arXiv:2603.02279v1 [math.AC] 2 Mar 2026

多项式方程组的坏约化素数

Jesse Elliott*† ´Eric Schost†

2026年3月4日

摘要

考虑域 $\mathbb{K}$ 上的多项式 F_1、.....、F_s in $\mathbb{K}[X_1,\dots,X_n]$，其零点集 $V(F_1$、.....、$F_n)$ in $\mathbb{K}^n$ 以及它的分解为等维分支 V_0、.....、V_n（其中对于所有 i，V_i 要么为空，要么维数为 i）。对于每个 V_i，我们可以关联其乔形式；乔形式是新变量 $(U_{k,j})_{0\le k\le i,\ 0\le j\le n}$ 的多项式，并且在标量因子意义下唯一确定。这些乔形式完全刻画了 V_i：我们可以从中恢复 V_i 的方程，而其次数为 V_i 的次数的 $(i+1)$ 倍。

我们讨论 F_i 具有整数系数的情形，并研究如下问题：将按上述方式定义的 V_i 的乔形式模 p 约化后，何时能够得到 V 的等维分支的乔形式（F_1 模 p、.....、F_s 模 p）。我们证明，只要 p 不整除某个高度为 $O(n^{14}shd^{3n+4})$ 的非零整数 Δ，就一定成立；其中 d 和 h 分别是 F_i 的次数和高度的界。

关键词— 多项式系统求解；乔形式；位复杂度

1 引言

考虑具有整数系数的多项式 $F_1,\dots,F_s$；它们在 $\mathbb{C}^n$ 中定义了代数集 $V=V(F_1,\dots,F_s)$。我们不对这些多项式作任何正则性假设，尤其不假设 V 是等维的。因此，我们可以将 V 写成等维分解 $V=V_0\cup\cdots\cup V_{n-1}\cup V_n$，其中对于所有 i，V_i 都是我们所称的 V 的 i维等维分支，即其维数为 i 的不可约分支之并（也可能为空）。

本文旨在量化 V 的“坏约化”素数。定义“好”素数和“坏”素数有多种可能的方式。例如，可以要求 $(F_1,\dots,F_s)$ 的 Gr¨obner 基模 p 素数约化后，等于 $(F_1$ 模 $p,\dots,F_s$ 模 $p)$ 的 Gr¨obner 基。我们的

*索邦大学，Inria，IMJ–PRG，法国巴黎。电子邮箱：jesse.elliott@inria.fr。

†滑铁卢大学，David R. Cheriton计算机科学学院，加拿大滑铁卢。电子邮箱：jakellio@uwaterloo.ca，eschost@uwaterloo.ca。

定义将具有几何性质：我们希望表达的是，将 $V_0, \ldots, V_{n-1}, V_n$ 模 p 素数约化后，得到 $V(F_1$ 模 $p, \ldots, F_s$ 模 $p) \subset \mathbb{F}_p{}^n$ 的等维分解。特别地，这将意味着对于所有 i， V 的第 i 个等维分支与 $V(F_1$ 模 $p, \ldots, F_s$ 模 $p)$ 的第 i 个等维分支具有相同的次数，但我们的要求会更强。注意，即使在 $V(F_1, \ldots, F_s)$ 为零维这一简单情形下， $V(F_1$ 模 $p, \ldots, F_s$ 模$p)$ 仍可能具有任意维数的分支（它们产生理想 $\langle F_1, \ldots, F_s \rangle \subset \mathbb{Z}[X_1, \ldots, X_n]$ 的主分量，而这些主分量包含素数 p）。

等维代数集 Y 可由其乔形式描述：若 Y 定义在域 $\mathbb{K}$ 上且维数为 r，其乔形式便是无平方因子多项式，先验地属于$\mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r]$，其中 $\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r$ 是新的不定元，且 $\boldsymbol{U}_i = U_{i,0}, \ldots, U_{i,n}$ 对所有 i均成立。所有这些多项式都相差一个 $\mathbb{K}$中的非零乘法因子；并且由于 Y 定义在 $\mathbb{K}$上，它也存在系数属于 $\mathbb{K}$ 的乔形式。若 Y 为空，按惯例，其乔形式为常数 $c \in \mathbb{K} - \{0\}$。

我们将在第3节回顾乔形式的定义；此处先指出几个值得注意的性质。首先， Y的乔形式关于 $\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r$是多齐次的，其对任一变量组 $\boldsymbol{U}_i$ 的次数等于 Y的次数。其次，给定 Y 的一个乔形式，便可恢复其定义方程（参见 [12, 推论 3.2。6] 以及 [2]；我们将在第4.2节简要推导这一结论）。此外，对于主要结果可能的应用而言很重要的是，若 Y 是零维的，则可由其任一乔形式通过中的一元多项式（$Q, V_1, \ldots, V_n$）来描述，形式为

$$Y = \left\{ \left(\frac{V_1(\tau)}{Q'(\tau)}, \ldots, \frac{V_n(\tau)}{Q'(\tau)} \right) \mid Q(\tau) = 0 \right\}.$$

事实上，当 Y的维数为 $r = 0$ 时，其乔形式是变量 $U_{0,0}$，……， $U_{0,n}$ 以及 Q 中的多项式，分别地 V_1，……， V_n，上面这些是通过求值其一个乔形式、分别地求值其偏导数，在 T， α_1，……， α_n 处，对某个 α_1，……， α_n 属于 $\mathbb{K}$ 而得到的（这可追溯到 [17] 与 [19]）。

在任意维数下，当 Y 定义在 $\mathbb{K} = \mathbb{Q}$ 上时，它具有有理系数的乔形式。消去分母并提取公因子，我们推得 Y 恰好有两个本原乔形式，即具有整数系数且内容为 1 的乔形式（具有整数系数的非零多项式的内容是其系数集合的最大公因式）。特别地，这些多项式可模任意素数 p 进行约化。

回到我们关于 $V = V(F_1, \ldots, F_s)$ 的情形，我们对好素数p 的定义如下： p 是好素数，当且仅当 $V(F_1, \ldots, F_s)$ 的等维分支的本原乔形式模 p 的约化是 $V(F_1 \bmod p, \ldots, F_s \bmod p)$ 的等维分支的乔形式。由于我们考虑的是本原多重齐次多项式，它们的次数在模任意素数 p 时不会下降，因此对于好素数 p， $V(F_1, \ldots, F_s)$ 与 $V(F_1 \bmod p, \ldots, F_s \bmod p)$ 的第 i 个等维分支确实具有相同的次数。

陈述主要结果所需的最后一个要素是高度：首先是非零整数的高度，其次是带整数系数的非零多项式的高度：非零整数 c 的高度 $h(c)$是自然对数 $\ln(|c|)$，而P 上非零多项式的高度 $h(P)$是其非零系数的高度的最大值。稍后，我们将把这个定义扩展到有理系数多项式。

定理 1.1。 设 F_1，……， F_s 属于 $\mathbb{Z}[X_1, \ldots, X_n]$，次数至多为 d，高度至多为 h。则存在一个非零整数 Δ，使得

$$h(\Delta) \in O(n^{14} s h d^{3n+4})$$

使得若素数 p 不整除 Δ，则 $V(F_1, \ldots, F_s)$ 的等维分支的本原乔形式模 p 的约化是 $V(F_1$ 模 $p, \ldots, F_s$ 模 $p)$的等维分支的乔形式。

这一结果受到我们先前工作的启发 [8, 9, 10]。在基于中国剩余定理的模算法（例如求解多项式方程组的算法）的背景下，Pernet [23] 与 B¨ohm等人 [3] 提出了允许若干不幸素数（对于这些素数，我们得不到正确的模像）并使用纠错的想法。在 [8, 9, 10], 我们对该方法进行了定量分析，强调需要一个先验关于不幸素数个数的界，并用求解多项式方程组的算法为例说明了这一想法。对于这一问题，我们依赖于 D'Andrea 等人 [7], 所给出的与我们主定理中类似的界，但该界仅当 $V(F_1, \ldots, F_s)$为零维时适用。

将 [7] 的结果推广到任意 F_i是一个自然的问题，但我们用于证明主定理的技术并非对该文献中方法的延伸。相反，我们将描述一种算法，用于计算 $V(F_1, \ldots, F_s)$的等维分支的乔形式，并确定哪些素数 p 使得我们可以将其所有步骤模p约化。该算法受到 [15], 先前提出的一种算法的启发，并借鉴了该文献（以及 [2]）中的许多基本要素，但它要简单一些：[15] 中的算法采用了比我们更先进的技术（例如牛顿迭代），以控制运行时间。我们的算法无论如何都不太可能高效，但分析它在何种素数下会退化将相当直接，因为它几乎完全基于多项式最大公因式。

我们还提及Tsigaridas等人 [6], 的工作，该工作利用确定性的基于结式的算法，首次给出了计算乔形式（以及赫尔维茨形式）的位复杂度界。不过，我们的工作并未使用这一结果。

备注 1.2. 为便于阅读，我们以渐近形式陈述定理1.1 ，因为明确的不等式很快就会变得冗长且难以理解。我们还提供了一个 Maple 脚本，用于生成完整的不等式（见 代码库）。在第 6 节中，我们将此上界与以下不等式进行比较： [7], 该不等式量化了满足以下条件的素数 p ： 多项式方程组已知在 $\mathbb{Q}$上是零维的，但其模 p后的解的数量有所不同。 □

2 有理系数多项式

2.1 高度

我们在引言中定义了整数和整系数多项式的高度。我们可以将这个定义推广到有理系数多项式。本节中，我们的

主要参考文献是 [16]。

定义 2.1。 非零多项式 F 的高度 $h(F)$ 是其最小分母 d的高度与其非零系数 dF （它们都是整数）的高度中的最大值。

以下关于整系数多项式高度的事实将会用到：

- 若 F, G 是 $\mathbb{Z}[Y_1, \ldots, Y_s]$ 中的多项式，且 G 在 $\mathbb{Z}[Y_1, \ldots, Y_s]$中整除 F，则由 [18, 命题 2.12]可得

$$h(G) \leq h(F) + s \deg(F). \tag{1}$$

- 若 S是一个元素属于 $\mathbb{Z}[Y_1, \ldots, Y_s]$ 的 $N \times N$矩阵，其列次数至多为 $d_1, \ldots, d_N$，列高度至多为 $h_1, \ldots, h_N$，则其行列式（若非零）的高度为

$$h(\det(S)) \leq N \ln(N) + \sum_{i \leq N} h_i + \ln(s+1) \sum_{i \leq N} d_i, \tag{2}$$

参见 [16, 引理 1.2]。

2.2 模素数 p 约化的基本知识

我们将反复论证，某些在 $\mathbb{Q}$ 上进行的运算所得结果在素数 p 模下“约化良好”。在这种情况下，下面的记号会很有用。

定义 2.2。 对于 p 素数，我们用 $\mathbb{Z}_{(p)}$ 表示在素理想 (p) 处的局部化 .

这是由分母的最小分母模 p 不为零的分数组成的子环。存在良定义的模 p 约化同态 $\mathbb{Z}_{(p)} \to \mathbb{F}_p$，记作 $F \mapsto f = F \bmod p$；这一记号也沿用于系数属于 $\mathbb{Z}_{(p)}$ 的多项式。

在下面引理及其他几个引理的证明中，我们将把一个有理系数非零多项式 A 写成 $A = n_A A'/d_A$，其中 n_A, d_A 是互素正整数，且 A' 是本原的，也就是说，它具有整数系数且内容为 1。高斯引理指出，本原多项式的乘积仍是本原多项式：这在单变量情形下广为人知，对多元多项式也依然成立（使用指数足够高的克罗内克代换，以确保它对我们所考虑的所有多项式的指数都是一一对应的）。

引理 2.3. 设 A、B、C 为系数在 $\mathbb{Q}$ 中的多项式，使得 $A = BC$。设 p 为一个素数，并假设

- A 与 B 的系数在 $\mathbb{Z}_{(p)}$ 中，从而我们可以定义 $a = A$ 模 p 与 $b = B$ 模 p,
- B 在模 p下不为零。

那么， C 的系数属于 $\mathbb{Z}_{(p)}$，若记 $c = C$ 模 p，则有 $a = bc$。

证明。我们首先证明 C 的系数属于 $\mathbb{Z}_{(p)}$。将 $A = n_A A'/d_A$、 $B = n_B B'/d_B$和 $C = n_C C'/d_C$写成 A', B', C'为本原，且(n_A, d_A)、(n_B, d_B)、(n_C, d_C)为互素整数对；特别地， d_A 是 A 中系数分母的最小公倍数（对 B 和 C同样如此）。

利用高斯引理，我们得到 $n_A d_B d_C = d_A n_B n_C$。若 p 整除 d_C，则它必定整除$d_A n_B$ （因为 d_C 与 n_C 互素）。这是不可能的:

- ，因为 A 的系数属于 $\mathbb{Z}_{(p)}$， d_A 模 p 非零
- ，因为 b 非零， n_B 模 p 非零。

因此， p 不整除 d_C。既然已知 C 的系数属于 $\mathbb{Z}_{(p)}$，我们便可对 $A = BC$ 模 p进行约化，从而完成证明。 □

2.3 最大公因式及其模 p约化

多元多项式环中的最大公因式并不唯一。设 $\mathbb{K}$ 是一个域，并考虑 $\mathbb{K}[Y_1, \ldots, Y_s]$中的多项式 F和 G。 F和 G 的最大公因式是所有满足以下条件的多项式：其不可约因子是 F 和 G共有的不可约因子，并且这些因子在 F和 G的分解中的指数分别取最小值。它们之间只相差非零乘法常数。我们将采用以下约定对它们进行规范化。

定义 2.4. 令 $\prec$ 为由 $Y_1 > \cdots > Y_s$ 在$\mathbb{K}[Y_1, \ldots, Y_s]$上诱导的分次字典序。对于不同时为零的 F、 G，F和 G的首一最大公因式 记作$\gcd(F$、 $G)$，它是这些多项式中相对于序 $\prec$首项系数为1 的唯一最大公因式。

