。事实上，将一个 S-多项式重写为

$$S_{\alpha,\beta} = S(f_\alpha, f_\beta) = \frac{x^\delta}{x^\alpha} f_\alpha - \frac{x^\delta}{x^\beta} f_\beta = \frac{x^\delta}{x^\alpha} g_\alpha - \frac{x^\delta}{x^\beta} g_\beta, \tag{5}$$

注意到 $\deg(S_{\alpha,\beta}) \leq \max\{|\delta| - |\alpha| + \deg(g_\alpha),\ |\delta| - |\beta| + \deg(g_\beta)\}$。根据 (2) 中的构造，当 $|\rho| = d_{\mathrm{reg}}$ 时，$\deg(g_\rho) < |\rho|$；而当$|\sigma| < d_{\mathrm{reg}}$时，$\deg(g_\sigma) \leq |\sigma|$。因此，

$$\deg(S_{\alpha,\beta}) \leq \begin{cases} |\delta| - 1, & \text{if } |\alpha| = |\beta| = d_{\mathrm{reg}}, \\ |\delta|, & \text{if } |\alpha| < d_{\mathrm{reg}} \text{ or } |\beta| < d_{\mathrm{reg}}. \end{cases}$$

这意味着对于除 $f_\alpha = x_j^q - x$、 $q < |\beta| = d_{\mathrm{reg}}$ 和 $|\delta(\alpha,\ \beta)| = d_{\mathrm{reg}} + 1$ 之外的所有情况，$\deg(S_{\alpha,\ \beta}) \leq d_{\mathrm{reg}}$。然而，在这种情况下 $\beta_j = q - 1$ and

$$S_{\alpha,\beta} = -x_j \prod_{i \neq j} x_i^{\beta_i} - x_j g_\beta.$$

由于 $\deg(g_\beta) < d_{\mathrm{reg}}$ and $q \geq 2$，我们得到

$$\deg(S_{\alpha,\beta}) \leq \max\{d_{\mathrm{reg}} - q + 2,\ 1 + \deg(g_\beta)\} \leq d_{\mathrm{reg}}.$$

因此，算法选取的每个 S-多项式的次数至多为 d_{reg} .

得益于上述修改，算法仅约化次数为 $\leq d_{\mathrm{reg}}$ 的多项式，而所添加的余式次数为 $< d_{\mathrm{reg}}$。每次迭代后，方程组保持结构 (2)。算法以求解次数 $\leq d_{\mathrm{reg}}$. 终止

2.4 计算一个解

一旦构造出格罗布纳基，就可以通过

[11, 定理 2.2]中描述的过程，求出由式 (1) 中的多项式定义的方程组的一个解，或证明该方程组无解。通过删除冗余的首项单项式并约简其余多项式，将该基转换为约化 Gröbner 基，这需要 $O(N^3)$ 次域运算。若约化后的基为 $\{1\}$，则方程组无解；否则，通过添加线性多项式 $x_i - a_i$ 并更新 Gröbner 基，迭代地为变量赋值$a_i \in \mathbb{F}_q$，同时舍弃会得到基 $\{1\}$ 的赋值。每次更新需要 $O(N^3)$ 次域运算。由于最多测试 qn 个赋值，额外开销为 $O(qnN^3)$；当q 固定时，该开销可简化为 $O(nN^3)$。对于固定的 q，若存在解，则求解的开销可计入定理 1 中给出的构造格罗布纳基的复杂度界。

3 构造 Gröbner基的复杂度

本节根据第2节中的算法，估计由多项式系统 (2) 构造格罗布纳基的复杂度。我们将所得界限与 Semaev 和 Tenti [11] 的算法所得到的界限进行比较。我们的改进既源于较低的求解次数，也源于应用 Buchberger 判据后需要处理的配对数量减少。

假设所有参数 q、d_{reg} 和 n 都可能增长。设 $d_{\mathrm{reg}} \geq 2$。注意，d_{reg} 受约束 $d_{\mathrm{reg}} \leq n(q-1)$。事实上，$R^h$ 中的每个单项式在每个变量上的指数至多为 $q-1$，因此其次数至多为 $n(q-1)$。我们还假设 (1) 中的每个多项式 f_i 的次数至多为 d_{reg}。否则，对于每个满足 $\deg(f_i) > d_{\mathrm{reg}}$ 的 f_i，先将其替换为除以 (2) 中多项式后所得的余式，额外代价为 $O\big(L_q(n,\ \deg(f_i))\, L_q(n,\ d_{\mathrm{reg}})\big)$。为简化记号，在本节全文中令 $D = d_{\mathrm{reg}}$ 且 $N = L_q(n,\ D)$。

