arXiv:2304.13485v1 [math.AC] 26 Apr 2023

正则度意义下求解次数的上界

Flavio Salizzoni

摘要

求解次数是估算求解多项式方程组复杂度的重要参数。本文给出了正则度意义下求解次数的一个上界，并证明该上界是最优的。由此可直接推出最后下降次数和 Macaulay 界的一个上界。

1 引言

许多问题都可以建模为多项式方程组。一旦已知该方程组的约化 Gr¨obner 基，就可以在多项式时间内找到这类方程组的解。目前，已有许多计算 Gr¨obner 基的算法，其中效率最高的算法属于基于线性代数的算法这一类。该类算法包括 F4、F5 和 XL 算法等 [6, 7, 8]。由于这些算法应用于后量子密码学，其计算复杂度的估算变得愈发重要。

给定一个用于求解多项式方程组 $\mathcal{F}$的基于线性代数的算法 H，相对于 H 的 $\mathcal{F}$ 求解次数，定义为使用 H求解 $\mathcal{F}$ 时出现的多项式的最高次数。人们关注这一参数，是因为它的上界可以给出这些算法复杂度的上界。然而，显式计算求解次数通常极其困难。因此，根据其他参数（如正则度、最后下降次数和 Castelnuovo-Mumford 正则性）给出求解次数的上界很有用。例如，在 [11] 中，Huang、Kosters、Yang 和 Yeo 描述了一种求解多项式系统的算法，其复杂度以上界最后下降次数为界。在 [4], 中，Caminata 和 Gorla 证明，对于一个族 $\mathcal{F} = \{f_1, \dots, f_k\}$，其求解次数不超过该族 $\mathcal{F}^h = \{f_1^h, \dots, f_k^h\}$的 Castelnuovo-Mumford 正则性，其中 f_i^h是 f_i的齐次化。

正则度 $\mathrm{d_{reg}}(\mathcal{F})$ 由 Bardet、Faug`ere 和 Salvy 在 [1, 9], 中引入，他们还为密码学半正则序列的这一次数提供了一个上界。尽管许多作者将正则度作为求解次数的启发式上界，但这两个参数之间的确切关系尚不完全清楚。例如，参见 [4,Examples 4.7] 和 [2, Examples 2.2、2.3 及 2.4]。在 [15, 16], 中，Semaev 和 Tenti 证明，在某些条件下，求解次数由 $2\mathrm{d_{reg}}(\mathcal{F}) - 2$ 从上方界定（参见 [16, Corollary 3.67] 以及 [15, Theorem 2.1] 下方的讨论）。

本文考虑一族算法的求解次数 sd_σ，其中包括 MutantXL [3] 和 MXL2 [14] 等算法。主要结果是以下关于正则度的求解次数上界。

定理 1.1. 设 $\mathcal{F} = \{f_1, \dots, f_n\}$ 为一个多项式族，使得 $\max \deg(f_i) \leq \mathrm{d_{reg}}(\mathcal{F})$，并设 σ 为一个次数相容项序。则，$\mathrm{sd}_\sigma(\mathcal{F}) \leq \mathrm{d_{reg}}(\mathcal{F}) + 1$。

我们证明此界是最优的：对于每个 $1 < d \in \mathbb{N}$，都存在一个多项式族 $\mathcal{F}$，使得 $\mathrm{d_{reg}}(\mathcal{F}) = d$，且 $\mathrm{sd}_\sigma(\mathcal{F}) = d + 1$。根据定理 1.1，我们得到最后下降次数总是有正则度作为上界。最后，我们改进了正则度有限的多项式族的 Macaulay界。

2 预备知识

设 $\mathbb{K}$ 是一个域（不一定是有限域）。对于 $\mathbb{K}[x_1,\dots,x_n]$ 中的理想 $\mathcal{I}$，我们用 $\mathcal{I}_d$ 表示 $\mathcal{I}$ 中次数为 d 的所有齐次多项式的集合。设 $\mathcal{F}=\{f_1,\dots,f_k\}$ 是一个由 $\mathbb{K}[x_1,\dots,x_n]$ 构成的有限族，并设 $\langle\mathcal{F}\rangle$ 是由 $\mathcal{F}$ 生成的理想。

定义 2.1. 固定一个项序 σ。我们用 $\mathrm{Gbd}_\sigma(\mathcal{F})$ 表示关于 σ 的 $\langle\mathcal{F}\rangle$ 的约化 Gr¨obner 基中元素的最大次数。

现在回顾正则度的定义，该定义最初由 Bardet、Faug`ere 和 Salvy 在 [1, 9] 中给出。对于多项式 $p\in\mathbb{K}[x_1,\dots,x_n]$，令 p^{top} 为 p 的最高次数齐次部分。