备注 2.5。如果 $\mathbb{L}$ 是 $\mathbb{K}$的域扩张，那么无论在 $\mathbb{K}[Y_1, \ldots, Y_s]$还是在 $\mathbb{L}[Y_1, \ldots, Y_s]$中求 $\gcd(F,\ G)$, 结果都相同。 □

在下文中，当我们提及多项式 F 的首项系数时，指的是上文引入的排序；我们将其记为 $\mathrm{lc}(F)$。首项系数取决于我们对变量排序的方式，因此两个多项式 F, G 在 $\mathbb{K}[Y_1, \ldots, Y_s]$ 中的首一最大公因式，一般而言会不同于 F, G 在 $\mathbb{K}[Y_{\sigma(1)}, \ldots, Y_{\sigma(s)}]$ 中所见的首一最大公因式，其中 σ 是 $\{1, \ldots, s\}$ 的一个置换。

引理 2.6. 设 F、 G 为 $\mathbb{Q}[Y_1, \ldots, Y_s]$ 中的非零元，次数分别至多为 d_F、 d_G，高度分别为 h_F、h_G，并设 H 为其首一最大公因式。存在非零整数 $\Delta_{F,G}$，使得

$$h(\Delta_{F,G}) \in O(sd_F \ln(d_F) + sd_G \ln(d_G) + sd_F h_G + sd_G h_F + s^2 d_F d_G)$$

使得若素数 p p 不整除 $\Delta_{F,\ G}$, F, G, H 的系数都属于 $\mathbb{Z}_{(p)}$，并且若将它们模 p 化简后记作 $f, g,$ h，则有 $h =$最大公因式(f, g)。

证明。将 $F = n_F F'/d_F, G = n_G G'/d_G$和 $H = n_H H'/d_H$ 写成 F'， G'， H' 在 $\mathbb{Z}[Y_1, \ldots, Y_s]$ 中的本原表示，且 $(n_F,\ d_F), (n_G,\ d_G), (n_H,\ d_H)$ 是互素整数对。由于 H 是首一的，$\mathrm{lc}(d_H H) = d_H$，但这等于 $n_H \mathrm{lc}(H')$，因此 n_H 整除 d_H；这又意味着 $n_H = 1$。

再定义 $A = F'/H'$ 和 $B = G'/H'$；它们是具有先验 有理系数的多项式。由等式 $F' = AH'$，按惯例若写作 $A = n_A A'/d_A$，则可得$d_A F' = n_A A' H'$，再由高斯引理可得 $n_A = d_A$ 和 $A = A'$。因此， A 以及类似地 B都是 $\mathbb{Z}[Y_1, \ldots, Y_s]$中的本原多项式，且在 $\mathbb{Q}[Y_1, \ldots, Y_s]$中没有非恒定公因子。

我们的第一个条件是 p不应整除 $\delta = d_F d_G \ell_F$，其中 ℓ_F是 $d_F F$的首项系数，因此 $f = F$模 p和 $g = G$模 p都有定义。等式$F' = AH'$给出 $d_F F = n_F A(d_H H)$，所以 $d_H H$ 的首项系数整除 $d_F F$在$\mathbb{Z}$中的首项系数，也就是说， d_H 整除 ℓ_F。因此，我们的假设还意味着 d_H 模p不为零，从而可以定义 $h = H$ 模 p。

于是我们可以将关系式 $d_F F = n_F d_H AH$模 p化简；由于我们知道 d_F模 p是一个单位，因此 h 整除 f。同理， h 整除 g。因为 h 是首一的，这表明最大公因式$(f,\ g)$ = 最大公因式$(a,\ b)$，因此只需给出能保证a和 b 模 p仍互素的 p 的条件。

ˆ 对于 $i = 1$、.....、 s，令 $D_i \in \mathbb{Z}[Y_1, \ldots, Y_i, \ldots, Y_s]$ 为 A和 B关于Y_i的结式。 D_i 非零：否则， A和 B在 $\mathbb{Q}(Y_1$、.....、 Y_i、.....、 $Y_s)[Y_i]$中会有一个次数为正的公因子，这将导致ˆA和 B 在 $\mathbb{Q}[Y_1, \ldots, Y_s]$ 中存在一个非常数公因子（证明：将 $A = PQ$ 写成 $\mathbb{Q}(Y_1$、.....、 Y_i、.....、 $Y_s)[Y_i]$中的形式，其中 P的ˆY_i次数为正；改写为 $n_A A' = n/dP'Q'$，其中 A'、 P'和 Q'在 $\mathbb{Q}[Y_1, \ldots, Y_i, \ldots, Y_s][Y_i]$中是本原的；推出 $n_A = n/d$和 $A' = P'Q'$，再乘以 n_A得到 $A = n_A P'Q'$，因此 P'在$\mathbb{Q}[Y_1, \ldots, Y_s]$中整除 A。同理，它也整除 B）。

假设 p 满足 D_i 模 p 不为零。因此， A 和 B 的首 Y_i 次系数模 p 不会同时为零（否则，它们的 Y_i-Sylvester 矩阵的第一行将为零）。按照 [11], 中引理 6.25 的证明，我们可知， $a = A$ 模 p ˆ 和 $b = B$ 模 p 在 $\mathbb{F}_p(Y_1, \ldots, Y_i, \ldots, Y_s)[Y_i]$ 中的最大公因式是常数。特别地， a 和 b 在 $\mathbb{F}_p[Y_1, \ldots, Y_s]$ 中没有次数为正的公因子，其 Y_i 次数为正。

对所有 i 重复此过程；我们得出结论：如果所有 D_i 模 p 都非零，那么 $a = A$ 模 p 和 $b = B$ 模 p 在 $\mathbb{F}_p[Y_1, \ldots, Y_s]$ 中没有非常数公因子，这正是我们要保证的结论。对于 $i \le s$，令 $\delta_i \in \mathbb{Z}$ 为 D_i 的任意一个非零系数，并令 $\Delta_{F,\ G} = \delta\delta_1 \cdots \delta_s$。

总之，只需给出多项式 D_i 的高度上界。对于 $i \le s$， A和 B的 Y_i-次数至多为 d_F，分别为 d_G，且高度至多为 $h_F + sd_F$，分别为$h_G + sd_G$（参见小节 2.1中的说明）。由此可得 D_i，因此 δ_i的高度至多为

$$(d_F + d_G)\ln(d_F + d_G) + d_F(h_G + sd_G) + d_G(h_F + sd_F) + 2\ln(s+1)d_F d_G.$$

乘以 s ，以涵盖所有变量，并为 δ加上 $2h_F + h_G$ 。经过少许简化后，即得引理中所述的界。 □

3 乔形式

我们回顾代数集的乔形式的定义，以及当我们在 $\mathbb{Q}$上工作时，如何利用它定义其高度。再次说明，我们主要参考 [16]。

一些基本概念在此视为已知：对于域 $\mathbb{K}$ 及其代数闭包 $\overline{\mathbb{K}}$，代数集 $V \subset \overline{\mathbb{K}}^n$ 是 $\overline{\mathbb{K}}[X_1, \ldots, X_n]$中某些多项式（$F_i$）的公共零点集。代数集 V 可唯一地写成其不可约分支的并，这些不可约分支是出现在 $I(V)$ 的初等分解（此处为素理想分解）中的素理想的零点集。对于 $r = 0, \ldots, n$， V的 r等维分支是指其维数为 r的不可约分支之并，我们有时将其记作 V_r。最后，如果 V 非空且 $V = V_r$，则称 V 是 r-等维的。

维数和次数首先对不可约代数集定义，然后推广到任意代数集（分别取其不可约分支上的最大值和总和）。

如果代数集 V的定义理想 $I(V) \subset \overline{\mathbb{K}}[X_1, \ldots, X_n]$ 有一组系数属于 $\mathbb{K}$的生成元，则称其定义在 $\mathbb{K}$ 上。即使在这种情况下，V 的不可约分支也未必都定义在 $\mathbb{K}$上，我们仍可定义其 $\mathbb{K}$-不可约分支：它们是取自 $I(V) \cap \mathbb{K}[X_1, \ldots, X_n]$的初等分解中的素理想所对应的分支。它们都定义在 $\mathbb{K}$上，而 V的 r-等维分支则等于 V 中维数为 r的 $\mathbb{K}$-不可约分支之并。

3.1 定义乔形式

设 $\mathbb{K}$ 是一个域，$V \subset \overline{\mathbb{K}}^n$ 是一个次数为 D 的 r 等维代数集。考虑集合 $\Delta_V \subset \mathbb{P}^n \times \cdots \times \mathbb{P}^n$（$r+1$ 个因子），其中包含所有 $\boldsymbol{u} = (\boldsymbol{u}_0, \ldots, \boldsymbol{u}_r)$，满足 $\boldsymbol{u}_i = (u_{i,0} : \cdots : u_{i,n})$，对于所有 i，存在 $(x_1, \ldots, x_n)$ 属于 V，使得

$$u_{i,0} + u_{i,1}x_1 + \cdots + u_{i,n}x_n = 0, \quad i = 0, \ldots, r. \tag{3}$$

Δ_V 的扎里斯基闭包是一个超曲面，而 V 的一个乔形式是定义该超曲面的任意无平方因子多项式。所有这些多项式相差一个 $\overline{\mathbb{K}}$ 中的非零乘法因子；它们属于 $\overline{\mathbb{K}}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r]$，其中 $\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r$ 是新的不定元，且 $\boldsymbol{U}_i = U_{i,0}, \ldots, U_{i,n}$ 对所有 i 都在每组变量 $\boldsymbol{U}_i$ 中齐次，次数为 D，并且在 $\overline{\mathbb{K}}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r]$ 中没有非平凡的多重因子。如果 V 定义在 $\mathbb{K}$ 上，它也存在系数属于 $\mathbb{K}$ 的乔形式。以下性质都是经典结果。

事实 3.1. 设 V^{proj} 是 $\mathbb{P}^n$ 中 V 的射影闭包，且 C 是 V 的乔形式。那么，$\boldsymbol{u} = (\boldsymbol{u}_0, \ldots, \boldsymbol{u}_r) \in \mathbb{P}^n \times \cdots \times \mathbb{P}^n$ 消去 C，当且仅当存在$(x_0 : \cdots : x_n)$ 属于$V^{\text{射影}}$，使得 $u_{i,0}x_0 + u_{i,1}x_1 + \cdots + u_{i,n}x_n = 0$ 对所有 i 均成立。

证明见 [15] 中的引理 1.1。

事实 3.2. 等维簇的乔形式是其不可约分支的乔形式之积，而后者在 $\overline{\mathbb{K}}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r]$中不可约。

事实 3.3。 $\mathbb{A}^n$ 和 $\mathbb{P}^n$ 的乔形式为 $c\det(\boldsymbol{U}_0, \ldots, \boldsymbol{U}_n)$，$c \in \overline{\mathbb{K}} - \{0\}$。

通过考虑任意选取次数的形式的交，而不仅仅是超平面的交，可以扩展乔形式的定义，如[24]中所述。在本文中，我们将使用以下构造，称为 [15, 16]中的广义乔形式：我们在仿射情形下工作，并将最后一个线性形式$U_{r,0}+U_{r,1}X_1+\cdots+U_{r,n}X_n$替换为一个次数为 d 且具有一般系数 $\boldsymbol{V}=(V_\alpha)$的多项式$F(X_1,\ldots,X_n)$，其中 $\alpha\in\mathbb{N}^n$ 满足 $|\alpha|\le d$（其他线性形式不变）。按照 $d=1$情形中的相同构造，我们现在得到 $\mathbb{P}^n\times\cdots\times\mathbb{P}^n\times\mathbb{P}^{N-1}$中的一个集合 $\Delta_V^{(d)}$，其中 $N=\binom{n+d}{n}$。对于 $d=1$，我们恢复先前的定义，只需将 $n+1$ 不定元 $\boldsymbol{V}$替换为$\boldsymbol{U}_r=U_{r,0},\ldots,U_{r,n}$。

$\Delta_V^{(d)}$ 的扎里斯基闭包的任意定义多项式都称为 V的次数 d 乔形式。这些是关于变量 $\boldsymbol{U}_0,\ldots,\boldsymbol{U}_{r-1},\boldsymbol{V}$ 的多重齐次多项式；关于 $\boldsymbol{V}$ 的次数为 D，关于其他所有变量组的次数均为 dD；它们彼此只相差一个非零乘法常数因子。如果 $C_d\in\mathbb{K}[\boldsymbol{U}_0,\ldots,\boldsymbol{U}_{r-1},\boldsymbol{V}]$ 是这样的多项式，且 F属于 $\mathbb{K}[X_1,\ldots,X_n]$ 且次数不超过 d，我们将 $C_d[F]$ 记作多项式 $C_d($ $\boldsymbol{U}_0,\ldots,\boldsymbol{U}_{r-1},$**系数(**$F$**)**)，其中**系数(**$F$**)**是 F的系数向量。

3.2 乔形式的规范化

现在我们讨论如何为代数集 V的乔形式定义一个规范选择。当 V 定义在 $\mathbb{Q}$上时，我们在引言中确实提到了它的本原乔形式，但其定义无法推广到任意域。相反，我们将采用 Krick、Pardo 和 Sombra [16], 提出的一种构造，该构造适用于处于一般坐标下的 V。

在下文中，对于诸如 $\mathbb{K}[\boldsymbol{U}_0,\ldots,\boldsymbol{U}_r]$这样的环，我们采用定义 2.4 中引入的分次序，它由 $U_{0,0}>\cdots>U_{0,n}>\cdots>U_{r,0}>\cdots>U_{r,n}$ 诱导。

引理 3.4。若 V 是一个 r等维代数集，次数为 D，且 C 是它的乔形式，则 C不含大于 $U_0^D{}_{,0}\cdots U_{r-1,r-1}^D U_r^D{}_{,r}$ 的单项式。