[11] 中介绍的算法由两个主要阶段组成。第一阶段确定正则度，并通过 Macaulay 三角化构造基（2），同时对域多项式进行必要的约化。该阶段的复杂度上界为 $O(D^2N^4 + qN^2)$ 次域运算。第二阶段对（2）中的多项式应用朴素的 Buchberger 算法，以构造格罗布纳基。其复杂度上界为 $O(N^6)$，通过跟踪已经处理的 S-多项式，可以将其降低至 $O(N^5)$。下文的比较采用后一个上界。

对于当前算法，根据第2节，待处理的每个 S-多项式的次数为$\leq D$，并且将其除以当前基中的多项式，而这些多项式的次数同样为 $\leq D$。因此，单次约化至多需要

$O(N^2)$ 次域运算。此外，该算法不必处理全部 $\binom{N}{2} = O(N^2)$ 个可能的有序对。根据引理 1，只需处理至多 $N_1 + N_2$ 个不涉及域多项式的有序对。用 N_1 表示式 (2) 中满足 $\mathrm{supp}(\alpha) \cap \mathrm{supp}(\beta) \neq \varnothing$ 且 $|\alpha| = |\beta| = D$ 的无序对 $f_\alpha \neq f_\beta$ 的数量，并且 $|\delta| = D+1$.用 N_2 表示满足 $\mathrm{supp}(\alpha) \cap \mathrm{supp}(\beta) \neq \varnothing$ 且 $|\delta| \leq D$. 的无序对 $f_\alpha \neq f_\beta$ 的数量。

此外，仅当 $q \leq D$ 时，才需要考虑涉及域多项式的对。由于共有 n 个域多项式，且每个域多项式至多可与来自 $\{f_\rho, f_\sigma\}_{\rho的\sigma}$ 个多项式配对，因此它们的总数上界为 $\mathbf{1}_{\{q \leq D\}} nN$。这一粗略上界已足够，因为其贡献会被吸收到下面推导出的渐近上界中。

Let

$$\rho = \frac{N_1 + N_2 + \mathbf{1}_{\{q \leq D\}} nN}{N^2},$$

其取决于 n、D和 q，因此第二阶段的复杂度变为 $O(\rho N^4)$。我们在定理 1 中证明，在 $D = o(n)$ 的情况下，ρ 的衰减会带来进一步改进；与 [11] 中此前的 $O(N^5)$ 上界相比，该复杂度将接近降低 N 的两个幂次。

我们首先在第 3.1 节中估计 N_1 和 N_2。在第 3.2 节中，我们将这些上界与第一阶段经过细化的开销结合起来，分析不同情况下的复杂度，并展示相较于此前上界的改进。最后，我们在第 3.3 节中给出完整算法的内存复杂度。

3.1 已处理对的数量

设 $l_c(n, d) = |\{(\alpha_1, \ldots, \alpha_n) : \sum_i \alpha_i = d,\ 0 \leq \alpha_i < c\}|$ 对任意 $c \geq 1$。为简化下文中的记号，我们假设 $\alpha = (\alpha_1, \ldots, \alpha_n)$ $0 \leq \alpha_i < q$以及 $\beta = (\beta_1, \ldots, \beta_n)$ $0 \leq \beta_i < q$。因此，$\delta = \delta(\alpha, \beta) = (\delta_1, \ldots, \delta_n)$ 和 $\delta_i = \max(\alpha_i, \beta_i)$。此外，令 $\gamma = \gamma(\alpha, \beta) = (\gamma_1, \ldots, \gamma_n)$，其中 $\gamma_i = \min(\alpha_i, \beta_i)$。最后，令 $B_q(z) = \sum_{j=0}^{q-1} (2j+1) z^j$.

以下引理根据上一节的冗余结果，给出了已处理对数量的界。如前所述，只要满足 $q \leq D$，涉及域多项式的对就会被纳入。下文所用的界足以进行复杂度分析。相应的精确计数公式，以及涉及域多项式的对的一个更精细的界，见附录 A。

引理 3。

$$N_1 \leq \binom{n}{2} l_q(n, D-1), \qquad N_2 \leq \frac{1}{2} \sum_{t=1}^{D} [z^t] B_q(z)^n.$$

证明。 我们首先统计对 N_1 有贡献且不涉及域多项式的对。由于 $|\alpha| = |\beta| = D$ 和 $|\delta| = D+1$， 平凡恒等式$|\gamma| + |\delta| = |\alpha| + |\beta|$ 给出 $|\gamma| = D-1$. 因此，存在两个不同的指标 i， j，使得 $\alpha = \gamma + e_i$ 且 $\beta = \gamma + e_j$。 对于每个次数为 $D-1$的指数元组 γ，不同坐标的选择至多有 $\binom{n}{2}$ 种。因此，我们采用如下界

$$\binom{n}{2} l_q(n, D-1).$$

现在我们统计对 N_2 有贡献且不涉及域多项式的有序对。固定 δ. 对于一个坐标，满足 $\max(\alpha_i, \beta_i) = \delta_i$的有序对 (α_i, β_i) 数量为 $(\delta_i+1)^2 - \delta_i^2 = 2\delta_i + 1$. 因此，与此类 δ 对应的有序对 (α, β) 数量为 $\prod_{i=1}^{n}(2\delta_i+1)$。 展开 $B_q(z)^n$ 可得

$$[z^t]B_q(z)^n = \sum_{\substack{|\delta|=t \\ 0 \le \delta_i < q}} \prod_{i=1}^{n} (2\delta_i + 1),$$