定义 2.2. $\mathcal{F}$ 的正则度 $\mathrm{d}_{\mathrm{reg}}(\mathcal{F})$ 是满足下式的最小整数 d

$$\left(\langle\mathcal{F}^{\mathrm{top}}\rangle\right)_d=(\mathbb{K}[x_1,\dots,x_n])_d,$$

其中 $\mathcal{F}^{\mathrm{top}}=\left\{f_1^{\mathrm{top}},\dots,f_{\mathrm{top}_k}\right\}$。若不存在这样的 d，则令 $\mathrm{d}_{\mathrm{reg}}(\mathcal{F})=+\infty$。

注 2.3. 若项序 σ 是次数相容的，则 $\mathrm{Gbd}_\sigma(\mathcal{F})\le\mathrm{d}_{\mathrm{reg}}(\mathcal{F})$，正如 Caminata 和 Gorla 在 [4, 注 4.6] 中已观察到的那样。

对于一个族 $\mathcal{F}$，另一个重要参数是最后下降次数，该参数最早由 Huang、Kosters 和 Yeo 在 [12] 中定义。

Defi义 2.4. 对于整数 d，我们将 $V_{\mathcal{F},\,d}$ 记作关于 t 的最小 $\mathbb{K}$-线性空间 o 包含关系，使得

- $\{f\in\mathcal{F}:\ \deg(f)\le d\}\subseteq V_{\mathcal{F},\,d}$,
- 对于 $\mathbb{K}[x_1,\dots,x_n]$ 中的每个 m 单项式，以及满足 $\deg(mf)\le d$ 的每个 $f\in V_{\mathcal{F},\,d}$，则 $mf\in V_{\mathcal{F},\,d}$。

我们设定 $V_{\mathcal{F},\,+\infty}=\langle\mathcal{F}\rangle$。最后下降次数 $\mathrm{Lfd}(\mathcal{F})$ 是满足以下条件的最小 $d\in\mathbb{Z}_{>0}\cup\{+\infty\}$：对于所有 $f\in\langle\mathcal{F}\rangle$，都有 $f\in V_{\mathcal{F},\,\max\{d,\deg(f)\}}$。

求解次数通常从 Macaulay矩阵 $M(\mathcal{F},d)$ 出发定义，并向其中添加若干行，显式讨论可参见 [10, 第 2 节2]。不过，就本文的目的而言，直接用空间$V_{\mathcal{F},\,d}$来定义求解次数更为方便。请注意，正如 [10, 定理 1]所示，以下定义与标准定义等价。

Defi义 2.5。设 σ 为一个次数相容项序。$\mathcal{F}$ 的求解次数 $\mathrm{sd}_\sigma(\mathcal{F})$ 是满足以下条件的最小 e smal d：使得 $V_{\mathcal{F},\,d}$ 包含 $\langle\mathcal{F}\rangle$ 关于 σ的一个 Gr¨obner 基。

在 [5], 中，Caminata 和 Gorla 证明了以下结果，揭示了求解次数与最后下降次数之间的关系。

The理 2.6. 设 $\mathcal{F}$ 是一个多项式系统，且 σ 是一个次数相容项序。 n

$$\mathrm{sd}_\sigma(\mathcal{F})=\max\{\mathrm{Lfd}(\mathcal{F}),\mathrm{Gbd}_\sigma(\mathcal{F})\}.$$

关于求解次数、正则度和最后下降次数的更详细讨论，请参阅 [4, 5]。

3 定理 1.1 的证明

从现在起，设 $\mathcal{F}=\{f_1,\dots,f_k\}$ 是 $\mathbb{K}[x_1,\dots,x_n]$ 中的一个多项式族，使得对所有 $1\le i\le k$，$\mathrm{d}_{\mathrm{reg}}(\mathcal{F})=d<+\infty$ 且 $\deg(f_i)\le d$。

引理 3.1. 对于每个 m 次数为 d 的单项式，都存在$p\in V_{\mathcal{F},\,d}$ 使得 $p^{\mathrm{top}}=m$.