证明。 的乔形式是齐次的，其在 $D=\deg(V)$ 次的 $(r+1)$ 阶子式 $M_{i_0,\ldots,i_r}$上，次数为 $r+1)\times(n+1)$ 矩阵的 $(U_{i,j}$ [5]，该矩阵的元素为，且每个此类子式的首项系数都小于或等于 $U_{0,0}\cdots U_{r-1,r-1}U_{r,r}$。 □

定义 3.5. 次数为 D 的 r 等维代数集 V 处于正规位置，当且仅当其乔形式的首项为 U_0^D、$_0\cdots U_{r-1}^D$、$_{r-1}U_r^D$、$_r$。

若满足此条件，我们用 C_V 表示 V 的唯一一个首项系数为1的乔形式，并称其为 V 的归一化乔形式。

引理 3.6. 若 V_1、...、V_s 是两两不同的不可约 r 维代数集，且 $V=V_1\cup\cdots\cup V_s$，则：

- V 处于正规位置，当且仅当所有 V_i 都是

V 处于正规位置时，●，则 $C_V=C_{V_1}\cdots C_{V_s}$。

证明。 设 $C_1,\ldots,C_s$ 是 $V_1,\ldots,V_s$的乔形式，因此 $C=C_1\cdots C_s$ 是V的乔形式（事实 3.2）。若记 $D_i=\deg(C_i)$（对所有 i和 $D=D_1+\cdots+D_s$），引理 3.4表明

C_i中的所有单项式都小于或等于$U_0^{D_i,0}\cdots U_r^{D_i,r}$。这意味着$\ell$中$U_0^{D,0}\cdots U_r^{D,r}$的系数，是$\ell_i$中对应单项式系数$U_0^{D_i,0}\cdots U_r^{D_i,r}$的乘积，其中$,\ldots,C_s$。特别地，$\ell$非零当且仅当所有的$\ell_i$都非零（这证明了第一点）；当所有的$\ell_i$都为一时，$\ell$等于一（这证明了第二点）。□

在 [16], Krick 等人 给出了使 V 处于正规位置的一个充分条件：即下述引理中的蕴含关系 (2) $\Longrightarrow$ (3)。下文中，一般 性质是指在相应参数空间的非空 Zariski 开集上成立的性质。

引理 3.7。 设 $V\subset\mathbb{K}^n$是次数为 D的 r-等维代数集。以下条件等价：

1. 对一般的 $x_1,\ldots,x_r\in\mathbb{K}$，集合 $V\cap V(X_1-x_1,\ldots,X_r-x_r)$ 的基数为 D *2.* 存在 $x_1,\ldots,x_r\in\mathbb{K}$，使得集合 $V\cap V(X_1-x_1,\ldots,X_r-x_r)$ 的基数为 D *3.* V 处于正规位置 *4.* 射影代数集 $V_{\mathrm{proj}}\cap V(X_0,\ldots,X_r)$ 为空集。

证明。 显然，(1) 蕴含 (2)。反过来，假设 (2) 成立，我们来证明 (1)。首先证明可以假设 V 不可约。

对于 (2) 中的 $x_1,\ldots,x_r$，以及 V 的任一不可约分支 W，其次数为 D_W，$W\cap V(X_1-x_1,\ldots,X_r-x_r)$ 是有限的（因为 V 的纤维是有限的），因此其基数为 $d_W\le D_W$（根据贝祖定理）。但由于 $V\cap V(X_1-x_1,\ldots,X_r-x_r)$ 的基数为 $D=\sum D_W$，我们得出，对所有 W，$d_W=D_W$。如果我们对所有 W 证明了 (1)，那么 (1) 对 V 也成立，因为对于一般的 $x_1,\ldots,x_r$，纤维 $W\cap V(X_1-x_1,\ldots,X_r-x_r)$ 两两不相交。

此处假定 V 不可约，我们接着证明 (1)，并记 π_r 为到 $X_1,\ldots,X_r$-空间上的投影。若$\pi_r(V)$的扎里斯基闭包的维数小于r，则由纤维维数定理 [21, 定理 9.9], ，π_r 到 V 的限制的所有非空纤维都具有正维数，这与 (2) 矛盾。由此可知，$\pi_r:V\to\mathbb{K}^r$ 是支配的，且一般纤维有限。然后，由 [13, 命题 1], ，该映射的所有有限纤维的基数小于或等于一般纤维的基数，因此一般纤维的次数至少为 D。另一方面，它的次数不可能大于 D，故得证。

接下来，我们证明 (3) 与 (4) 等价。设 V^{proj} 为 V的射影闭包，并设 C为 V的一个乔形式。若令 $D=\deg(V)$，则 C中$U_0^{D,0}\cdots U_r^{D,r}$的系数，是通过对所有在第$U_{i,i}$个分量取值为 1 的 i，将 C在 $\boldsymbol{U}_i=(0,\ldots,0,1,0,\ldots,0)$处求值而得到的。特别地，该系数非零（即 V 处于正规位置）当且仅当在 $V_{\text{射影}}$ 中不存在满足 $x_0=\cdots=x_r=0$的 $(x_0:\cdots:x_n)$，也就是说，$V_{\text{射影}}\cap V(X_0,\ldots,X_r)$ 为空。这就证明了我们的断言。

最后，我们证明 (1) 和 (2) 都等价于 (4)。假设 (2) 成立，并考虑交集 $V_{\text{投影}}\cap V(X_1-x_1X_0,\ldots\ldots,X_r-x_rX_0)$。根据 B´ezout 不等式（对于

射影簇），其次数至多为 D，但我们的假设表明它包含 D个孤立点（位于有限距离处），因此它没有无穷远点。这表明

$$V^{\mathrm{proj}} \cap V(X_0, X_1 - x_1X_0, \ldots, X_r - x_rX_0) = V^{\mathrm{proj}} \cap V(X_0, X_1, \ldots, X_r)$$

为空，因此我们得到 (4)。

最后，假设 (4) 成立，因此 $V_{\mathrm{proj}} \cap V(X_0, X_1, \ldots\ldots, X_r)$ 为空。根据 [22,推论 5。6], 将 π_r 限制到 V^{proj} 所得映射的次数等于 $D = \deg(V)$。按定义，此类映射的次数就是其一般纤维的基数，因此 (1) 成立。

□

假设 V处于正规位置，因此 $V_{\mathrm{proj}} \cap V(X_0, \ldots\ldots, X_{r-1}, X_r)$ 为空。由此可知，对于 $d \geq 1$, $V_{\mathrm{proj}} \cap V(X_0, \ldots\ldots, X_{r-1}, X_r^d)$ 为空。进而，这意味着如果 C是 V 的一个次数为 d 的乔形式 $C(\boldsymbol{e}_0, \ldots\ldots, \boldsymbol{e}_{r-1}, \boldsymbol{e}_{r,d}) \neq 0$，其中 $\boldsymbol{e}_i$是 X_i 的系数向量（对于 $0 \leq i < r$），而 $\boldsymbol{e}_{r,d}$是 X_r^d 的系数向量。

定义 3.8. 若 V处于正规位置，则对 $d \geq 1$，我们用 $C_{d,V}$ 表示 V的唯一 d次乔形式，使得 $C_{d,V}(\boldsymbol{e}_0, \ldots, \boldsymbol{e}_{r-1}, \boldsymbol{e}_{r,d}) = 1$。

3.3 特征多项式

我们的算法中所需的最后一类多项式是代数集的特征多项式。设 $V \subset \mathbb{K}^n$ 为一个 r-等维代数集，$\mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r]$为其乔形式所在的环。考虑新的变量组 $\boldsymbol{U}'_0, \ldots, \boldsymbol{U}'_r$，其中对所有 i, $\boldsymbol{U}'_i = T_i, U_{i,0}, \ldots, U_{i,n}$（$T_i$为一个新符号）。再定义 $\boldsymbol{v}_i = U_{i,0} - T_i, U_{i,1}, \ldots, U_{i,n}$。

定义 3.9. 设 V 为一个次数为 D的 r-等维代数集。V的特征多项式 是形如 $P = (-1)^D C(\boldsymbol{v}_0, \ldots, \boldsymbol{v}_r) \in \mathbb{K}[\boldsymbol{U}'_0, \ldots, \boldsymbol{U}'_r]$的所有多项式，其中 C 为 V的一个乔形式。

V的特征多项式是关于变量组 $\boldsymbol{U}'_i$ 的齐次多项式，其次数为 $D = \deg(V)$，对所有 i 均如此，因此其总次数为 rD。关于这一构造的几何动机，参见 [15, 第 3 节。1]

对于下一个引理，回想一下，在 $\mathbb{K}[\boldsymbol{U}'_0, \ldots, \boldsymbol{U}'_r]$ 中，我们使用由 $T_0 > U_{0,0} > \cdots > U_{0,n} > \cdots > T_r > U_{r,0} > \cdots > U_{r,n}$ 所诱导的分次字典序。

引理 3.10。 设 V 是一个次数为 D 且处于正规位置的 r-等维代数集，并设 C_V 是它的归一化乔形式。那么，$P_V = (-1)^D C_V(\boldsymbol{v}_0, \ldots, \boldsymbol{v}_r)$ 的首项为 $T_0^D U_{1,1}^D \cdots U_{r,r}^D$，首项系数为 *1*。

证明。记 $M_0 = T_0^D U_{1,1}^D \cdots U_{r,r}^D$。考虑乔形式$C$中一个单项式 $m = \boldsymbol{U}_0^{\boldsymbol{\alpha}_0} \cdots \boldsymbol{U}_r^{\boldsymbol{\alpha}_r}$，并令 M 为它在 $\boldsymbol{v}_0, \ldots, \boldsymbol{v}_r$ 处的取值。对于我们的单项式序，M 中的首项（相差一个符号）为 m'，这是将 m 中的$U_{i,0}$ 替换为 T_i 得到的（对所有 i）。我们知道，m 小于或等于 $U_{0,0}^D \cdots U_{r,r}^D$（引理 3.4），因此 m' 小于或等于 M_0。

由于 V 处于正规位置，其归一化 Chow 形式 C_V 包含单项式$U_{0,0}^D \cdots U_{r,r}^D$，其系数为 1；在 $\boldsymbol{v}_0, \ldots, \boldsymbol{v}_r$处的取值则包含上述单项式 M_0，其系数为 $(-1)^D$。

□

自然地，我们将 P_V 称为上述规范化的关于 V 的特征多项式。下一个引理可直接由引理 3.6 得出。

引理 3.11。 如果 V_1，……，V_s 是两两不同的不可约 r 维代数集，且都处于正规位置，并且 $V = V_1 \cup \cdots \cup V_s$，那么 $P_V = P_{V_1} \cdots P_{V_s}$。

3.4 簇的高度

最后，我们介绍本文所使用的簇的高度这一概念，沿用 [25, 16],并陈述其主要性质。

设 $V \subset \mathbb{C}^n$ 是 r 等维的，并在 $\mathbb{Q}$ 上定义；设 C 是 V 的任意一个乔形式，其系数属于 $\mathbb{Q}$。于是，我们定义

$$h(V) = \sum_{p \text{ prime}} \ln(|C|_p) + m(C, S_{n+1}^{r+1}) + (r+1)\deg(V) \sum_{i=1}^{n} \frac{1}{2i},$$

其中

- $|C|_p = \max_\alpha(|c_\alpha|_p)$，对 C 的所有非零系数 c_α 均成立，其中 $|\ |_p$ 是 p-进绝对值，定义为 $|p|_p = 1/p$，且 $|p'|_p = 1$ （p' 素数 $\neq p$），并通过乘法性将其扩展到 $\mathbb{Q} - \{0\}$,

- $m(C, S_{n+1}^{r+1})$ 是通常的马勒测度的一种变体，定义为在 $S_{n+1} \times \cdots \times S_{n+1}$ ($r+1$ 因子) 上对 $\ln(|C|)$ 积分，其中 S_{n+1} 是 $\mathbb{C}^{n+1}$ 中的单位球面，并赋予总质量为 1 的哈尔测度。

只要 C具有有理系数，结果就不依赖于 C的选取；定义在 $\mathbb{Q}$ 上的等维代数集 V 的高度，是其$\mathbb{Q}$-不可约分支的高度之和。最后，对于任意仍定义在 $\mathbb{Q}$上的 V，令 $h(V)$ 等于其等维分支的高度之和。

如果 V处于正规位置，我们强调了其 Chow 形式的一种特定选取，即归一化 Chow 形式 C_V；不过，引言中还指出了另一种可能：选取一个本原肖氏形式（因此具有整数系数） $C_V^{\text{primitive}}$，它在相差一个符号的意义下唯一。

引理 3.12. 当 V处于正规位置时，等式 $h(C_V) = h(C_V^{\text{primitive}})$ 成立。

证明. 因为 C_V的首项系数为 1，我们可以写成 $C_V = C_V^{\text{primitive}}/d$，其中 d 是 $C_V^{\text{primitive}}$ 的首项系数。由定义 2.1 可得 $h(C_V) = h(C_V^{\text{primitive}})$。 □

引理 3.13. 当 V 处于正规位置时，我们有

$$h(C_V) \leq h(V) + (r+1)\ln(n+2)\deg(V).$$

证明. 将 $C_V^{\text{primitive}}$ 代入 $h(V)$ 的表达式后， $h(V)$ 的定义中所有 p-进项都消失；于是剩下

$$h(V) = m(C_V^{\text{primitive}}, S_{n+1}^{r+1}) + (r+1)\deg(V)\sum_{i=1}^{n}\frac{1}{2i}.$$

令 $m(C_V^{\text{primitive}})$ 为多项式 $C_V^{\text{primitive}}$ 的马勒测度，即对环面 $S_1^{(r+1)(n+1)}$ 上的 $\ln(|C_V^{\text{primitive}}|)$ 积分。由 [16, 式 (1.2)]

$$m(C_V^{\text{primitive}}) \le m(C_V^{\text{primitive}}, S_{n+1}^{r+1}) + (r+1)\deg(V)\sum_{i=1}^{n}\frac{1}{2i} = h(V). \tag{4}$$

于是我们可以应用 [16, 引理 1.1]，，得到

$$h(C_V^{\text{primitive}} \le m(C_V^{\text{primitive}}) + (r+1)\ln(n+2)\deg(V) = h(V) + (r+1)\ln(n+2)\deg(V$$

而前一个引理使我们得以得出结论。 □

为了证明关于次数为 d 的乔形式的类似估计，我们将使用代数集 V 的局部高度，其定义见 [16] 的第 1.2.4 节。对于定义在 $\mathbb{Q}$ 上的 V、 r-等维且处于正规位置的情形，令

- $h_\infty(V) = m(C_V, S_{n+1}^{r+1}) + (r+1)\deg(V)\sum_{i=1}^{n}\frac{1}{2i}$
- $h_p(V) = \ln(|C_V|_p)$, p prime.