因此，满足 $0 < |\delta| \le D$ 的有序对数量为

$$\sum_{t=1}^{D} [z^t]B_q(z)^n.$$

□

3.2 复杂度的改进

回顾一下，第二阶段的复杂度为 $O(\rho N^4)$。令 $T(n, D, q)$ 表示第一阶段中 Macaulay 三角化的代价，并令 $R(n, D, q)$ 表示当 $q > D$时进行域多项式约简所需的额外代价。因此，当前算法的总复杂度上界为

$$O\left(T(n, D, q) + R(n, D, q) + \rho N^4\right). \tag{6}$$

现在，我们推导 $T(n, D, q)$ 和 $R(n, D, q)$ 的精细界。

第一阶段通过依次构造并对 $d \le D$ 的 Macaulay 矩阵进行三角化，确定正则度 D；这些矩阵由 (1) 中多项式的首项形式在 R^h 中构成。在次数 d 时，将次数为 $k \le d$ 的每个形式分别乘以次数为 $d-k$ 的单项式，即可得到各行。在次数 D 时，行约简会产生覆盖次数为 D 的所有单项式的首项形式。追踪原始多项式的相同线性组合，即可得到用于构造基 (2) 的多项式。因此

这一阶段的主要计算是对这些 Macaulay 矩阵进行三角化。

上文引用的来自 [11] 的界 $O(D^2N^4)$ 是通过对其行数和列数使用一致上界得到的。为了与新的第二阶段复杂度进行比较，更精确地保留其按次数划分的维数是有益的。

令 r_d 表示次数为 $d \leq D$ 时 Macaulay矩阵的行数。根据线性无关性假设，次数为 k 的输入多项式至多有 $l_q(n,\ k)$ 个，每个输入多项式分别乘以 $l_q(n,\ d-k)$ 个次数为 $d-k$ 的单项式。因此

$$r_d \leq \sum_{k=1}^{d} l_q(n,k) l_q(n,d-k) \leq l_q(2n,d).$$

由于次数为 d 的 Macaulay矩阵 有 $c_d = l_q(n,\ d)$ 列，其三角化需要

$$O\left(l_q(2n,d) l_q(n,d)^2\right)$$

次域运算。在次数 D 下，通过选取 c_D 个线性无关的行，并将所得 $c_D \times c_D$ 矩阵的逆矩阵应用于相应的非齐次多项式，可以构造出 (2) 中的多项式 f_ρ 。这需要额外进行 $O(c_D^2 N)$ 次域运算。由于 $N \leq l_q(2n,\ D)$，该成本可由次数为 D 的三角化界吸收。对所有次数求和得到

$$T(n,D,q) = O\left(\sum_{d=0}^{D} l_q(2n,d) l_q(n,d)^2\right) = O\left(L_q(2n,D) L_q(n,D)^2\right). \quad (7)$$

当 $q > D$ 时，还必须根据已计算出的基约化 n 域多项式。在一次除法过程中，出现的首项单项式具有 $x_i^b x^a$ 的形式，其中 $0 \leq b \leq q$ 和 x^α 是剩余 $n-1$ 个变量中的一个次数为 $< D$ 的单项式，因此最多有 $(q+1) L_q(n-1, D-1)$ 个；每个约化步骤都涉及一个基多项式 f_ρ，其中至多包含 $L_q(n, D-1)$ 个 $+1$ 单项式。因此，所有约化至多需要 $O\left(nqL_q(n,D-1)^2\right)$ 次运算。由于 $q > D$，指数上限在次数 D 之前不起作用，因此

$$N = \binom{n+D}{D}, \quad L_q(n,D-1) = \binom{n+D-1}{D-1} = \frac{D}{n+D} N.$$

由此可得

$$R(n,D,q) = O\left(\mathbf{1}_{\{q>D\}} qn \left(\frac{D}{n+D}\right)^2 N^2\right). \quad (8)$$

在定理 1 中，我们证明了精细化的 Macaulay 贡献 $T(n,\ D,\ q)$ 已包含在 ρN^4 的界中。然而，为了计算总复杂度，仍必须考虑额外的域多项式约化代价 $R(n,\ D,\ q)$。特别是，当 q 增大时，这一贡献可能占主导地位。另一方面，在假设 q 固定的情况下，与其他步骤的代价相比，代价 $R(n,\ D,\ q)$ 可以忽略不计。