证明. 由于 d 是 $\mathcal{F}$ 的正则度，存在 $m_1, \ldots, m_k$ 个单项式，使得 $\sum_{i=1}^{k} m_i f_i^{\mathrm{top}} = m$、$m_i \neq 0$，并且对于所有 $1 \leq i \leq k$ 都有 $\deg(m_i f_i) \leq d$。令 $p = \sum_{i=1}^{k} m_i f_i$。显然，$\deg(p) = \deg(m) = d$，$p \in V_{\mathcal{F},\, d}$，且 $p^{\mathrm{top}} = m$。 □

令 $D = \binom{d+n-1}{d}$，并令 $\mathcal{P}_{\mathcal{F}} = \{p_1, \ldots, p_D\} \subseteq V_{\mathcal{F},\, d}$ 为一个集合，使得对于每个次数为 d 的首一单项式 m，存在 $1 \leq i \leq D$ 使得 $p_i^{\mathrm{top}} = m$。由引理 3.1 可知 $\mathcal{P}_{\mathcal{F}}$ 的存在性。注意到 $\mathcal{P}_{\mathcal{F}} \subseteq V_{\mathcal{F},\, d+1}$，因为 $V_{\mathcal{F},\, d} \subseteq V_{\mathcal{F},\, d+1}$。

¯引理 3.2。对于每个次数为 d 的 $f \in V_{\mathcal{F},\, d+1}$，存在 a_1、……、$a_D \in \mathbb{K}$ 和 $f \in V_{\mathcal{F},\, d+1}$，满足 $\deg(\bar{f}) < d$，使得 $f = \bar{f} + \sum_{i=1}^{D} a_i p_i$，其中 $p_i \in \mathcal{P}_{\mathcal{F}}$。

证明。由于 $\langle p_1^{\mathrm{top}}$、……、$p_D^{\mathrm{top}} \rangle_{\mathbb{K}} = \mathbb{K}[x_1, \ldots, x_n]_d$，存在 a_1、……、$a_d \in \mathbb{K}$，使得 $f - \sum_{i=1}^{D} a_i p_i =$ ¯f 的次数严格小于 d。
由于 f、p_1、……、$p_D \in V_{\mathcal{F},\, d+1}$，我们也可得出 $f \in V_{\mathcal{F},\, d+1}$。 □

我们用 $\mathscr{P}_{\mathrm{fin}}(\mathbb{K}[x_1, \ldots, x_n]^3)$ 表示 $\mathbb{K}[x_1, \ldots, x_n]^3$ 的所有有限子集构成的集合。现在定义 A_d 为 $\mathscr{P}_{\mathrm{fin}}(\mathbb{K}[x_1, \ldots, x_n]^3)$ 的一个子集，并给出其元素的具体描述。集合 $\{(m_1, a_1, g_1) \ldots, (m_\ell, a_\ell, g_\ell)\} \in A_d$ 当且仅当满足以下条件：

- 恰有一个元素使得 $m_i = 1$。为简单起见，我们假设 $m_1 = 1$。那么，$a_1 = 1$ 且 $g_1 \in V_{\mathcal{F},\, d+1}$，
- $m_2, \ldots, m_\ell$ 是次数至少为 2 的首一单项式，
- a_2、……、$a_\ell \in \mathbb{K} \setminus 0$ 和 g_2、……、$g_\ell \in \mathcal{P}_{\mathcal{F}}$，
- 若 $m_i = m_j$，则 $g_i \neq g_j$。

对于 X，我们将 $Y \in A_d$ 定义如下。如果 $(1, 1, f_x) \in X$ 且 $(1, 1, f_y) \in Y$，那么 $(1, 1, f_x + f_y) \in X \oplus Y$。此外，对于次数至少为 2 的 m，我们有 $(m, a, p) \in X \oplus Y$ 当且仅当且仅当以下情况之一发生：

- $(m, a, p) \in X$，并且对于所有 $b \in \mathbb{K} \setminus 0$，我们有 $(m, b, p) \notin Y$，
- $(m, a, p) \in Y$，并且对于所有 $b \in \mathbb{K} \setminus 0$，我们有 $(m, b, p) \notin X$，
- 存在 $(m, b, p) \in X$ 和 $(m, c, p) \in Y$，使得 $a = b + c \neq 0$.

L引理 3.3. 我们有，$(A_d, \oplus)$ 是一个阿贝尔群，其单位元为 $\{(1, 1, 0)\}$。

证明。$\oplus$ 是结合的且交换的，这一事实源于 $+$ 在 $\mathbb{K}$ 上是结合的且交换的。此外，根据定义显然，对于所有 $X \in A_d$，都有 $\{(1, 1, 0)\} \oplus X = X$。最后，设 $X = \{(1, 1, f_x), (m_2, a_2, g_2) \ldots, (m_\ell, a_\ell, g_\ell)\} \in A_d$，那么集合 $\{(1, 1, -f_x), (m_2, -a_2, g_2) \ldots, (m_\ell, -a_\ell, g_\ell)\}$ 也是 A_d 的一个元素。我们将这个集合记为 $-X$。容易验证，$X \oplus -X = \{(1, 1, 0)\}$。 □