特别地，我们看到 $h(V) = h_\infty(V) + \sum_p h_p(V)$。由于 C_V 有一个系数等于 1，我们看到对于所有 p， $h_p(V) \ge 0$。无穷远处高度也同样如此；这一结论很可能是众所周知的，但我们没有找到相关文献。

引理 3.14。 对于处于正规位置的 V， $h_\infty(V) \ge 0$。

证明。 与前一个引理的证明中等式 (4) 中的做法相同（但这次应用于 C_V），我们使用 [16, 等式 (1.2)] 得到

$$m(C_V) \le m(C_V, S_{n+1}^{r+1}) + (r+1)\deg(V)\sum_{i=1}^{n}\frac{1}{2i} = h_\infty(V).$$

因此，我们只需证明 $m(C_V)$本身是非负的。

对于非零多项式 $P \in \mathbb{C}[Y_1, \dots, Y_t]$，我们有马勒测度之间的不等式 $m(P) \ge m(P_{d_1})$；若令 $P_{d_1} \in \mathbb{C}[Y_2, \dots, Y_t]$ 为其关于Y_1的首项系数（见 [4, 第 117]页），则成立。反复取首项系数，可推出 $m(P) \ge \ln(|\text{lc}_{\text{lex}}(P)|)$，其中 $\text{lc}_{\text{lex}}(P)$ 是多项式 P在字典序 $Y_1 > \cdots > Y_t$下的首项系数。

我们看到，归一化乔形式 C_V 在分次字典序 $U_{0,\ 0} > \cdots > U_{r,\ n}$下的首项为 $U_{0,\ 0}^D \cdots U_{r-1,\ r-1}^D U_{r,\ r}^D$，其中 $D = \deg(V)$ 且 $r = \dim(V)$，首项系数为 1。由于 C_V 是齐次的，它在字典序下也有相同的首项，因此结论成立。 □

前面的结论使我们能够推导出次数为 d 的乔形式的高度上界。只需对 $C_{d,\ V}[F]$ 在给定 F 的情况下给出高度上界即可（定义见小节末尾 3.1）。

引理 3.15。 假设 V 定义在 $\mathbb{Q}$上， r等维且处于正规位置。对于 $\mathbb{Z}[X_1,\ldots,X_n]$ 中的 $d\geq 1$和 F，若其次数至多为 d 且高度至多为 h，则有

$$h(C_{d,V}[F])\leq dh(V)+h\deg(V)+(r+1)\ln(n+1)d\deg(V).$$

证明。 中的引理2.1 给出了以下不等式：

- $m(C_{d,V}[F],S^r_{n+1})+rd\deg(V)\sum_{i=1}^n 1/2i\leq dh_\infty(V)+h\deg(V)+\ln(n+1)d\deg(V)$
- $h_p(C_{d,V}[F])\leq dh_p(V)$ if p is prime,

其中 $h_p(C_{d,\ V}[F])=\max(0,\ln(|C_{d,\ V}[F]|_p))$，其中 p为素数。 [16] 中的假设与我们的假设略有不同：该文献假设 $V\cap V(X_1,\ \ldots,\ X_r)$ 的基数等于 $\deg(V)$。然而，该假设仅用于证明（如引理 3.7中所示） V 处于正规位置。

由于 $C_{d,\ V}[F]$ 在每个变量组 $\boldsymbol{U}_i$中的次数至多为 $d\deg(V)$，根据 [16] 中的方程(1.2)，$C_{d,\ V}[F]$ 的马勒测度满足

$$m(C_{d,V}[F])\leq m(C_{d,V}[F],S^r_{n+1})+rd\deg(V)\sum_{i=1}^n\frac{1}{2i}.$$

因此，我们有 $m(C_{d,\ V}[F])\leq dh_\infty(V)+h\deg(V)+\ln(n+1)d\deg(V)$，而引理2.12在 [16] 给出

$$\ln(|C_{d,V}[F]|)\leq dh_\infty(V)+h\deg(V)+(r+1)\ln(n+1)d\deg(V),\tag{5}$$

其中，$|C_{d,\ V}[F]|$是 $C_{d,\ V}[F]$各系数绝对值的最大值。现在令$h_\infty(C_{d,\ V}[F])=\max(0,\ \ln(|C_{d,\ V}[F]|))$，并证明

$$h_\infty(C_{d,V}[F])\leq dh_\infty(V)+h\deg(V)+(r+1)\ln(n+1)d\deg(V)$$

- 若 $\ln(|C_{d,\ V}[F]|)\leq 0$，从而 $h_\infty(C_{d,\ V}[F])=0$，则由前一个引理可知，$h_\infty(V)\geq 0$，因此不等式成立，所以右侧整体非负
- 否则，结论可直接由等式 (5) 得出。

最后，我们利用这一观察 [16, p. 10]，即 C_d 的高度 $_V[F]$ 可表示为 $h(C_{d,V}[F])=h_\infty(C_{d,V}[F])+\sum_p h_p(C_{d,V}[F])$。将 $h_p(C_{d,V}[F])$（ p 为素数）和 $h_\infty(C_{d,V}[F])$ 的上界相加，得到 $h(C_{d,V}[F])\leq dh(V)+h\deg(V)+(r+1)\ln(n+1)d\deg(V)$。 □

4 使用乔形式进行基本运算

在本节中，我们介绍一些算法，通过乔形式对代数集进行基本的集合论运算；这些结果大多最初见于 [15]和 [2]。

这些算法通常以多元多项式作为输入；这些多项式旨在表示某些代数集的乔形式，有时还假设这些代数集处于正规位置。并非所有多元多项式都表示代数集的乔形式（参见 [12, 第 4]章中关于 Chow 簇的讨论）；对于不满足此类假设的输入，算法可能会返回（无意义的）输出，某些情况下也可能返回未定义。例如，记号 gcd(.,.) 表示两个多项式的首一最大公因式；如果两个参数都为零，则该记号未定义。遇到这种情况时，我们约定，尝试执行此计算的过程会立即中止，并同样返回未定义。其他会返回未定义的情况还包括发生除零。

在所有情况下，我们还会讨论输入定义在 $\mathbb{Q}$上的特殊情形，并给出关于素数 p的充分条件，以保证计算中的所有步骤都可以模 p进行。

4.1 并集

设 V_1, V_2 是定义在域 $\mathbb{K}$ 上的 r 维等维代数集，并设 C_1, C_2 是 V_1, V_2 的乔形式。根据定义， $V = V_1 \cup V_2$ 的乔形式是 C_1C_2 的无平方因子部分（其定义仅相差乘法常数）。我们将使用以下过程来计算这类多项式。

UNION_CHOW
INPUT: 多项式 C_1, C_2 属于 $\mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r]$，其中 $\boldsymbol{U}_i = U_{i,0}, \ldots, U_{i,n}$ 对所有 i
OUTPUT: 多项式 C 属于 $\mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r]$ 或未定义
1: $P \leftarrow C_1C_2$ 2: $Q \leftarrow \gcd(P, \partial P/\partial U_{0,0})$ 3: **返回** P/Q

注意，当 C_1 或 C_2 为零时（使用此过程时绝不会发生这种情况）， Q 未定义（因为只有当参数不同时为零时，我们才定义首一最大公因式）。

在正确性证明中，我们将采用以下假设：两个输入多项式分别与其关于 $U_{0,0}$ 的偏导数的最大公因式均为平凡的。对于处于正规位置的代数集，我们首先验证，在特征零域上该假设总是成立。

引理 4.1。 设 V 是定义在特征零域 $\mathbb{K}$ 上的 r-等维代数集。则对于 V 的任意乔形式，最大公因式$(C, \partial C/\partial U_{0,0}) = 1$。

证明。 假设 C 和 $\partial C/\partial U_{0,0}$ 有一个非常数不可约公因子 A，其系数属于 $\mathbb{K}$。若记 $C = AB$，其中 B是某个多项式，我们知道 A 不

整除 B （因为 C 在 $\mathbb{K}$上没有重因子）。对 U_0,0 求偏导数，可知 A 整除 $\partial A/\partial U_0$, $_0B + A\partial B/\partial U_0$,0，因此它整除 $\partial A/\partial U_0$,0。这只有在 $\partial A/\partial U_{0,0} = 0$时才可能；由于我们处于零特征下，这意味着$A$ 与 U_0无关。但是 A 是 V的一个不可约分支的乔形式，因此根据 [15,引理 3.7], ，它依赖于 U_0,0，矛盾。 □

引理 4.2. 假设 V_1 和 V_2 是定义在域 $\mathbb{K}$上的代数集，且二者要么为空，要么都是处于正规位置的 r-等维代数集。给定它们的归一化乔形式C_{V_1}, C_{V_2}，并假设 最大公因式(C_{V_1}, $\partial C_{V_1}/\partial U_{0,0}$) $=$最大公因式(C_{V_2}, $\partial C_{V_2}/\partial U_{0,0}$) $= 1$，且$\mathbb{K}$ 的特征不为二，则 Union Chow返回$V = V_1 \cup V_2$的归一化乔形式。

证明。写作 $V = \cup_i W_i \cup \cup_j Y_j \cup \cup_k Y'_k$，其中 W_i是 V_1 和 V_2共有的不可约分支， Y_j是仅属于 V_1 的不可约分支，而 Y'_k 是仅属于 V_2 的不可约分支。由于我们假设 V_1, V_2 处于正规位置，因此所有 W_i, Y_j, Y'_k 也都处于正规位置，于是 V（引理 3.6 的第一项），由此可得 $C_V = \prod_i C_{W_i} \prod_j C_{Y_j} \prod_k C_{Y'_k}$（引理 3.6 的第二项）。另一方面，我们还有 $C_{V_1} = \prod_i C_{W_i} \prod_j C_{Y_j}$和 $C_{V_2} = \prod_i C_{W_i} \prod_k C_{Y'_k}$（同一引理），因此 $P = C_{V_1} C_{V_2} = \prod_i C^2_{W_i} \prod_j C_{Y_j} \prod_k C_{Y'_k}$。

我们的最大公因式假设C_{V_1}、$\partial C_{V_1}/\partial U_0$和0) $= 1$ 意味着，对于所有 i， C_{W_i} 都不整除 $\partial C_{W_i}/\partial U_0$、$_0$：只有后者为零时才可能如此，但在这种情况下， C_{W_i} 会是 C_{V_1} 和$\partial C_{V_1}/\partial U_0$、$_0$的一个公因子。对于所有 C_{Y_j}，结论同样成立；考虑到C_{V_2}，对于所有 $C_{Y'_k}$也同样成立。

对给出 P的等式求导，我们得到

$$\frac{\partial P}{\partial U_{0,0}} = \sum_i \left(2C_{W_i} \frac{\partial C_{W_i}}{\partial U_{0,0}} \prod_{i' \neq i} C^2_{W_{i'}} \prod_j C_{Y_j} \prod_k C_{Y'_k} \right) + \sum_j \left(\frac{\partial C_{Y_j}}{\partial U_{0,0}} \prod_i C^2_{W_i} \prod_{j' \neq j} C_{Y_{j'}} \prod_k C_{Y'_k} \right)$$
$$+ \sum_k \left(\frac{\partial C_{Y'_k}}{\partial U_{0,0}} \prod_i C^2_{W_i} \prod_j C_{Y_j} \prod_{k' \neq k} C_{Y'_{k'}} \right).$$

P 及其偏导数可能具有的唯一公因子是 C_{W_i}（或其平方）、 C_{Y_j}和 $C_{Y'_k}$:

- 所有 C_{W_i}都整除$\frac{\partial P}{\partial U_{0,0}}$，但没有 $C^2_{W_i}$ 整除它，因为否则 C_{W_i} 将整除$2\partial C_{W_i}/\partial U_{0,\ 0}$ 这是不可能的，因为我们假设 2 在 $\mathbb{K}$中非零，并且已经看到 C_{W_i} 不整除其偏导数。

- 没有 C_{Y_j} 整除$\frac{\partial P}{\partial U_{0,0}}$，因为这将意味着它整除 $\frac{\partial C_{Y_k}}{\partial U_0}$, $_0$，而我们已经指出事实并非如此。

- 同理，没有$C_{Y'_k}$整除$\frac{\partial P}{\partial U_0}$, $_0$。——

我们推得， $Q =$最大公因式(P, $\partial P/\partial U_{0,0}$) 等于 $c \prod_i C_{W_i}$，其中 c 是某个非零常数。由于所有 C_{W_i} 的首项系数均为 1，它们的乘积也如此，因此

上述乘积的首项系数等于 c。由于 Q 是首一最大公因式，我们得到 $c=1$，进而得到 $Q=\prod_i C_{W_i}$。最后，输出 P/Q 为 $\prod_i C_{W_i}\prod_j C_{Y_j}\prod_k C_{Y'_j}$，我们已经看到它是 V 的归一化 Chow 形式。