现在，我们分别估计两种情形 $D = o(n)$ 和 $D = \Omega(n)$ 下的这些贡献。前者表示 $D/n \to 0$，后者表示对于某个常数 $c > 0$ 以及所有充分大的 n，都有 $D \geq cn$ 。在前一种情形下，我们得到更精确的复杂度界；在后一种情形下，我们给出更一般的估计。附录 B 对 $D = \Omega(n)$ 情形进行了更精细的分析，并在某些范围内取得了进一步改进。

定理 1。 算法的总复杂度满足以下界。

(i) 若 $D = o(n)$ 且 $D \to \infty$:

$$O\left(N^{3+o(1)} + \mathbf{1}_{\{q>D\}} q \frac{D^2}{n} N^2\right).$$

(ii) 如果 $D = O(1)$:

$$O(n^{3D+1} + \mathbf{1}_{\{q>D\}} q n^{2D-1}).$$

(iii) *If* $D = \Omega(n)$*:*

$$O(N^4 + \mathbf{1}_{\{q>D\}} q n\, N^2).$$

证明。 回顾总复杂度界 $O(T(n,\ D,\ q) + R(n,\ D,\ q) + \rho N^4)$ 。我们分别估计两种情形下的三项贡献。首先，通过对 N_1 和 N_2 进行界定来估计 $\rho = (N_1 + N_2 + \mathbf{1}_{\{q \leq D\}} nN)/N^2$ ；它们由引理（ 3 ）计算得出。随后，我们估计 $T(n,\ D,\ q)$。 贡献项 $R(n,\ D,\ q)$ 可直接由（8）得出。

（*i*） D 随 n的增长呈次线性。
为估计 $N_1 \leq \binom{n}{2} l_q(n,\ D-1)$，我们证明

$$l_q(n, D-1) \leq \frac{D}{(n-D+1)} l_q(n, D).$$

事实上，考虑从 γ到 $\gamma + e_i$的所有可容许增量。由于 $|\gamma| = D-1$， γ 中至多有 $\lfloor \frac{D-1}{q-1} \rfloor \leq D-1$ 个坐标等于 $q-1$。因此，每个 γ 至少有 $n-D+1$ 个增量。另一方面，每个次数为 D 的元组至多可能来自 D 个元组，每个正坐标对应一个。因此 $(n-D+1) l_q(n, D-1) \leq D\, l_q(n, D)$。由于 $D = o(n)$ 且 $N = (1 + O(D/n)) l_q(n, D)$，我们有 $N_1 = O(nDN)$。

对于 $N_2 \le \frac{1}{2}\sum_{t=1}^{D}[z^t]B_q(z)^n$，回想一下，

$$[z^t]B_q(z)^n = \sum_{\substack{|\delta|=t \\ 0\le\delta_i<q}} \prod_{i=1}^{n}(2\delta_i+1).$$

由于对于每个非负整数 a，$2a+1 \le 3^a$，因此 $\prod_{i=1}^{n}(2\delta_i+1) \le 3^{|\delta|}$。因此，

$$N_2 \le \frac{1}{2}\sum_{t=1}^{D} 3^t l_q(n,t) \le \frac{3^D}{2}N.$$

项 $\mathbf{1}_{\{q\le D\}}nN$ 被吸收到 $O(nDN)$。综上可得

$$\rho = O\left(\frac{nD+3^D}{N}\right). \tag{9}$$

我们有

$$nD + 3^D \le D^2 N^{1/D} + 3^D \le 2\cdot 3^D N^{1/D},$$

因为 $N \ge (n/D)^D$ 且 $D^2 \le 3^D$。此外，$3^D = N^{o(1)}$，因为

$$\frac{\log(3^D)}{\log N} \le \frac{\log 3}{\log(n/D)} \longrightarrow 0.$$

将其代入 (9)，可知当 $D \to \infty$ 时，项 $\rho N^4 = O(N^{3+o(1)})$。

现在我们估计 $T(n,D,q) = O(N^2 L_q(2n,D))$。由于 $L_q(2n,D) \le \binom{2n+D}{D}$ 且 $N \ge l_q(n,D) \ge \binom{n}{D}$，我们有

$$\frac{L_q(2n,D)}{N} \le \frac{\binom{2n+D}{D}}{\binom{n}{D}} = \prod_{k=0}^{D-1} 2\left(1+\frac{D+k}{2(n-k)}\right).$$

使用 $1+x \le e^x$ 和 $n-k \ge n-D+1$，我们得到

$$\frac{L_q(2n,D)}{N} \le 2^D \exp\left(\frac{1}{2(n-D+1)}\sum_{k=0}^{D-1}(D+k)\right) \le 2^D \exp\left(\frac{D^2}{n-D+1}\right).$$