对于 $X = \{(1, 1, f_x), (m_2, a_2, g_2) \ldots (m_\ell, a_\ell, g_\ell)\} \in A_d$ 以及 $a \in \mathbb{K}$，我们将 $a \star X$ 定义为

$$a \star X = \begin{cases} \{(1, 1, af_x), (m_2, aa_2, g_2), \ldots (m_\ell, aa_\ell, g_\ell)\} & a \neq 0 \\ \{(1, 1, 0)\} & a = 0 \end{cases}$$

显然，我们有 $a \star X \in A_d$。还可以验证，$(A_d, \oplus, \star)$ 是 $\mathbb{K}$ 上的向量空间。

对于 $X \in A_d$，我们将 X 的次数定义为 $\deg(X) = \max\deg(m_i g_i)$。由 $\oplus$ 和 $\star$ 的定义可直接得到以下引理。

引理 3.4. 设 X、$Y \in A_d$ 和 $0 \neq a \in \mathbb{K}$，则 $\deg(X \oplus Y) \leq \max\{\deg(X), \deg(Y)\}$，且 $\deg(a \star X) = \deg(X)$。

对于 $f \in \mathbb{K}[x_1, \ldots, x_n]$，令 $A_{d,\ f}$ 为 A_d 的子集，其定义为

$$A_{d,f} = \left\{ \{(m_1, a_1, g_1), \ldots, (m_\ell, a_\ell, g_\ell)\} \in A_d : \sum_{i=1}^{\ell} m_i a_i g_i = f \right\}.$$

注意到集合 $A_{d,\ f}$（其中 $f \in \mathcal{F}$）构成了 $A_d = \bigsqcup_f A_{d,\ f}$的一个划分。下面的引理说明了运算 $\oplus$ 和 $\star$ 如何作用于这一划分。由于证明是直接的，我们将其略去。

Le引理 3.5。设 $X \in A_{d,\ f_x}$、$Y \in A_{d,\ f_y}$和 $0 \neq a \in \mathbb{K}$。则 $X \oplus Y \in A_{d,\ f_x+f_y}$ 以及 $a \star X \in A_{d,\ af_x}$.

我们现在的目标是证明，对于每个 $f \in$ （$\mathcal{F}$），相应的 $A_{d,\ f}$ 非空。 o achi为证明这一结果，我们还需要最后一个引理。

引理 3.6。设 m 是一个首一单项式。若 $f \in V_{\mathcal{F},\ d+1}$ 且 $\deg(f) \leq d$，则存在 $X \in A_{d,\ mf}$，使得 $\deg(X) = \deg(mf)$。

证明。我们对 $\deg(mf)$ 使用归纳法。若 $\deg(mf) \leq d+1$，由于 $f \in V_{\mathcal{F},\ d+1}$，我们有 $mf \in V_{\mathcal{F},\ d+1}$，因此 $X = \{(1, 1, mf)\} \in A_{d,\ mf}$。现在假设 $\deg(mf) > d+1$。若 $\deg(f) < d$，则存在 m_1、m_2 这两个首一单项式，使得 $m = m_1 m_2$ 且 $\deg(m_1 f) = d$。由于 $m_1 f \in V_{\mathcal{F},\ d+1}$，不失一般性，我们可以假设 $\deg(f) = d$。

根据引理 3.2，我们写作 $f = \bar{f} + \sum_{i=1}^{D} a_i p_i$，其中 $\deg(\bar{f}) < d$。根据归纳假设，存在 $\bar{X} \in A_{d,\ m\bar{f}}$ 使得 $\deg(\bar{X}) \leq \deg(m\bar{f})$。令 $f' = \sum_{i=1}^{D} a_i p_i$。显然，$X' = \{(1, 1, 0)\} \cup \{(m, a_i, p_i) : a_i \neq 0\} \in A_{d,\ mf'}$ 并且 $\deg(X') = \deg(mf')$。由于 $mf = mf + mf'$，根据引理 3.5，我们得出 $X \oplus X' \in A_{d,\ mf}$ 并且 $\deg(X \oplus X') = \max\{\deg(mf), \deg(mf')\} = \deg(mf)$。 □

命题 3.7. 设 $f \in (\mathcal{F})$，则 $A_{d,\ f} \neq \emptyset$。

证明。由于 $f \in (\mathcal{F})$，存在 $q_1, \ldots, q_k \in \mathbb{K}[x_1, \ldots, x_n]$ 使得 $f = \sum q_i f_i$。每个 $q_i f_i$ 都可以写成 $\sum m_{i,\ j} a_{i,\ j} f_i$，其中 $m_{i,\ j}$ 是首一单项式。由于对每个 i, j，$\deg(a_{i,\ j} f_i) \leq d$，由引理 3.6 可得存在 $X_{i,\ j} \in A_{d,\ a_{i,\ j} m_{i,\ j} f_i}$。由引理 3.5 可得 $\sum_{i,\ j} X_{i,\ j} \in A_{d,\ f}$。 □