□

引理 4.3。设 V_1 和 V_2 是定义在 $\mathbb{Q}$上的 $\mathbb{C}^n$中的代数集，二者要么都为空，要么都是处于正规位置的 r-等维代数集，其次数分别至多为 D_1、D_2，高度分别至多为 H_1、H_2。存在一个非零整数$\Delta^{\text{union}}_{V_1,V_2}$ 使得

$$h(\Delta^{\text{union}}_{V_1,V_2}) \in O(n^6(D_1+D_2)(H_1+H_2+D_1+D_2))$$

若素数 p p 不整除$\Delta^{\text{union}}_{V_1,V_2}$，则：

- C_{V_1}、C_{V_2}和$C=\text{UNION CHOW}(C_{V_1}$、$C_{V_2})$ 的系数属于 $\mathbb{Z}_{(p)}$，
- $\text{UNION\_CHOW}(C_{V_1}$ 模 p，C_{V_2} 模 $p)=C$ 模 p，
- $(C_{V_1}$ 模 p，$\partial C_{V_1}/\partial U_{0,\,0}$ 模 $p)=(C_{V_2}$ 模 p，$\partial C_{V_2}/\partial U_{0,\,0}$ 模 $p)=1$。

证明。我们先给出保证前两项成立的条件。输入多项式 C_{V_1}，C_{V_2}的次数分别至多为 $(r+1)D_1$和 $(r+1)D_2$，高度分别至多为 $H_1+(r+1)\ln(n+2)D_1$和 $H_2+(r+1)\ln(n+2)D_2$(引理 3.13)。

乘积 $P=C_{V_1}C_{V_2}$ 的次数至多为 $(r+1)(D_1+D_2)$，高度至多为$H=H_1+H_2+(r+1)\ln(n+2)(D_1+D_2)+\ln((r+1)(n+1)+1)(D_1+D_2)$（[16]中的引理 1.2.1.b）。其偏导数 $\partial P/\partial U_0$,0 的次数上界相同，高度至多为$H+\ln(D_1+D_2)$，因为 $\deg(P,U_0,0)\le D_1+D_2$。特别地，这两个多项式的高度均为 $O(n(H_1+H_2+D_1+D_2)\ln(n))$。

由于这些是关于 O 个n^2变量的多项式，根据引理 2.6，存在一个高度为 Δ_0 $O(n^6(D_1+D_2)(H_1+H_2+D_1+D_2))$ 的非零整数，使得如果 p不整除 Δ_0，P及其偏导数的系数属于 $\mathbb{Z}_{(p)}$，且第 2 步的最大公因式计算与模 p约化可交换。注意，由于 C_{V_1} 和 C_{V_2} 的首项系数均为 1，因此它们的乘积P 的系数属于 $\mathbb{Z}_{(p)}$ 意味着 C_{V_1} 和 C_{V_2} 本身也具有这一性质。

接着，引理 2.3 保证了第 3 步中进行的除法也与模 p 约化可交换（注意，Q 是首一最大公因式，因此模 p时不可能为零）。总之，若 p 不整除 Δ_0，则前两项成立。

最后，我们给出保证第三项成立的条件。由引理 4.1 可知，$\gcd(C_{V_1},\partial C_{V_1}/\partial U_{0,0})=1$。再次应用引理 2.6，可得存在一个非零整数 Δ_1，其渐近高度界与 Δ_0 相同，并且若 p 不整除Δ_1，则 C_{V_1} 的系数属于 $\mathbb{Z}_{(p)}$（我们已知这也可由 p 不整除 Δ_0 推出），且 $\gcd(C_{V_1}$ 模 p,$\partial C_{V_1}/\partial U_{0,0}$ 模 $p)=1$。对 C_{V_2} 重复此过程，定义一个非零整数 Δ_2，并令 $\Delta^{\text{union}}_{V_1,V_2}=\Delta_0\Delta_1\Delta_2$。

□

4.2 标量扩张与一般投影

考虑一个定义在域 $\mathbb{K}$ 上的 r 等维代数集 V，以及新变量$\ell_{i,\,1}$，……，$\ell_{i,\,n}$，$i=0$，……，r。令 $\mathbb{L}$ 为 $\mathbb{K}(\ell_{0,\,1}$，……，$\ell_{r,\,n})$ 的代数闭包，并令 $V_{\mathbb{L}}\subset\mathbb{L}^n$

为 V在 $\mathbb{L}$上的扩张，即理想 $I(V)\cdot\mathbb{L}[X_1,\dots,X_n]$ 的零点集。以下简单的观察将在第 4.4 节中用到。

引理 4.4. 设 $I(V)=\cap_i P_i$ *in* $\mathbb{K}[X_1,\dots,X_n]$ 是 $I(V)$ 的素理想极小分解。那么：

- 我们有 $I(V_{\mathbb{L}})=I(V)\cdot\mathbb{L}[X_1,\dots,X_n]$，其极小主分解为 $\cap_i(P_i\cdot\mathbb{L}[X_1,\dots,X_n])$，其中右侧所有理想都是素理想。
- 对所有 i，若 C 是 $V(P_i)\subset\mathbb{K}^n$的乔形式，则 C 也是$V(P_i\cdot\mathbb{L}[X_1,\dots,X_n])\subset\mathbb{L}^n$的乔形式。

证明。令 $P_i'=P_i\cdot\mathbb{L}[X_1,\dots,X_n]$对所有 i成立。所有 P_i'仍为根式这一事实由 [26,引理 10.44.4]得出。另一方面，由 [26, 引理 10.47.2] 可知，对所有 i，$\mathbb{L}[X_1,\dots,X_n]/P_i'$只有一个极小素理想；又由于它是约化的，因此是一个整环。这表明所有P_i'都是素理想。由于 $\mathbb{L}[X_1,\dots,X_n]$是自由的，因而是平坦的 $\mathbb{K}[X_1,\dots,X_n]$-代数，扩张与交可交换 [20, 定理 7.4.(i)]。这表明 $I(V)\cdot\mathbb{L}[X_1,\dots,X_n]=\cap_i P_i'$，因此该理想是根式；于是它必等于 $I(V_{\mathbb{L}})$。由于该扩张也忠实平坦，$P_i'\cap\mathbb{K}[X_1,\dots,X_n]=P_i$对所有 i成立，因此这些 P_i'两两不同，并且没有任何一个 P_i'包含在其余项的交中。这表明它们的交是 $I(V_{\mathbb{L}})$的极小主分解。

对于第二项：$V(P_i)$ 的乔形式 C 生成消去理想 $(P_i+(U_{j,0}+U_{j,1}X_1+\cdots+U_{j,n}X_n)_{0\le j\le r})\cap\mathbb{K}[\boldsymbol{U}_0,\dots,\boldsymbol{U}_r]$（验证这一点时，注意该理想是素理想，因为 P_i 是素理想，而且每个新方程都有新的首项$U_{j,0}$），并且在 $\mathbb{L}$ 上这一性质仍然成立。 □

不定元 $(\ell_{i,j})$ 用作线性形式 $L_i=\ell_{i,1}X_1+\cdots+\ell_{i,n}X_n, i=0,\dots,r$ 的系数。这使我们能够定义一般投影

$$\pi:\boldsymbol{x}=(x_1,\dots,x_n)\mapsto(L_0(\boldsymbol{x}),\dots,L_r(\boldsymbol{x})).$$

像 $\pi(V_{\mathbb{L}})$ 是 $\mathbb{L}^{r+1}$ 中的扎里斯基闭集，它定义在 $\mathbb{K}(\ell_{0,1},\dots,\ell_{r,n})$ 上。我们的目标是计算一个 $\mathbb{K}[\ell_{0,1},\dots,\ell_{r,n}][X_1,\dots,X_n]$ 中的多项式，使其在 $\mathbb{L}^n$ 中的零点集为柱体 $\pi^{-1}(\pi(V_{\mathbb{L}}))$.

GENERIC PROJECTION CHOWINPUT: 多项式 C在 $\mathbb{K}[\boldsymbol{U}_0,\dots,\boldsymbol{U}_r]$中，带有$\boldsymbol{U}_i=U_{i,0},\dots\dots,U_{i,n}$对于所有 iOUTPUT: 多项式 F在 $\mathbb{K}[\ell_{0,1},\dots,\ell_{r,n}][X_1,\dots,X_n]$中。1:
返回 $C(L_0,\ -\ell_{0,1},\dots\dots,\ -\ell_{0,n},\dots\dots,\ L_r,\ -\ell_{r,1},\dots\dots,\ -\ell_{r,n})$

引理 4.5. 假设 V 为空集，或是一个$\mathbb{K}$域上定义的 r等维集合，并令 $V_{\mathbb{L}}$ 为 $I(V)$ 在 $\mathbb{K}(\ell_{0,1},\dots,\ell_{r,n})$ 的代数闭包 $\mathbb{L}$ 上的零点集。给定 V 的乔形式 C，
GENERIC PROJECTION CHOW 会返回一个多项式 F，使得$V(F)=\pi^{-1}(\pi(V_{\mathbb{L}}))$ 属于 $\mathbb{L}^n$。

证明。当 V 为空集时，无需证明，因为 C 因而 F 都是非零常数。否则，该结果已在 [2], 的命题15中证明，但我们可以沿用本文的记号重复这一简短论证。点 $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{L}^n$ 消去 F，当且仅当 $(\ell_{0,1}x_1 + \cdots + \ell_{0,n}x_n, -\ell_0, 1, \ldots, -\ell_{0,n}, \ldots, \ell_{r,1}x_1 + \cdots + \ell_{r,n}x_n, -\ell_r, 1, \ldots, -\ell_{r,n})$ 消去 C。现在，C 也是 $V_{\mathbb{L}}$ 的一个乔形式，因此，若以 $V\text{proj}_{\mathbb{L}}$ 表示 $V_{\mathbb{L}}$ 的射影闭包，则当且仅当存在 $\boldsymbol{y} = (y_0 : \cdots : y_n)$ 属于 $V\text{proj}_{\mathbb{L}}$，使得

$$y_0(\ell_{0,1}x_1 + \cdots + \ell_{0,n}x_n) = \ell_{0,1}y_1 + \cdots + \ell_{0,n}y_n$$
$$\cdots$$
$$y_0(\ell_{r,1}x_1 + \cdots + \ell_{r,n}x_n) = \ell_{r,1}y_1 + \cdots + \ell_{r,n}y_n.$$

如果 $y_0 = 0$，所有 $y_1\ell_{i,1} + \cdots + y_n\ell_{i,n}$ 都为零，那么所有 $y_0\ell_{i,0} + y_1\ell_{i,1} + \cdots + y_n\ell_{i,n}$ 也都为零；这意味着 $C(\ell_0, 0, \ldots, \ell_{r,n}) = 0$，矛盾。因此，$F(\boldsymbol{x}) = 0$ 当且仅当存在 $\boldsymbol{y} = (y_1, \ldots, y_n)$ 属于 $V_{\mathbb{L}}$，使得对所有 i，都有 $\ell_{i,1}x_1 + \cdots + \ell_{i,n}x_n = \ell_{i,1}y_1 + \cdots + \ell_{i,n}y_n$，也就是说，使得 $\pi(\boldsymbol{x}) = \pi(\boldsymbol{y})$。

□

注记 4.6。将 $G_{\mathbb{L}}$ 关于 $\ell_{0,\ 1}, \ldots, \ell_{s,\ n}$ 展开并取系数，得到一族关于 $\mathbb{K}[X_1, \ldots, X_n]$ 的多项式，其零点集为 W。另请参见 [2],中的相关构造，其中使用随机线性形式代替。

□

请注意，此处无需要求 V 处于正规位置，尽管使用这一过程时会满足正规位置假设。不过，对于下面的引理，我们将作出正规位置假设。

引理4.7。设 V 是定义在 $\mathbb{Q}$ 上的 $\mathbb{C}^n$ 中的代数集，它要么为空，要么是 r 等维且处于正规位置，其次数至多为 D，高度至多为 H。那么 Generic Projection Chow(C_V) 是一个关于 $X_1, \ldots, X_n$ 的多项式，其次数至多为 D，关于 $\ell_{0,1}, \ldots, \ell_{r,n}$ 的次数至多为 $(r+1)D$，且高度为 $O(H + nD\ln(n))$。

证明。次数的界显然成立。我们知道，C_V 的高度至多为 $H' = H + (r+1)D\ln(n+2)$（引理 3.13）；与该引理的证明一样，我们可以将其写成商 $C_V^{\text{primitive}}/d$，其中 d 是一个高度至多为 H' 的整数，$C_V^{\text{primitive}}/d$ 是 V 的本原肖氏形式，其整数系数的高度也至多为 H'（引理 3.12）。将 C_V 代入 $L_0, -\ell_0, 1, \ldots, -\ell_{0,n}, \ldots, L_r, -\ell_r, 1, \ldots, -\ell_{r,n}$，得到多项式 $1/d\, C_V^{\text{primitive}}(L_0, -\ell_0, 1, \ldots, -\ell_{0,n}, \ldots, L_r, -\ell_r, 1, \ldots, -\ell_{r,n})$。

我们将分子的高度估计为关于 $\mathbb{Z}[\ell_{0,1}, \ldots, \ell_{r,n}, X_1, \ldots, X_n]$ 的多项式。多项式 $C_V^{\text{primitive}}$ 有 $(r+1)(n+1) \in O(n^2)$ 个变量，次数至多为 $(r+1)D$，高度至多为 H'；这些自变量有 $(r+2)n \in O(n^2)$ 个变量，次数至多为二，高度为零。由 [16] 的引理 1.2.1.c 可知，结果的高度为 $O(H' + nD\ln(n))$。

□

4.3 超曲面分离

给定 $\mathbb{K}^n$ 中的两个代数集 V, Y，我们定义集合论运算

$$V_{\text{zero}}, V_{\text{proper}} = \text{Separate}(V, Y)$$

令 V_{zero} 为 Y 中包含的 V 的不可约分支之并，令 V_{proper} 为 V 中所有其他不可约分支之并（这两个集合中的任一个都可能为空）。

在本段中，我们讨论 V 为等维且处于正规位置，而 $Y = V(G)$ 为超曲面的情形。我们回顾 Jeronimo 等人 [15]提出的一个过程，该过程以 G 和 V 的归一化 Chow 形式作为输入，并返回 V_{zero} 和 V_{proper}的归一化 Chow 形式。我们从以下子程序开始：该子程序以环 G 上的、关于变量 X_1、……、 X_n 的多项式 $\mathbb{A}$以及齐次化变量 X_0作为输入；输出为 G的齐次化。