因此

$$T(n,D,q) = O\left(2^D \exp\left(\frac{D^2}{n-D+1}\right)N^3\right) = O(3^D N^3),$$

因为对于 $D = o(n)$，$\exp\left(\binom{D^2}{n-D+1}\right) \le (3/2)^D$。

有 $T(n,\ D,\ q) + \rho N^4 = O(N^{3+o(1)})$。加上贡献项$R(n,\ D,\ q) = O(\mathbf{1}_{\{q>D\}} qD\, N^2)$，这就证明了 (i) 中的第一个界。

（*ii*） D 有界的情形。

此情形可由情形（i）中的估计推出。这里，对于每个 d，$l_q(n,\ d) = O(n^d)$，因此 $N = O(n^D)$。将此代入（9）即可证明断言（ii）。

（*iii*） $D = \Omega(n)$的情形。

显然，$N_1 \le \binom{n}{2} l_q(n,\ D-1) \le n^2 N$。此外，由于 $|\delta(\alpha,\ \beta)| \le D$ 蕴含$|\alpha|, |\beta| \le D$，根据 B_q 的系数解释可得

$$N_2 \le \frac{1}{2} \sum_{t=1}^{D} [z^t] B_q(z)^n \le \frac{N^2}{2}.$$

再加上 $\mathbf{1}_{\{q\le D\}} nN$的贡献，

$$\rho \le \frac{n^2 N + N^2/2 + nN}{N^2} \le \frac{1}{2} + O\left(\frac{n^2}{N}\right) \le \frac{1}{2} + o(1),$$

因为 N 随 n呈指数增长。事实上，由于存在常数 $c > 0$，使得当 n充分大时 $D \ge cn$ 成立，取 $0 < c_< \min\{c, 1\}$，我们有

$$N \ge \binom{n}{\lfloor c_0 n \rfloor} \ge \left(\frac{1}{c_0}\right)^{\lfloor c_0 n \rfloor}.$$

此外，$T(n,\ D,\ q) = O(N^2 L_q(2n,\ D)) = O(N^4)$，因为 $L_q(2n,\ D) \le L_q(n,\ D)^2$。将这些估计与 $R(n,\ D,\ q) = O\left(\mathbf{1}_{\{q>D\}} qnN^2\right)$结合起来，即可证明 (iii)。

□

3.3 内存复杂度

现在，我们根据所存储的 $\mathbb{F}_q$ 元素数量，估算第2.3节所述算法的内存需求。我们将考察 Macaulay 三角化以及第一阶段中域多项式约化所需的存储空间（如第 3.2 节所述），以及第二阶段中格罗布纳基和已处理的配对所需的存储空间。

Macaulay 矩阵可以逐步进行三角化，每次处理一行。每个新行都用先前各行进行约简，且仅当它与先前各行线性无关时才予以存储。由于有 $l_q(n,\ d)$ 列，因此至多有 $l_q(n,\ d)$ 个主元，次数为 d 时所需的存储空间为 $O(l_q(n,\ d)^2)$。

在次数为 D 时，我们从齐次 Macaulay 矩阵中选取 $l_q(n,\ D)$ 个线性无关的行，构成可逆矩阵 C。将相同行对应的低次项纳入考虑，可得到矩阵 $[C \mid E]$。乘以 C^{-1} 后得到 $[I_{l_q(n,\ D)} \mid C^{-1}E]$，其各行表示多项式 $f_\rho = x^\rho + g_\rho$，且 $\deg g_\rho < D$。这部分重构需要 $O(l_q(n,\ D)N)$ 的内存。重构还会考虑多项式 f_σ，其首项单项式的次数为 $< D$。此类多项式至多有 $L_q(n,\ D-1)$ 个，每个最多包含 N 个单项式；存储这些多项式还需要 $O(L_q(n,\ D-1)N)$ 的额外空间。对方程组 (2) 进行整体重构需要 $O(N^2)$ 的内存。

因此，按次数逐步处理时，Macaulay 三角化及其重构所需的内存为

$$O\left(\max_{d\le D} l_q(n,d)^2 + N^2\right) = O(N^2).$$

当 $q > D$ 时，域多项式的约化可以逐个进行。由于每个中间多项式至多包含 $qL_q(n-1, D-1)$ 个单项式，这些约化至多需要

$$O\left(qL_q(n-1, D-1)\right)$$

额外存储空间。

在第二阶段，当前格罗布纳基至多包含 N 个多项式，每个多项式至多包含 N 个单项式，因此需要 $O(N^2)$ 的存储空间。至多需要考虑 $N_1+N_2+\mathbf{1}_{\{q\le D\}}nN$ 对。用索引对表示它们至多需要 $O(N^2)$ 的额外存储空间。