下一个定理是证明定理 1.1 的关键。

定理 3.8. 若 $f \in (\mathcal{F})$ 且 $\deg(f) \leq d+1$，则 $f \in V_{\mathcal{F},\ d+1}$。

证明。令 $\delta = \min_{X \in A_{d,\ f}} \deg X$，且 $A_\delta = \{X \in A_{d,f} : \deg(X) = \delta\}$。由命题 3.7 可知 $A_{d,\ f} \neq \emptyset$，因此 $A_\delta \neq \emptyset$。对于 $X, Y \in A_\delta$，若 X 中出现的最大首一单项式小于 Y 中出现的最大首一单项式（按次数字典序，满足：$x_1 > x_2 > \cdots > x_n$），则称 $X \leq Y$。令 $X = \{(m_1, a_1, g_1) \ldots, (m_\ell, a_\ell, g_\ell)\}$ 是按照此序的 A_δ 的一个极小元素。若 $\delta \leq d+1$，则 $X = \{(1, 1, f)\}$，这意味着 $f \in V_{\mathcal{F},\ d+1}$。

若 $\delta \geq d+2$，例如，假设 $m_2 = x_1^{b_1} \ldots x_n^{b_n}$ 是 X 中满足 $\deg(\bar{g}_2) < d$ 的单项式中按 $g_2 = x_1^{c_1} \ldots x_n^{c_n} + \bar{g}_2$ 排列最大的。由于 $\deg(f) \leq d+1$，存在一个指标 i，使得 $(m_i g_i)^{\mathrm{top}} = (m_2 g_2)^{\mathrm{top}}$ 且 $m_i < m_2$。这意味着

$$\bar{i} = \min\{i : b_i \neq 0\} < \max\{j : c_j \neq 0\} = \bar{j}.$$

设 $p \in \mathcal{P}_{\mathcal{F}}$ 满足 $p^{\mathrm{top}} = x_1^{c_1} \ldots x_{\bar{i}}^{c_{\bar{i}}+1} \ldots x_{\bar{j}}^{c_{\bar{j}}-1}$ 和 $m = x_{\bar{i}}^{b_{\bar{i}}-1} \ldots x_{\bar{j}}^{b_{\bar{j}}+1} \ldots x_n^{b_n}$。那么，我们可以将 f 写成

$$f = \sum a_i m_i g_i + a_2 mp - a_2 mp = x_{\bar{i}}^{b_{\bar{i}}-1} \ldots x_{\bar{j}}^{b_{\bar{j}}} \ldots x_n^{b_n} a_2 (x_{\bar{i}} g_2 - x_{\bar{j}} p) + \sum_{i \neq 2} a_i m_i g_i + a_2 mp.$$

注意到 $\deg(x_{\bar{i}} g_2 - x_{\bar{j}} p) \leq d$，且 $g = x_{\bar{i}} g_2 - x_{\bar{j}} p \in V_{\mathcal{F},d+1}$ 因为 $g_2, p \in V_{\mathcal{F},d_0}$。因此，根据引理 3.6，存在 $X_1 \in A_{d, a_2 x_{\bar{i}}^{b_{\bar{i}}-1} \ldots x_{\bar{j}}^{b_{\bar{j}}} \ldots x_n^{b_n} g}$，使得 $\deg(X_1) \leq \delta - 1$。令 $h = \sum_{i \neq 2} a_i m_i g_i$，则 $X_2 = \{(1, 1, 0), (m_3, a_3, g_3) \ldots, (m_\ell, a_\ell, g_\ell)\} \in A_{d,h}$，且 $\deg(X_2) \leq \delta$。显然 $X_3 = \{(1, 1, 0), (m, a_2, p)\} \in A_{d, a_2 mp}$。根据引理 3.5，$X_1 \oplus X_2 \oplus X_3 \in A_{d,f}$。由于 m 小于m_2，以下情况之一成立：

- $X_1 \oplus X_2 \oplus X_3$ 中的最大单项式等于 X中的最大单项式，但 i t 出现的次数严格更少，
- $X_1 \oplus X_2 \oplus X_3$ 中的最大单项式小于 X中的最大单项式。

由于在每一步中，等于 m_2 的单项式数量都严格减少，重复这一过程˜有限次后，我们可以在A_d中找到一个 X , $_f$ 其最大单项式小于 X的最大单项式。这与 X的最小性矛盾。因此，我们得出 $\delta \leq d+1$ ，从而$f \in V_{\mathcal{F},\ d+1}$。 □