HomogenizeInput: 多项式 G 关于 $\mathbb{A}[X_1, \ldots, X_n]$Input: 个变量 X_0 以及 $(X_1$、……、 $X_n)$Input: 整数 dOutput: 中的齐次多项式 $\mathbb{A}[X_0, X_1, \ldots, X_n]$1: **返回** $\sum_{\boldsymbol{\alpha} \in \mathbb{N}^n,\ |\boldsymbol{\alpha}| \le d}$ 系数$(G,$ $X_1^{\alpha_1} \cdots X_n^{\alpha_n})X_0^{d-|\boldsymbol{\alpha}|} X_1^{\alpha_1} \cdots X_n^{\alpha_n}$

话虽如此，以下是超曲面情形下的分离过程；它返回未定义 当其第一个输入，即多项式 C，为零时（在我们将其用于主过程时不会发生这种情况）。至于并运算，我们假设 C_V 与$\partial C_V / \partial U_{0,\ 0}$ 没有公因子，而引理 4.1 表明该假设在零特征下始终成立。

Separate_Hypersurface_ChowInput: 多项式 C于 $\mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r]$，其中 $\boldsymbol{U}_i = U_i$,0, . . . ,$U_{i,n}$ 对所有 iInput: 多项式 G 于 $\mathbb{K}[X_1, \ldots, X_n]$Output: 多项式 K, L 于 $\mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r]$ 或未定义 1: $D \leftarrow$ deg$(C,U_{r,r})$ 2: $P \leftarrow (-1)^D C(\boldsymbol{v}_0, \ldots, \boldsymbol{v}_r)$ 其中 $\boldsymbol{v}_i = U_i$, $_0 - T_i, U_i$,1, . . . ,$U_{i,n}$ 对所有 $i, T_0, \ldots, T_r$ 新变量 3: $G^h \leftarrow$ Homogenize$(G, X_0, (X_1, \ldots, X_n),$ deg$(G))$▷ G 的齐次化，使用一个新变量 $X_0$4: $G[P] \leftarrow G^h\left(\frac{\partial P}{\partial T_0}, -\frac{\partial P}{\partial U_{0,1}}, \ldots, -\frac{\partial P}{\partial U_{0,n}}\right)$5: $Q \leftarrow$最大公因式$(P, G[P])$ 6: $R \leftarrow P/Q$7: 返回 $(-1)^{\deg(Q,T_0)}Q(T_0 = \cdots = T_r = 0), (-1)$ $^{\deg(R,T_0)}R(T_0 = \cdots = T_r = 0)$

引理 4.8. 设 V 为空集，或为 r-等维且处于正规位置，并且定义在域 $\mathbb{K}$上。给定其归一化乔形式 C_V以及 G，其中 $\mathbb{K}[X_1, \ldots, X_n]$，并假设 最大公因式$(C_V,\partial C_V/\partial U_{0,0}) = 1$, Separate Hypersurface Chow 分别返回 V_{zero}、 $V_{\text{proper}} =$ separate$(V, V(G))$的归一化乔形式。

证明. V为空集的情形显然（因为此时 $C = P = Q = R = 1$）。否则，我们先证明多项式 P和 $\partial P/\partial T_0$ 的最大公因式为常数。

假设并非如此，则存在 P的一个不可约因子 Q，它整除 $\partial P/\partial T_0$。由构造可知， P的不可约因子与 C_V的不可约因子一一对应，

特别地，P没有重因子（因为C_V没有）。这意味着Q必须整除$\partial Q/\partial T_0$，从而有$\partial Q/\partial T_0 = 0$。另一方面，我们知道$Q = (\pm 1)B(\boldsymbol{v}_0, \ldots, \boldsymbol{v}_r)$，其中$B$是$C_V$的一个不可约因子，并且对所有$i$有$\boldsymbol{v}_i = U_i, {}_0 - T_i, U_i, 1, \ldots, U_{i,n}$。由此得到$\partial Q/\partial T_0 = (\pm 1)\partial B/\partial U_0, 0(\boldsymbol{v}_0, \ldots, \boldsymbol{v}_r)$，故$\partial B/\partial U_{0,0} = 0$。但这样一来，$B$是$C_V$与$\partial C_V/\partial U_0, 0$的公因子，这与我们的假设最大公因式$(C_V, \partial C_V/\partial U_0, 0) = 1$相矛盾。

最大公因式$(P, \partial P/\partial T_0) = 1$等价于说，$\partial P/\partial T_0$在$V(P)$的任何不可约分支上都不恒为零。由此可知，[15, 引理 3.9]的证明表明，Q = 最大公因式$(P, G[P])$是V_{zero}的一个特征多项式（该文献假设为零特征，在那里不会出现此类问题）。由于V处于正规位置，V_{zero}也同样如此（引理3.6），因此后者有唯一的规范化特征多项式。由于规范化特征多项式和首一最大公因式的首项系数都为 1（前者由引理 3.10保证），可知Q实际上就是这个规范化特征多项式。

另一方面，P本身就是V的规范化特征多项式。由引理 3.11 可知，R是V_{proper}的规范化特征多项式。将所有T_i在 0 处取值，便得到V_{zero}和V_{proper}的乔形式。要将它们规范化，只需分别将其符号调整为$(-1)^{\deg(V_{\text{zero}})}$和$(-1)^{\deg(V_{\text{proper}})}$；根据引理3.10，这些次数恰好是$Q$和$R$在$T_0$中的次数。 □

引理 4.9。设V是定义在$\mathbb{Q}$上的代数集，且包含于$\mathbb{C}^n$中；它要么为空，要么是r等维且处于正规位置，其次数至多为D，高度至多为H；另设G的次数至多为d，高度至多为h。存在一个非零整数$\Delta_{VG}^{\text{separate H}}$，满足

$$h(\Delta_{V,G}^{\text{separate\_H}}) \in O(n^6 D(d\ln(d) + h + dH + dD))$$

使得若素数p不整除$\Delta_{VG}^{\text{separate H}}$，则：

- C_V，G和K，$L = \text{Separate Hypersurface Chow}(C_V, G)$的系数属于$\mathbb{Z}_{(p)}$
- $\text{Separate_Hypersurface_Chow}(C_V$模$p$，$G$模$p) = K$模$p$，$L$模$p$
- $(C_V$模p，$\partial C_V/\partial U_{0,0}$模$p) = 1$。

证明。将$C_V = C'/c$和$G = G'/g$改写为如下形式：其中c、g是整数，$C' = C_V^{\text{primitive}}$、$G'$具有整数系数，$c$、$C'$的高度至多为$H' = H + (r+1)D\ln(n+2)$（引理 3.12、3.13），而$g$、$G'$的高度至多为$h$。我们的首要要求是$p$不整除$\Delta_0 = c\,g\,\text{lc}(G')$。前两个因子非零，确保了$C_V$和$G$的系数属于$\mathbb{Z}_{(p)}$；最后一个条件则确保$G$或$G'$的次数模$p$后不会下降（因为我们使用分次序）。

- 在第 1 步，多项式C_V和C_V模p在$U_{r,r}$中的次数相同，因为C_V的首项为$U_0^D, {}_0 \cdots U_{r,r}^D$。
- 步骤 2 计算出$P = P'/c$，其中$P' = (-1)^D C'(\boldsymbol{v}_0, \ldots\ldots, \boldsymbol{v}_r)$的次数至多为$(r+1)D$，且具有整数系数。我们知道$C'$的高度至多为$H'$，因此$P'$的高度至多为$H' + rD$。

- 在步骤 3 中，由于 G 的次数模 p 后不下降，因此有等式 $(G \text{ 模 } p)^h = G^h$ 模 p。此外，G^h 可以写成 $G^h = G'^h/g$，其中 G'^h 是 G'的齐次化，其齐次次数至多为 d，且系数为高度至多为 h的整数。

- 在第 4 步，我们有 $G[P] = G'[P]/g = 1/(c\deg(G)g)G'[P']$。$P'$ 的所有偏导数的次数至多为 $(r+1)D$，高度至多为 $H'' = H' + rD + \ln(D)$，因此多项式 $G'[P']$ 的次数至多为 $(r+1)dD$，高度至多为 $h + d(H'' + \ln(n+2) + \ln((r+1)(n+2))(r+1)D)$，根据 [16]的引理 1.2.1.c。

- 现在我们可以对多项式 P' 和 $G'[P']$应用引理 2.6，其中 $d_F \in O(nD)$，$h_F \in O(H + n\ln(n)D)$，$d_G \in O(ndD)$，$h_G \in O(h + dH + dn\ln(n)D)$，以及 $s \in O(n^2)$。这表明存在一个非零整数 Δ_1 使得

$$h(\Delta_1) \in O(n^6 D(d\ln(d) + h + dH + dD))$$

  使得如果 p 不能整除 $\Delta_0\Delta_1$，第 5 步模 p 后仍然运行良好，尤其表明这一步的结果具有 $\mathbb{Z}_{(p)}$ 中的系数。

- 随后用引理 2.3 处理第 6 步中的商（因为最大公因式 Q 是首一的，所以模 p 后不会消失），而在第 7 步清除 Q 和 R 中的变量 T_i 并无困难。由于 Q 和 R 的首项分别为 $(T_0U_{1,1}\cdots U_{r,r})^{\deg(Q,T_0)}$ 和 $(T_0U_{1,1}\cdots U_{r,r})^{\deg(R,T_0)}$，且首项系数为 1（引理 3.10），当我们模 p 运行算法时，次数 $\deg(Q,T_0)$ 和 $\deg(R,T_0)$ 不会改变。

由此可知，如果 p 不能整除 $\Delta_0\Delta_1$，则引理中的前两个性质成立。为证明最后一个性质，如引理 4.3 的证明所示，p 应避免整除高度为 $O(n^6D(D+H))$ 的非零整数 Δ_2。我们取 $\Delta^{\text{separate}}_{\text{H}\,V,G} = \Delta_0\Delta_1\Delta_2$，引理得证。 □

4.4 一般情形下的分离

现在，我们讨论如下情形：两个输入 V、W 均由其乔形式给出，因此特别地，V和 W 都是等维的，但我们不再假设 W 是超曲面。过程如下；由于它使用
SEPARATE HYPERSURFACE CHOW，可能会返回未定义，不过我们将在下文证明，对于合法输入（代数集的乔形式，且第一个处于正规位置），输出是正确的。

SEPARATE_CHOW
INPUT: 多项式 C 在 $\mathbb{K}[\boldsymbol{U}_0,\ldots,\boldsymbol{U}_r]$中，其中 $\boldsymbol{U}_i = U_{i,0}, \ldots\ldots, U_{i,n}$ 对所有 i
INPUT: 多项式 D 在 $\mathbb{K}[\boldsymbol{U}_0,\ldots,\boldsymbol{U}_s]$中，其中 $\boldsymbol{U}_i = U_{i,0}, \ldots\ldots, U_{i,n}$ 对所有 i
OUTPUT: 多项式 Q，R 在 $\mathbb{K}[\boldsymbol{U}_0,\ldots,\boldsymbol{U}_r]$ 中，或未定义1:
$G_{\mathbb{L}} \leftarrow$ GENERIC PROJECTION CHOW(D)2: **返回**
SEPARATE HYPERSURFACE CHOW(C, $G_{\mathbb{L}}$)

引理 4.10. 设 V 为空，或为处于正规位置的 r等维对象；设W 为空，或为 s等维对象，二者均定义在域 $\mathbb{K}$ 上。给定的归一化

乔形式 C_V和 W的乔形式 D，并假设 最大公因式$(C_V, \partial C_V/\partial U_{0,0}) = 1$，
SEPARATE CHOW 分别返回 V_{zero}、V_{proper} =SEPARATE(V, W)的归一化乔形式。

证明。令 π 如第4.2节所述，令 $W_{\mathbb{L}}$ 为 $I(W)$ 在 $\mathbb{K}(\ell_0,1,\ldots,\ell_{s,n})$ 的代数闭包$\mathbb{L}$ 上的零点集，并令 $G_{\mathbb{L}}$ = GENERIC PROJECTION CHOW(D)。由引理 4.5，$V(G_{\mathbb{L}}) = \pi^{-1}(\pi(W_{\mathbb{L}}))$，其中左右两端均属于 $\mathbb{L}^n$。

对于 $\boldsymbol{x}$ 中的 $\mathbb{K}^n$，我们断言，$\boldsymbol{x}$ 属于 W 当且仅当它属于 $V(G_{\mathbb{L}})$（当然，这并不意味着 $W = V(G_{\mathbb{L}})$，因为后一个集合包含于 $\mathbb{L}^n$）。若 $\boldsymbol{x}$ 属于 W，它也属于 $W_{\mathbb{L}}$，因而属于 $V(G_{\mathbb{L}})$。反向结论由 [2] 的命题3得出：给定不属于 W 的 $\boldsymbol{x}$，该命题证明存在一个非空的Zariski开集 $O_{\boldsymbol{x}}$，W 属于 $\mathbb{K}^{(n+1)(r+1)}$，使得对于 $O_{\boldsymbol{x},W}$ 中的 $(\lambda_0,0,\ldots,\lambda_{r,n})$，若令

$$\pi_\lambda : \boldsymbol{z} \mapsto (\lambda_{0,0} + \lambda_{0,1}z_n + \cdots + \lambda_{0,n}z_n, \ldots, \lambda_{r,0} + \lambda_{r,1}z_n + \cdots + \lambda_{r,n}z_n),$$

那么 $\pi_\lambda(\boldsymbol{x})$不是 在 $\pi_\lambda(W)$ 中。如果 $\pi(\boldsymbol{x})$ 在 $\pi(W_{\mathbb{L}})$ 中，则存在 $\boldsymbol{y} = (y_1, \ldots\ldots, y_n)$ 在 $W_{\mathbb{L}}$ 中，使得

$$\ell_{i,1}x_n + \cdots + \ell_{i,n}x_n = \ell_{i,1}y_1 + \cdots + \ell_{i,n}y_n, \quad i = 0, \ldots, r.$$