因此，总体内存复杂度的上界为

$$O\left(N^2 + \mathbf{1}_{\{q>D\}} qL_q(n-1, D-1)\right).$$

对于固定的 q，第二项可被前一项吸收，因此内存复杂度为 $O(N^2)$。

参考文献

[1] Bruno Buchberger。 一种用于寻找关于零维多项式理想的剩余类环的基元素的算法。博士论文，因斯布鲁克大学，1965 年。

[2] Daniel Lazard。格罗布纳基、高斯消元与代数方程组的求解。载于 J. A. van Hulzen 编，计算机代数：*EUROCAL 1983*，《计算机科学讲义》第 162 卷，第 146–156 页。Springer，1983 年。

[3] Jean-Charles Faugère。计算格罗布纳基的一种高效新算法（F4）。《纯粹与应用代数杂志》，139(1–3)：61–88，1999 年。[4] Jean-Charles Faugère。无需归约为零即可计算格罗布纳基的一种高效新算法（F5）。载于*2002* 年国际符号与代数计算研讨会论文集，第 75–83 页。ACM，2002 年。[5] Nicolas Courtois、Alexander Klimov、Jacques Patarin 和 Adi Shamir。求解多元多项式超定方程组的高效算法。载于密码学进展 – *EUROCRYPT 2000*，《计算机科学讲义》第 1807 卷，第 392–407 页。Springer，2000 年。[6] Magali Bardet、Jean-Charles Faugère 和 Bruno Salvy。 $\mathbb{F}_2$ 上具有 $\mathbb{F}_2$解的半正则超定序列的格罗布纳基计算复杂度。研究报告 5049，INRIA，2003 年。

[7] Magali Bardet、Jean-Charles Faugère 和 Bruno Salvy。关于半正则超定代数方程格罗布纳基计算复杂度的研究。载于多项式系统求解国际会议，第 71–74 页，2004 年。

[8] Jenny Yuan-Chun Yeh、Chen-Mou Cheng 和 Bo-Yin Yang。关于变量数与方程数呈线性关系的 F_4/F_5 一般 $\mathcal{MQ}$，XL 与求解次数。在 Marc Fischlin 和 Stefan Katzenbeisser 编，数论与密码学：纪念 *Johannes Buchmann 60* 岁生日论文集，计算机科学讲义第 8260 卷，第 19–33 页。Springer，柏林、海德堡，2013 年。[9] Alessio Caminata 和 Elisa Gorla。多元多项式方程组的求解与交换代数中的一个不变量。在 有限域算术：*WAIFI 2020*，计算机科学讲义第 12542 卷，第 3–36 页。Springer，2021 年。[10] Alessio Caminata 和 Elisa Gorla。求解次数、最后下降次数及相关不变量。《符号计算杂志》，114：322–335，2023 年。[11] Igor Semaev 和 Andrea Tenti。有限域上 Macaulay 矩阵的概率分析与构造 Gröbner基的复杂度。《代数杂志》，565：651–674，2021 年。

[12] Flavio Salizzoni。根据正则度给出求解次数的上界。《数学密码学汇刊》，5(1)：1–7，2025 年。[13] Robin Kouba、Vincent Neiger 和 Mohab Safey El Din。带有追踪器数据的 F4 格罗布纳基算法的复杂度分析，2026年。[14] Rüdiger Gebauer 和 H. Michael Möller。关于 Buchberger 算法的一种实现。《符号计算杂志》，6(2)：275–286，1988 年。[15] Bruno Buchberger。构造 Gröbner基时检测不必要约化的判据。在 E. W. Ng 编，符号与代数计算，第 3–21 页。Springer，1979 年。[16] Bruno Buchberger。Gröbner基：多项式理想理论中的一种算法方法。在 N. K. Bose 编，多维系统理论，第 184–232 页。D. Reidel 出版公司，多德雷赫特，1985 年。

A 已处理对的精确计数公式

在本附录中，我们记录引理 3 所依据的更精确计数公式，以及等价的生成函数表示，并给出涉及域多项式的对数量的更精确上界。对于 N_1，下面的公式给出了对的确切数量。对于 N_2，该公式给出候选对的最坏情况数量，其假设计数中出现的每个可接受单项式都是算法可用的某个多项式的首项单项式；因此， N_2 的实际值可能更小。