此时，定理 1.1 的证明是直接的。

定理 1.1 的证明。如果 $\mathrm{d}_{\mathrm{reg}}(\mathcal{F}) = +\infty$，则该结论显然成立。否则，根据注 2.3，我们知道 $\mathrm{Gbd}_\sigma(\mathcal{F}) \leq \mathrm{d}_{\mathrm{reg}}(\mathcal{F})$。然后，根据定理 3.8，我们得到，属于约化 Gr¨obner 基的每个元素都在$V_{\mathcal{F},\ d+1}$中。 □

下一个例子表明，定理 1.1 中的界是最优的。

例 3.9. 设 $1 < k \in \mathbb{N}$，并令 $\mathcal{F}_k = \{x^k + y, y^k + x, xy\}$ 为 $\mathbb{K}[x_1, \ldots, x_n]$ 中的一族多项式。我们有 $\mathcal{F}_k^{\mathrm{top}} = \{x^k, y^k, xy\}$，因此 $\mathrm{d}_{\mathrm{reg}}(\mathcal{F}_k) = k$。注意到

$$x = -y^{k-1}(x^k + y) + (y^k + x) + x^{k-1}y^{k-2}(xy),$$

因此 $x \in (\mathcal{F}_k)$。由对称性，我们同样得到 $y \in (\mathcal{F}_k)$。特别地，对于每个项序，$\{x, y\}$ 是 $\mathcal{F}_k$ 的一个约化 Gröbner 基。在一方面，我们观察到 $xy \notin V_{\mathcal{F}_k,\ k}$。另一方面，我们有

$$y^2 = y(x^k + y) - x^{k-1}(xy) \in V_{\mathcal{F}_k,k+1} \implies x = (y^k + x) - y^{k-2}(y^2) \in V_{\mathcal{F}_k,k+1} \implies y \in V_{\mathcal{F}_k,k+1}.$$

因此，$\{x, y\} \subseteq V_{\mathcal{F}_k,\ k+1}$。这意味着，无论选择何种次数相容项序 σ，都有 $\mathrm{sd}_\sigma(\mathcal{F}_k) = k + 1 = \mathrm{d}_{\mathrm{reg}}(\mathcal{F}_k) + 1$。

下一个命题将定理 1.1 推广到了任意多项式族。

命题 3.10. 设 $\mathcal{F} = \{f_1, \ldots, f_k\}$ 是一个多项式族，且 σ 是一个与次数相容的项序。则，

$$\mathrm{sd}_\sigma \leq \max\{\mathrm{d}_{\mathrm{reg}}(\mathcal{F}) + 1, \deg(f_1), \ldots, \deg(f_k)\}.$$

证明. 设 $\mathcal{F} = \{f_1, \ldots, f_k\}$ 是一个多项式族，$t = \max \deg(f_i)$，并设 $\mathrm{d}_{\mathrm{reg}}(\mathcal{F}) < t$。我们用 $\mathrm{LT}(f)$ 表示 f 的首项。如果存在指标 i、j 以及一个单项式 m，使得 $\mathrm{LT}(f_i) = m\mathrm{LT}(f_j)$，则用 $f_i - mf_j$ 替换 f_i。以此方式继续进行，经过有限步后，我们得到一个族 $\mathcal{F}' = \{f_1', \ldots, f_s'\} \subseteq V_{\mathcal{F},\ t}$，使得 $(\mathcal{F}') = (\mathcal{F})$，并且对于每一对指标 i、j，都有 $\mathrm{LT}(f_i) \nmid \mathrm{LT}(f_j)$。这意味着 $\max \deg(f_i') \leq \mathrm{d}_{\mathrm{reg}}(\mathcal{F}') = d' \leq \mathrm{d}_{\mathrm{reg}}(\mathcal{F})$。根据定理 1.1，$V_{\mathcal{F}',\ d'+1}$ 包含 $\mathcal{F}'$ 的一个 Gr¨obner 基。由于 $(\mathcal{F}) = (\mathcal{F}')$，$d' < t$，并且 $\mathcal{F}' \subseteq V_{\mathcal{F},\ t}$，我们得出 $V_{\mathcal{F},\ t}$ 包含 $\mathcal{F}$ 的一个 Gr¨obner 基。 □

作为前一个命题的直接推论，我们得到最后下降次数的以下上界。

推论 3.11. 设 $\mathcal{F} = \{f_1, \ldots, f_n\}$ 为一个多项式族。那么，

$$\mathrm{Lfd}(\mathcal{F}) \leq \max\{\mathrm{d}_{\mathrm{reg}}(\mathcal{F}) + 1, \deg(f_1), \ldots, \deg(f_k)\}.$$