由此可知，对于 $\mathbb{K}^{(n+1)(r+1)}$ 中的一般点 $(\lambda_{0,\,0}, \ldots\ldots, \lambda_{r,\,n})$，存在 W 中的 $\boldsymbol{z} = (z_1, \ldots\ldots, z_n)$，使得

$$\lambda_{i,1}x_n + \cdots + \lambda_{i,n}x_n = \lambda_{i,1}z_1 + \cdots + \lambda_{i,n}z_n, \quad i = 0, \ldots, r,$$

从而 $\pi_\lambda(\boldsymbol{x}) = \pi_\lambda(\boldsymbol{z})$，这就产生了矛盾。因此，$\pi(\boldsymbol{x})$ 不在 $\pi(W_{\mathbb{L}})$ 中；根据 $G_{\mathbb{L}}$ 的定义，这意味着 $G_{\mathbb{L}}(\boldsymbol{x}) \neq 0$。

现在，考虑 $V_{\mathbb{L}}$ 的一个不可约分支 $V'_{\mathbb{L}}$。我们在引理 4.4 中看到，存在 V 的一个不可约分支 V'，使得 $I(V'_{\mathbb{L}}) = I(V') \cdot \mathbb{L}[X_1, \ldots, X_n]$。如果 V' 包含于 W，则可知 $V'_{\mathbb{L}}$ 包含于 $W_{\mathbb{L}}$，因而包含于 $\pi^{-1}(\pi(W_{\mathbb{L}})) = V(G_{\mathbb{L}})$。如果 V' 不包含于 W，那么它包含一个不属于 W 的点 $\boldsymbol{x} \in \mathbb{K}^n$。于是，根据上一段中的断言，$\boldsymbol{x}$ 不在 $V(G_{\mathbb{L}})$ 中，因此 V' 和 $V'_{\mathbb{L}}$ 都不包含于 $V(G_{\mathbb{L}})$。

换言之，若令 Y，Y' = SEPARATE$(V_{\mathbb{L}}, V(G_{\mathbb{L}}))$，$Y$就是所有满足以下条件的这些 $V'_{\mathbb{L}}$ 的并集：$V' \subset W$，而 Y' 则是其余所有 $V'_{\mathbb{L}}$的并集。由引理 4.4的第二点，我们推知，它们的归一化乔形式分别是V_{zero}，V_{proper} = SEPARATE(V, W)。

由于我们假设 V要么为空，要么处于正规位置，且最大公因式$(C_V, \partial C_V/\partial U_{0,\,0}) = 1$，因此 $V_{\mathbb{L}}$也满足这一条件，因为 C_V 仍是它的一个乔形式（这也可由引理 4.4的第二点推出）。于是，我们可以对4.8 应用引理 C_V 和 $G_{\mathbb{L}}$，从而完成证明。 □

引理 4.11。设 V 和 W 是 $\mathbb{C}^n$中的代数集，定义在 $\mathbb{Q}$上，二者要么为空，要么分别是 r-等维（分别为 s-等维）且处于正规位置，其次数分别不超过 D_V、D_W，高度分别不超过 H_V、H_W。存在一个非零整数$\Delta_{V,W}^{\text{separate}}$，使得

$$h(\Delta_{V,W}^{\text{separate}}) \in O(n^6 D_V(D_W \ln(D_W) + H_W + D_W H_V + D_V D_W))$$

使得如果素数 p 不整除 $\Delta_{V,W}^{\text{separate}}$，，则：

- C_V， C_W和 K， $L = \text{SEPARATE CHOW}$（C_V， C_W）的系数属于 $\mathbb{Z}_{(p)}$
- SEPARATE_CHOW(C_V模 p， C_W模 p) $= K$模 p， L模 p
- 最大公因式(C_V模 p， $\partial C_V/\partial U_{0,\,0}$模 p) $= 1$。

证明。证明与引理 4.9 的证明类似，取 $G = G_{\mathbb{L}}$。我们引入相同的多项式 C'、 P'、 G'和 G'^h，其中 P'的次数仍为 $O(nD_V)$，高度为 $O(H_V + nD_V \ln(n))$；现在，根据引理4.7， G'^h在 X_1中的次数为 $O(D_W)$，.....在ℓ_0中的次数为 $O(nD_W)$，1，.....， ℓ_s， n，高度为 $O(H_W + nD_W \ln(n))$。同样，首先要保证 P' 和 G' 中的分母模 p不为零，并且将 G 模 p 取模后，其次数不变。按照引理 4.9 的方法即可做到：只要 p 不整除某个高度为 $O(H_V + H_W + n(D_V + D_W)\ln(n))$的非零整数 Δ_0，这一条件就成立。

剩下的工作是给出一些条件，使得 Q'（即 P'和 $G'[P']$的首一最大公因式）在模 p下的计算能够良好约化。这是在变量 T_i， $U_{i,\,0}$，.....， $U_{i,\,n}$下，基域为 $\mathbb{Q}(\ell_{0,\,1}$，.....， $\ell_{s,\,n})$ 的最大公因式。不过，由于 P'属于 $\mathbb{Q}[T_0, \ldots, U_{r,n}]$， Q'属于$\mathbb{Q}[T_0, \ldots, U_{r,n}]$，因此它也是 P'和 $G'[P']$在 $\mathbb{Q}[\ell_{0,1}, \ldots, \ell_{s,n}, T_0, \ldots, U_{r,n}]$中的首一最大公因式。同样，对于任意不整除 Δ_0的素数 p p， P'模 p与$G'[P']$模 p的最大公因式可以在 $\mathbb{F}_p[\ell_{0,1}, \ldots, \ell_{s,n}, T_0, \ldots, U_{r,n}]$中计算。

于是我们可以再次应用引理 2.6，这次应用于多项式 P' 和 $G'[P']$，它们属于$\mathbb{Q}[\ell_{0,1}, \ldots, \ell_{s,n}, T_0, \ldots, U_{r,n}]$中的多项式。这些多项式有 $O(n^2)$ 个变量，其中前者的次数为 $O(nD_V)$，高度为 $O(H_V + nD_V \ln(n))$；后者的次数为 $O(nD_V D_W)$，高度为 $O(H_W + nD_W H_V + n^2 D_V D_W \ln(n))$。由此引理可知，存在一个高度为 Δ_1 的整数

$$h(\Delta_1) \in O(n^6 D_V (D_W \ln(D_W) + H_W + D_W H_V + D_V D_W))$$

使得如果 p 不整除 $\Delta_0\Delta_1$，那么最大公因式计算模 p (因此这一步的结果的系数属于 $\mathbb{Z}_{(p)}$) 可顺利进行。最后的除法再次由引理 2.3处理。

与引理 4.9 中一样，我们还需要保证 gcd(C_V模 p， $\partial C_V/\partial U_{0,\,0}$模 p) $= 1$；当 p不整除高度为 $O(n^6 D_V(D_V + H_V))$ 的非零整数 Δ_2 时，这一条件成立。我们取 $\Delta_V^{\text{separate}}$，$_W = \Delta_0\Delta_1\Delta_2$；其高度的上界与 Δ_1 的高度具有相同的渐近表达式。 □

4.5 计算次数为 d 的乔形式

取一个次数为 D、处于正规位置的 V r-等维对象，并假设已知其归一化乔形式 C_V。对于次数为 $d \geq 1$ 的 F，我们回顾 [15], 用于计算 $C_{d,\,V}[F]$ 的另一项结果（符号见第 3.1 节），其中 $C_{d,\,V}$是 V 的规范化次数为 d 的乔形式。

我们需要一个简单的子程序 PSEUDO-COMPANION，它以多项式 $P(T)$ 为输入，该多项式的次数为 D，并返回 P/a 的友矩阵乘以 a（无需进行除法或乘法，所有元素都是 P 的系数）。

在算法中，我们在多元多项式环中进行了一次除法（步骤 11）。在我们之前看到的算法中，所有除法都保证是精确的，因为它们的形式都是

P/最大公因式(P, ...)。在此例中，并非所有输入都满足这一条件，因此为涵盖所有可能情况，当除法不精确时，我们返回未定义。与往常一样，在下面的引理中，我们会指出，在我们关心的所有情况下，除法都是精确的。

DEGREE_d_CHOW_FORMINPUT: 多项式 C 于 $\mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r]$，其中 $\boldsymbol{U}_i = U_i$,0, . . . ,$U_{i,n}$ 对所有 iINPUT: 多项式 F 于 $\mathbb{K}[X_1, \ldots, X_n]$OUTPUT: 多项式 Q 于 $\mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_{r-1}]$ 或未定义 1: $d \leftarrow \deg(F)$ 2: $D \leftarrow \deg(C, U_0, 0)$ 3: $P \leftarrow (-1)^D C(\boldsymbol{U}_0, \ldots, \boldsymbol{U}_{r-1}, \boldsymbol{U}'_r)$ $\in \mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r][T]$，其中 $\boldsymbol{U}'_r = U_{r,0} - T, U_{r,1}, \ldots, U_{r,n}$4: $a \leftarrow \operatorname{coeff}(P, T^D)$ $\in \mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r]$5: $M_P \leftarrow$ PSEUDO-COMPANION(P)6 $w_0 \leftarrow \frac{\partial P}{\partial T}$: : 对 , . . . , n 执行 7 $i = 1$ $w_i \leftarrow -\frac{\partial P}{\partial U_r}$,$_i$8: 对 $i = 0, \ldots, n$ 执行 $w_i^h \leftarrow$ HOMOGENIZE($w_i, T', (T)\ D$)▷ w_i 的齐次化，次数为 D，关于 T，使用新变量 T'9: 对 $i = 0, \ldots, n$ 执行 $M_i \leftarrow w_i^h(a\mathrm{Id}\ M_P)$ 10: $F_{\text{gen}} \leftarrow \sum\overline{\ }_{|\boldsymbol{\alpha}| \le d} V_\alpha X_0^{d-|\alpha|} X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, $\boldsymbol{V} = (V_{\boldsymbol{\alpha}})_{|\boldsymbol{\alpha}| \le d}$ 新不定元次数为 d 的一般齐次多项式 11: $G \leftarrow a^d \det(F_{\text{gen}}(M_0, \ldots, M_n))/\det(M_0)^d$.12: 返回 $G(\boldsymbol{U}_0, \ldots, \boldsymbol{U}_{r-1}$, 系数($F$))

引理 4.12. 设 V 要么为空，要么是 r-等维且处于正规位置，并定义在域 $\mathbb{K}$上。给定其归一化 *Chow* 形式 C_V和 F在 $\mathbb{K}[X_1, \ldots, X_n]$中，并假设 $\gcd(C_V, \partial C_V/\partial U_{0,0}) = 1$, DEGREE d CHOW FORM返回 $C_{\deg(F),\ V}[F]$，且第 11 步的除法是精确的。

证明。 证明见 [15, 第3节.2]；这里我们仅指出 $\gcd(C_V, \partial C_V/\partial U_{0,0}) = 1$ 这一假设在何处用到。

为使第 11 步的除法定义良好，我们必须保证 $\det(M_0)$ 不为零（随后即可由上述参考文献证明该除法是精确的）。这个行列式除去 $a = \operatorname{coeff}(P, T^D)$ 的某个幂后，就是 P和 $\frac{\partial P}{\partial T}$关于 T的结式。因此，只需验证 $\gcd(P, \partial P/\partial T) = 1$ 在 $\overline{\mathbb{K}}(\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r)[T]$中。

由于 C_V关于 $\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r$ 对称，因此 $\gcd(C_V, \partial C_V/\partial U_{r,0}) = 1$。于是，我们可以重复证明引理 4.8 中使用的论证，并证明 $\gcd(P, \partial P/\partial T) = 1$在 $\mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r, T]$ 中。这意味着这两个多项式在$\mathbb{K}(\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r)[T]$中也有常数最大公因式。 □

引理 4.13. 设 V 是 $\mathbb{C}^n$中的一个代数集，在 $\mathbb{Q}$上定义，且要么为空，要么是r等维并处于正规位置，其次数至多为 D_V、高度至多为 H_V；并设 F 具有整数系数，次数至多为 d_F、高度至多为 h_F。那么，存在一个非零整数$\Delta_{VF}^{\text{Chow}}$，使得

$$h(\Delta_{V,F}^{\text{Chow}}) \in O(n^6 D_V (D_V + H_V) + h_F)$$

使得若素数 p 不整除$\Delta_{VF}^{\text{Chow}}$，，则：

- C_V和 $Q = \text{DEGREE } d \text{ CHOW FORM}(C_V, F)$ 的系数属于 $\mathbb{Z}_{(p)}$,
- $\text{DEGREE_}d\text{_CHOW_FORM}(C_V$模 p, F模 $p) = Q$ 模 p,
- 最大公因式$(C_V$模 $p, \partial C_V/\partial U_{0,0}$模 $p) = 1$.