A.1 对 N_1 的贡献

回想一下，对于一个对 N_1 有贡献的条件 $|\alpha| = |\beta| = D$和 $|\delta| = D + 1$, 可得 $|\gamma| = D - 1.$ 。因此，存在两个不同的指标 i， j，使得 $\alpha_i = \gamma_i + 1$, $\beta_j = \gamma_j + 1$，且 $0 \le \gamma_i$， $\gamma_j \le q - 2$。若 $\gamma_i + \gamma_j = k$，则此类 γ_i， γ_j 的可能取值数为 $l_{q-1}(2,\ k)$，而 γ 中剩余的 $n-2$ 个元素的总次数为 $D-1-k$，可通过 $l_q(n-2,\ D-1-k)$ 种方式选取。由于 i， j 有 $\binom{n}{2}$ 种可能取值，我们得到对的精确数量

$$\binom{n}{2} \sum_{k=\max\{0,D-1-(n-2)(q-1)\}}^{\min\{D-1,2(q-2)\}} l_{q-1}(2,k)\, l_q(n-2, D-1-k).$$

下限和上限恰好是确保被加数中的两个因子均非零的条件。也就是说，$0 \le k \le 2(q-2)$ 且 $0 \le D-1-k \le (n-2)(q-1)$。

等价地，利用系数提取，同一数量可写为

$$\binom{n}{2}[z^{D-1}]\left(\sum_{a=0}^{q-2} z^a\right)^2\left(\sum_{a=0}^{q-1} z^a\right)^{n-2}.$$

A.2 对 N_2有贡献的数对

我们证明了与 δ 对应的有序对（α，β）的数量为$\prod_{i=1}^{n}(2\delta_i+1)$。令 $s=|\operatorname{supp}(\delta)|.$。在这些有序对中，恰有 2^s 个支集不相交，必须将其移除。事实上，对于每个 $i \in \operatorname{supp}(\delta)$，必须选择（$\alpha_i$，$\beta_i$）为（$\delta_i$，$0$）或（$0$，$\delta_i$）。还要移除数对 $\alpha=\beta=\delta.$。因此，支集不相交且最大值等于 δ 的无序不同数对的数量为

$$\frac{1}{2}\left(\prod_{i=1}^{n}(2\delta_i+1)-2^s-1\right).$$

另请注意，在上述计数中，两个多项式中至少有一个的次数严格小于 D 这一条件自动成立。

对所有次数不超过 D 的非零指数元组 δ 求和，得到

$$\frac{1}{2}\sum_{\substack{0<|\delta|\le D\\ 0\le\delta_i<q}}\left(\prod_{i=1}^{n}(2\delta_i+1)-2^{|\operatorname{supp}(\delta)|}-1\right).$$

对于等价的生成函数表示，定义

$$A_q(z)=\sum_{j=0}^{q-1} z^j, \qquad B_q(z)=\sum_{j=0}^{q-1}(2j+1)z^j, \qquad C_q(z)=1+2\sum_{j=1}^{q-1} z^j.$$

于是，$B_q(z)^n$ 按照其逐坐标最大值的次数统计所有有序对，$C_q(z)^n$ 统计支集不相交的有序对，而 $A_q(z)^n$统计对角对。因此，前述数量等价于

$$\frac{1}{2}\sum_{t=1}^{D}[z^t]\left(B_q(z)^n-C_q(z)^n-A_q(z)^n\right).$$

A.3 涉及域多项式的对

剩下需要统计涉及域多项式的有序对。只有当 $q \le D$时，才需要考虑这类有序对。涉及两个不同域多项式的有序对具有互素的首项单项式，根据布赫伯格判据（C1）可以舍弃。

考虑由首项单项式为 x_j^q 的域多项式和首项单项式为 x^β 的多项式组成的一对。要使这两个支集相交，必须有 $1 \le \beta_j \le q-1$。此外，

$$|\delta| = q + \sum_{i \ne j} \beta_i.$$

根据引理 2，只有在 $|\delta| \le D$，或$|\beta| = D$ 和 $|\delta| = D+1$时，才需要考虑这样的一对。

在第一种情况下，条件 $|\delta| \le D$ 等价于

$$\sum_{i \ne j} \beta_i \le D - q.$$

对于固定的 j， β_j有 $q-1$ 种选择，其余坐标至多有 $L_q(n-1,\ D-q)$ 种选法。对 n 个域多项式求和可得

$$n(q-1)L_q(n-1, D-q).$$

在第二种情况下，由于 $|\beta| = D$ 且 $|\delta| = D+1$ 蕴含 $\beta_j = q-1$，因此有

$$\sum_{i \ne j} \beta_i = D - q + 1.$$

对于固定的 j，最多有 $l_q(n-1,\ D-q+1)$ 个可能的 β。因此，这恰好贡献

$$n\, l_q(n-1, D-q+1)$$

对。

因此，涉及一个域多项式的所选对的数量至多为

$$\mathbf{1}_{\{q \le D\}}\, n\left((q-1)L_q(n-1, D-q) + l_q(n-1, D-q+1)\right).$$