证明. 根据定理 2.6 和命题 3.10，我们得到

$$\mathrm{Lfd}(\mathcal{F}) \leq \max\{\mathrm{Lfd}(\mathcal{F}), \mathrm{Gbd}_\sigma(\mathcal{F})\} = \mathrm{sd}_\sigma(\mathcal{F}) \leq \max\{\mathrm{d}_{\mathrm{reg}}(\mathcal{F}) + 1, \deg(f_1), \ldots, \deg(f_k)\}. \quad \square$$

在下一个推论中，我们给出求解次数的一个上界，该上界关于变量的数量和方程组中元素的次数均为线性 $\mathcal{F}$。

推论 3.12（Macaulay界）。设 $\mathcal{F} = \{f_1, \ldots, f_k\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ 是一个多项式方程族，其次数至少为 1，满足 $\mathrm{d_{reg}}(\mathcal{F}) < \infty$ （因此 $k \geq n$）。令 $d_i = \deg(f_i)$，并假设 $d_1 \geq d_2 \geq \cdots \geq d_k$。那么，对于任意次数相容项序 σ

$$\mathrm{sd}_\sigma(\mathcal{F}) \leq d_1 + \cdots + d_n - n + 2.$$

证明。由于 $\mathrm{d_{reg}}(\mathcal{F}) < \infty$，存在 $J = \{j_1, \ldots, j_n\} \subseteq [k]$ 使得 $\mathrm{d_{reg}}(\mathcal{F}) \leq d_{j_1} + \ldots d_{j_n} - n + 1$。由于我们假设 $d_1 \geq d_2 \geq \cdots \geq d_k$，因此 $\mathrm{d_{reg}}(\mathcal{F}) \leq d_1 + \ldots d_n - n + 1$。此外，对于每个 $f \in \mathcal{F}$，我们有

$$\deg(f) \leq d_1 \leq d_1 + (d_2 - 1) + \cdots + (d_n - 1) = d_1 + \ldots d_n - n + 1.$$

应用命题 3.10，我们得出结论。 □

Macaulay界最初由 Lazard 在 [13, 定理 3] 中证明，用于约化 Gr¨obner 基中元素的最大次数，其中该基属于 $\mathcal{F}$。注意，我们的界（在适用时）更强。事实上，它只取决于 n 多项式的次数，而 Lazard 的界取决于 $n + 1$ 多项式的次数。 [4,推论 3.25]给出了一个类似但较弱的界。

最后，我们给出一个显式上界，用正则度来表示求解一个多项式方程组的简化 Gr¨obner 基（相对于次数相容项序）的复杂度。例如，使用 MutantXL、MXL2 等算法及其类似变体时，这个上界同样适用。

命题 3.13. 设 $\mathcal{F} = \{f_1, \ldots, f_k\} \subseteq \mathbb{K}[x_1, \ldots, x_n]$ 是一个满足 $\deg(f_i) \leq \mathrm{d_{reg}}(\mathcal{F}) = d$的族。那么，在 $\mathbb{K}$中，可以通过 $\mathcal{O}\left((n+1)^{4(d+1)}\right)$ 次运算求得 $\mathcal{F}$的 Gr¨obner 基。

证明. 令 $N = \binom{d+1+n}{d+1}$ 表示次数至多为 $d = \mathrm{d_{reg}}(\mathcal{F})$的单项式个数。根据定理 1.1，要构造 Gr¨obner 基，只需找到 $V_{\mathcal{F},d+1}$的一个基。为此，我们按如下步骤进行。通过线性运算，可以确保对所有 f_i, f_j，都有 $\mathrm{LT}(f_i) \neq \mathrm{LT}(f_j)$。这等价于计算一个有 N 列、N 行的矩阵的简化行阶梯形，可在 $\mathbb{K}$ 中通过 $\mathcal{O}(N^3)$ 次运算完成。令 $\mathcal{B} = \mathcal{F}$ 和 $\mathcal{M} = \{mf_i : f_i \in \mathcal{F}$，其中 m 是次数至少为 1 的单项式，且 $\deg(mf) \leq d + 1\}$。每一步中，我们选取 $\mathcal{M}$中的一个元素 f，并通过仅涉及 $\mathcal{B}$ 中元素的倍数的线性运算对 f 进行约化，直到得到一个元素 f，使得 $\mathrm{LT}(f) = 0$，或者 $\mathrm{LT}(f) \notin \{\mathrm{LT}(b) : b \in \mathcal{B}\}$。我们从 $\mathcal{M}$ 中移除 f。然后，如果 $\mathrm{LT}(f) \notin \{\mathrm{LT}(b) : b \in \mathcal{B}\}$，我们就将 f 加入 $\mathcal{B}$，并将所有满足以下条件的 mf 加入 $\mathcal{M}$： m 是次数至少为 1 的单项式，且 $\deg(m\bar{f}) \leq d + 1$。这一步需要 $\mathcal{O}(N^2)$次运算。我们重复这一步，直到 $|\mathcal{B}| = N$ 或 $|\mathcal{M}| = 0$成立。每次向$\mathcal{B}$中添加一个新元素时，我们至多向 $\mathcal{M}$中添加 N 个元素。由于在 $\mathcal{B}$ 中至多能添加 N 个元素，该算法至多经过 N^2步便会终止。每一步的代价为 $\mathcal{O}(N^2)$，因此我们可以通过 $\mathcal{O}(N^4)$次运算求得 $\mathcal{F}$的 Gr¨obner 基。由于 $N \leq (n+1)^{d+1}$，结论得证。 □

致谢

作者感谢 Elisa Gorla 提出的宝贵建议。

参考文献

[1] Magali Bardet.´关于超定代数系统的研究：在纠错码和密码学中的应用。博士论文，巴黎第六大学，2004年。[2] M. Bigdeli、E. De Negri、M. M. Dizdarevic、E. Gorla、R. Minko 和 S. Tsakou。半正则序列及其他随机方程组。密码学电子印本档案，论文 2020/1375，2020年。https://eprint.iacr.org/2020/1375。[3]Johannes A. Buchmann、Jintai Ding、Mohamed Saied Emam Mohamed 和 Wael Said Abd Elmageed Mohamed。MutantXL：用于密码分析的多元多项式方程求解。在 Helena Handschuh、Stefan Lucks、Bart Preneel 和 Phillip Rogaway 编，

《对称密码学》，Dagstuhl 研讨会论文集（DagSemProc）第9031卷，第1–7页，德国 Dagstuhl，2009年。Schloss Dagstuhl – Leibniz-Zentrum f¨ur Informatik。[4] Alessio Caminata 和 Elisa Gorla。求解多元多项式系统及交换代数中的一个不变量。载于 Jean Claude Bajard 和 Alev Topuzo˘glu 编，《有限域算术》，第3–36页，沙姆，2021年。施普林格国际出版公司。[5] 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。[6] Nicolas T. Courtois、Alexander Klimov、Jacques Patarin 和 Adi Shamir。求解超定多元多项式方程的高效算法。载于国际密码技术理论与应用会议，2000年。[7] Jean-Charles Faug`ere。一种计算 Gröbner 基的新型高效算法（F4）。《纯粹与应用代数杂志》，139(1-3)：61–88，1999年6月。[8] Jean Charles Faug`ere。一种无需归约为零即可计算 Gröbner 基的新型高效算法（F5）。载于2002年国际符号与代数计算研讨会论文集（ISSAC ’02），第75–83页，美国纽约，2002年。计算机协会。[9] Jean-Charles Faug`ere、Magali Bardet 和 Bruno Salvy。半正则超定代数方程的 Gröbner 基计算复杂度。2004年。[10] Elisa Gorla、Daniela Mueller 和 Christophe Petit。HFE系统 Gröbner 基计算成本的更紧上界。《符号计算杂志》，109：386–398，2022年。[11] Ming-Deh A. Huang、Michiel Kosters、Yun Yang 和 Sze Ling Yeo。零维韦尔下降系统的最后下降次数。《符号计算杂志》，87：207–226，2018年。[12]Ming-Deh A. Huang、Michiel Kosters 和 Sze Ling Yeo。ECDLP上的最后下降次数、HFE和韦尔下降攻击。密码学电子印本档案，论文 2015/573，2015年。https://eprint.iacr.org/2015/573。¨D. Lazard。Gröbner 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》，第146–156页，柏林、海德堡，1983年。施普林格柏林海德堡。[14] Mohamed Saied Emam Mohamed、Wael Said Abd Elmageed Mohamed、Jintai Ding 和 Johannes Buchmann。MXL2：使用改进的突变策略求解 GF(2) 上的多项式方程。载于 Johannes Buchmann 和 Jintai Ding 编，《后量子密码学》，第203–215页，柏林、海德堡，2008年。施普林格柏林海德堡。[15] Igor Semaev 和 Andrea Tenti。有限域上 Macaulay 矩阵的概率分析及构造 Gröbner 基的复杂度。《代数杂志》，565：651–674，2021年。[16] Andrea Tenti。充分超定的随机多项式系统表现得如同半正则系统。博士论文，卑尔根大学，2019年。