B 正则度的大幅指数级改进

关于人工智能使用的声明。 我们使用 ChatGPT（OpenAI，GPT-5.6 Sol）作为工具，探索本节所述结果的其他证明策略。

最终的数学论证由作者提出并验证，作者对其正确性承担全部责任。

回顾一下，总复杂度有界于 $O(T(n,\ D,\ q)+R(n,\ D,\ q)+\rho N^4)$，其中 $N = L_q(n,\ D)$ $\rho = (N_1 + N_2 + \mathbf{1}_{\{q\le D\}}\, nN)/N^2$ 且

$$T(n,D,q) = O\left(N^2 L_q(2n,D)\right), \quad R(n,D,q) = O\left(\mathbf{1}_{\{q>D\}}\frac{nqD}{n+D}N^2\right).$$

我们在范围 $\frac{1}{2} \le \lambda \le \theta_q - \varepsilon$，内改进了 $D = \Omega(n)$ 的复杂度界，其中

$$\lambda = \frac{D}{n(q-1)}, \qquad \theta_q = \frac{4q+1}{6q},$$

且 $\varepsilon > 0$ 为固定值。

定理 2。 在上述范围内，算法的总复杂度为O（$c^n N^4$） ，其中某个常数 $c < 1$ 与 n 和 q无关。

证明。 分量映射

$$(\alpha_1, \ldots, \alpha_n) \mapsto (q-1-\alpha_1, \ldots, q-1-\alpha_n)$$

对的指数元组的次数之和为 $n(q-1)$。因此，至少一半的所有 q^n 元组的次数不超过 $n(q-1)/2$。因此 $N \ge q^n/2$，因为 $\lambda \ge 1/2$。

令 α 和 β 为 $\{0, \ldots, q-1\}^n$ 中相互独立且均匀分布的指数元组，并设 $X_i = \max(\alpha_i, \beta_i)/(q-1)$。变量 X_i 相互独立，属于 $[0,1]$, ，且满足 $\mathbb{E}[X_i] = \theta_q$。事实上，对于固定的坐标 i，恰有 $2j+1$ 个有序对 (α_i, β_i) 满足 $\max(\alpha_i, \beta_i) = j,\ 0 \le j < q$。因此，$\Pr(\max(\alpha_i, \beta_i) = j) = (2j+1)/q^2$, 于是

$$\mathbb{E}[X_i] = \frac{1}{q^2(q-1)}\sum_{j=0}^{q-1} j(2j+1) = \theta_q.$$

根据 Hoeffding不等式,

$$\Pr\left(\sum_{i=1}^{n} X_i \le n\lambda\right) \le \exp\left(-2n(\theta_q - \lambda)^2\right) \le e^{-2\varepsilon^2 n}.$$

回顾一下， $B_q(z) = \sum_{j=0}^{q-1}(2j+1)z^j$，并且对于每个 t，系数 $[z^t]B_q(z)^n$ 统计满足 $\sum_{i=1}^{n}\max(\alpha_i, \beta_i) = t.$ 的指数元组有序对 (α, β)。由于 $\sum_{i=1}^{n}\max(\alpha_i, \beta_i) = (q-1)\sum_{i=1}^{n} X_i$ 且 $D = n(q-1)\lambda,$，因此

$$\sum_{t=0}^{D}[z^t]B_q(z)^n = q^{2n}\Pr\left(\sum_{i=1}^{n} X_i \le n\lambda\right).$$

因此，

$$\frac{1}{2}\sum_{t=1}^{D}[z^t]B_q(z)^n \le \frac{1}{2}q^{2n}e^{-2\varepsilon^2 n}.$$

利用 (3) 和 $N \ge q^n/2$，我们得到

$$\rho = \frac{N_1+N_2}{N^2} \le 2e^{-2\varepsilon^2 n} + O\left(\frac{n^2}{N}\right) = O(e^{-2\varepsilon^2 n}).$$

为估计贡献 $T(n,\ D,\ q)$，令 $Y_i = (\alpha_i + \beta_i)/(q-1)$。这些变量相互独立，属于 $[0,2],$，且均值为 1。由于 $\lambda \le \theta_q \le 3/4$，Hoeffding不等式给出

$$\begin{aligned} L_q(2n, D) &= q^{2n}\Pr\left(\sum_{i=1}^{n} Y_i \le n\lambda\right) \\ &\le q^{2n}\exp\left(-\frac{n}{2}(1-\lambda)^2\right) \\ &\le q^{2n}e^{-n/32} \le 4N^2 e^{-n/32}. \end{aligned}$$

因此，$T(n,\ D,\ q) = O(e^{-n/32}N^4)$。

最后，$\lambda \ge 1/2$ 意味着当 n 足够大时，$q \le D$ 成立，因此用于约化域多项式的额外代价 $R(n,\ D,\ q)$ 消失。结合这两个阶段，对于某个 $c < 1$，得到 $O(c^n N^4)$。

□