证明。与前面一样，我们将 C_V改写为 $C_V = C_V^{\text{primitive}}/c$，其中 c是 C_V的最小分母，并令 Δ_0 为 c 与 F中任意一个最高次数单项式的系数的乘积。由于 C_V的高度至多为 $H' = H_V + (r+1)\ln(n+2)D_V \in O(H_V + nD_V\ln(n))$，且 F至多为 h_F，因此 Δ_0 的高度为 $O(H_V + nD_V\ln(n) + h_F)$。

与引理 4.3 的证明一样，存在非零的 Δ_1，使得 $h(\Delta_1) \in O(n^6 D_V(D_V + H_V))$；若 p 不整除 $\Delta_0\Delta_1$，则还有最大公因式$(C_V$模 $p, \partial C_V/\partial U_0, 0$ 模 $p) = 1$。因此，设素数 p 不整除 $\Delta_0\Delta_1$，那么特别地， C_V 的系数属于 $\mathbb{Z}_{(p)}$。在前两个步骤中计算得到的整数 d 和 D 模 p后保持不变（对于前者，这是由 Δ_0的构造所致；对于后者，这是因为 C_V 的首项系数为 1）。这意味着截至第 10 步计算出的所有量的系数都属于 $\mathbb{Z}_{(p)}$，且它们的计算与模 p约化可交换。因此，$A = a^d \det(F_{\text{gen}}(M_0, \ldots, M_n))$ 和 $B = \det(M_0)^d$的系数属于 $\mathbb{Z}_{(p)}$；并且根据前一个引理，我们知道 B 非零且整除 A。

为了应用引理2.3，我们必须确保 $\det(M_0)$ 模 p不为零；但我们在前一个引理的证明中已经看到确实如此，因为 $\gcd(C_V$模 $p, \partial C_V/\partial U_{0,0}$模 $p) = 1$。于是，引理2.3 保证在步骤 G处计算得到的11 的系数属于 $\mathbb{Z}_{(p)}$，并且除法与模 p约化可交换。最后，在 F 的系数处进行特化不会造成任何困难。

总之，我们令 $\Delta_{V,f}^{\text{Chow}} = \Delta_0\Delta_1$，其高度为 $O(n^6 D_V(D_V + H_V) + h_F)$，引理得证。 □

4.6 正常交

最后，取 V r-等维且处于正规位置，并取 F于 $\mathbb{K}[X_1, \ldots, X_n]$，现在假设 $W = V \cap V(F)$ 的维数为 $r-1$（或为空）。这里我们回顾一个来自 [15], 本身的另一过程，该过程使用 Philippon 的一个结果 [24], ，为 W给出一个乔形式。我们先给出两个定义。

定义4.14。假设 Q 是 $\mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_{r-1}]$ 中的一个非零多项式，并考虑它的绝对分解，即在 $\mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_{r-1}]$ 中将其分解为首一不可约因子。将依赖于 $U_{0,\,0}$ 的不可约因子与不依赖于它的因子分开，得到如下表达式

$$Q = \text{lc}(Q) \prod_{i \in I_1} C_i^{m_i} \prod_{i \in I_2} C_i^{m_i}, \tag{6}$$

重数为正数 m_i，若 C_i 不依赖于 U_0，则为 $i \in I_1$，$_0$；若依赖，则为 $i \in I_2$。Q 的弱无平方因子部分 $S(Q)$ 是乘积 $C = \prod_{i \in I_2} C_i$。

这是一个首一多项式，先验地 其系数属于 $\mathbb{K}$。若 $\mathbb{K}$是完美域，则在 $\mathbb{K}$ 上进行因式分解即可：从关于（6）的不可约因式分解出发，但在 $\mathbb{K}$上进行分解，也能得到 $S(Q)$。

定义 4.15. 设 Q 是 $\mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_{r-1}]$中的非零多项式。我们称$Q$ 是驯顺的，如果 $C = S(Q)$ 满足 最大公因式 $(C, \partial C/\partial U_{0,0}) = 1$，并且 (6) 中的重数全都是 $\mathbb{K}$ 中的单位。

如果 $\mathbb{K}$ 是完美的，那么将 Q 在 $\mathbb{K}$ 上因式分解得到的重数，与在 $\mathbb{K}$上因式分解得到的重数相同。如果 $\mathbb{K}$的特征为零，那么任何非零 Q 都是驯顺的。

引理 4.16. 设 Q 是驯顺的。那么 $S(Q) = Q/(\mathrm{lc}(Q)$最大公因式$(Q, \partial Q/\partial U_{0,0}))$。

证明。 写作 $C = S(Q)$。从 $C = \prod_{i \in I_2} C_i$出发，我们的第一个假设意味着，对于 I_2中的所有 i，最大公因式$(C_i, \partial C_i/\partial U_{0,0}) = 1$。对定义 Q 的方程求导，得到

$$\frac{\partial Q}{\partial U_{0,0}} = \mathrm{lc}(Q) \left(\prod_{i \in I_1} C_i^{m_i} \right) \sum_{i \in I_2} m_i \frac{\partial C_i}{\partial U_{0,0}} C_i^{m_i - 1} \prod_{i' \in I_2 - \{i\}} C_{i'}^{m_{i'}}.$$

由于所有 m_i 在 $\mathbb{K}$ 中都非零，因此可得 $\gcd(Q, \partial Q/\partial U_{0,0}) = \prod_{i \in I_1} C_i^{m_i} \prod_{i \in I_2} C_i^{m_i - 1}$（两边均为首一），最后得到

$$\frac{Q}{\gcd(Q, \partial Q/\partial U_{0,0})} = \mathrm{lc}(Q) C \qquad \square$$

这个定义的要点来自 [24, 命题 2.4] 和 [15, 引理 3.7]：如果V在正规位置上是 r-等维的，并且 F在 $\mathbb{K}[X_1, \ldots, X_n]$中，而 $W = V \cap V(F)$ 的维数为 $r - 1$（或为空），那么 $C = S(C_{\deg(F),\, V}[F])$ 是 W 的乔形式；特别地，如果 W 处于正规位置，则 $C = C_W$，因为 C 是首一的。

这引出了以下过程。给定任意输入，如果 Degree d Chow form 未定义或 Q 为零（这与上述假设矛盾），则它可能返回未定义，因为此时第 3 步中的首一最大公因式未定义。下面的引理总结了保证输出有效的条件。

Intersection_ChowInput: 多项式 C于 $\mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_r]$，其$\boldsymbol{U}_i = U_{i,0}, \ldots, U_{i,n}$对所有 iInput: 多项式 F于 $\mathbb{K}[X_1, \ldots, X_n]$Output: 多项式 D于 $\mathbb{K}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_{r-1}]$或未定义1: $Q \leftarrow$ Degree d Chow form(C, F)
2: $R \leftarrow$ 最大公因式$(Q, \partial Q/\partial U_{0,0})$3: $S \leftarrow Q/R$4: **return** $S/\mathrm{lc}(Q)$

引理 4.17。 设 V 是在域 $\mathbb{K}$ 上定义的代数集，且 F 属于 $\mathbb{K}[X_1, \ldots, X_n]$。假设满足以下条件：

- V 要么为空，要么是 r-等维的并处于正规位置
- $W = V \cap V\ (F)$ 要么为空，要么是（$r-1$）等维的
- 最大公因式$(C_V,\ \partial C_V/\partial U_{0,\ 0}) = 1$
- Degree d Chow form (C_V, F) 是驯顺的。

那么，给定 C_V 和 V 的归一化乔形式以及 F， Intersection Chow 返回 W的一个乔形式。如果 W处于正规位置，输出就是其归一化乔形式 C_W。

证明。 利用引理 4.12，第一个和第三个假设推出在步骤 1， $Q = C_{\deg(F),\ V}[F]$。关于 W的假设表明，$S(C_{\deg(F)\ V}[F])$ 是 W的一个乔形式，而最后一个假设允许我们应用前一个引理来计算它。

□

引理 4.18。 设 V是定义在 $\mathbb{Q}$上的代数集，且 F属于 $\mathbb{Z}[X_1, \ldots, X_n]$。假设满足以下条件：

- V 要么为空，要么是 r等维且处于正规位置，
- $W = V \cap V(F)$ 要么为空，要么是$(r-1)$等维且处于正规位置。

假设 V 的次数至多为 D_V，高度至多为 H_V，且 F 的次数至多为 d_F，高度至多为 h_F。那么，存在一个非零整数$\Delta_{VF}^{\text{interesection}}$,使得

$$h(\Delta_{V,F}^{\text{intersection}}) \in O(n^6 d_F^2 D_V H_V + n^6 d_F h_F D_V^2 + n^7 d_F^2 D_V^2 \ln(n))$$

满足：若素数 p p 不整除$\Delta_{VF}^{\text{intersection}}$,，则：

- C_V和 Intersection Chow(C_V, F) 的系数属于 $\mathbb{Z}_{(p)}$
- Intersection_Chow$(C_V$模 p, F模 $p)$ = Intersection Chow(C_V, F) 模 p
- 最大公因式$(C_V$模 $p,\ \partial C_V/\partial U_{0,\ 0}$模 $p) = 1$
- Degree_d_Chow_form$(C_V$模 p， F模 $p)$ 是驯顺的。

证明。 首先，注意到由于 V 定义在 $\mathbb{Q}$上，前一个引理中的第三和第四个假设自动成立（前者由引理 4.1 得出，后者由引理 4.16之前的评注得出，因为$C_{\deg(F),\ V}[F]$非零），因此该引理证明了C_W = Intersection Chow$(C_V,\ F)$。

我们对 p 的第一个约束是，它不整除整数$\Delta_{VF}^{\text{Chow}}$, 即引理4.13中的那个整数。当满足该条件时，我们得到在第1步计算出的 C_V与 Q = Degree d Chow form$(C_V,\ F)$的系数属于 $\mathbb{Z}_{(p)}$， Q 模 p = Degree d Chow form（C_V模 p, F模 p），并且最大公因式$(C_V$模 $p,\ \partial C_V/\partial U_{0,\ 0}$模 $p) = 1$。特别地，这确立了该引理的第三项。

我们进一步假设 p 不整除分子 Δ_1，亦即 Q的首项系数的分子。由此，Q模 p 的首项系数是 Q的首项系数模 p约化所得。然后我们可以考虑 Q 的绝对分解，如（6）：

$$Q = \mathrm{lc}(Q) \prod_{i \in I_1} C_i^{m_i} \prod_{i \in I_2} C_i^{m_i}.$$

由于 $\mathbb{Q}$ 是完美的，Q 也可在 $\mathbb{Q}$ 上分解为

$$Q = A \prod_{j \in J} B_j^{\mu_j},$$

其中 A和 $\mathbb{Q}[\boldsymbol{U}_0, \ldots, \boldsymbol{U}_{r-1}]$中的所有 B_j均为 $A =$，$\mathrm{lc}(Q)$ $\prod_{i \in I_1} C_i^{m_i}$在$U_0$中的次数为 0，所有 B_j在U_0中均为首一且次数为正，$\prod_{j \in J} B_j = \prod_{i \in I_2} C_i$ 和 $\{\mu_j\}_{j \in J} = \{m_i\}_{i \in I_2}$。

记 $Q = cQ'/e$，其中 Q' 是本原的（因此具有整数系数），且 c，e 是互素整数。对于 J中的 j，我们还可以将 Q 改写为 $Q = R_j B_j$，其中 R_j 的系数属于 $\mathbb{Q}$，因此 $cQ'/e = r_j R_j'/s_j$ B_j'/t_j，其中 R_j'，B_j' 是本原的，且 r_j，s_j 互素（B_j 是首一的，因此 $t_j B_j$ 是本原的）。由此得到 $cs_j t_j Q' = e r_j R_j' B_j'$，进而通过取内容得到 $cs_j t_j = e r_j$。另一方面，由于 B_j 是首一的，B_j' 的首项系数为 t_j，因此 $cs_j t_j \mathrm{lc}(Q') = e r_j \mathrm{lc}(R_j') t_j$，且 $\mathrm{lc}(Q') = \mathrm{lc}(R_j') t_j$。我们对 p 的选择确保 $\mathrm{lc}(Q')$ 模 p 非零，因此 B_j 的系数属于 $\mathbb{Z}_{(p)}$。

另一方面，由于 $Q = C_{\deg(F),\ V}[F]$（引理 4.12），我们知道 $C_W = \prod_{i \in I_2} C_i$，也就是说，$C_W = \prod_{j \in J} B_j$。由此可知，$C_W$ 的系数属于 $\mathbb{Z}_{(p)}$，因此引理的第一项得证。此外，由引理 2.3 可知，对于 A也同样成立。用小写 a 和 b_j 表示多项式 A 和 B_j 模 p后的约化，我们得到Q 模 $p = a \prod_{j \in J} b_j^{\mu_j}$，其中 a 与 $U_{0,\ 0}$无关。由于 C_W 是规范化的，所有 C_i'均成立（引理 3.6），这意味着所有 B_j'的首项（按照我们的分次序）在 $U_{0,\ 0}$中的次数均为正。由于 B_j'是首一的，b_j'也都是首一的，并且在 $U_{0,\ 0}$中的次数为正。

接下来，我们给出确保第四项成立的条件，即 Degree d Chow form(C_V模p，F模 p) 是驯顺的。假设 p 不整除 $\Delta_{V,\ F}^{\mathrm{Chow}}$ Δ_1，我们已经看到，这等价于 Q模 p 是驯顺的。

- 我们令 Δ_2 为所有整除其中一个整数 $\{m_i\}_{i \in I_2} = \{\mu_j\}_{j \in J}$ 的素数之积
- 我们令 Δ_3 为一个非零整数，使得如果 p 不整除 Δ_3，那么 $\gcd(C_W$模p，$\partial C_W/\partial U_{0,\ 0}$模 $p) = 1$。在这种情况下，由于 $\prod_{j \in J} b_j = C_W$模 p，所有 b_j 两两互素，且所有 b_j 都是绝对无平方因子的。

由此可知，当 p 不整除 $\Delta_{V,\ F}^{\mathrm{intersection}} = \Delta_{V,\ F}^{\mathrm{Chow}}$ $\Delta_1 \Delta_2 \Delta_3$ 时，C_W 模 p 是 Q模 p 的弱无平方因子部分，而对应因子在 Q模 p 中的重数均非零模 p，因此 Q模 p 是驯顺的。这给出了引理中的第四个性质。

最后，在关于 p 的相同假设下，我们证明引理中的第二点，即 Intersection Chow(C_V模 p，F模 p) $=$ C_W模 p。由于我们已经证明Q 模 $p =$ Degree d Chow form(C_V模 p，F模 p)，且该多项式是驯顺的，

我们知道（利用引理 4.16），INTERSECTION CHOW(C_V 模 p，F 模 p) 给出 Q 模 p 的弱无平方因子部分，而我们已经知道它是 C_W 模 p。

此时，尚需给出 $\Delta_{VF}^{\text{intersection}}$ 的高度上界。引理 4.13 给出了 $O(n^6 D_V(D_V + H_V) + h_F)$ 的高度上界 $\Delta_{VF}^{\text{Chow}}$。$\Delta_1$ 的高度小于或等于 $h(Q) = C_{\deg(F),\, V}[F]$ 而根据引理 3.15，我们知道后者属于 $O(d_F H_V + h_F D_V + n d_F D_V \ln(n))$。

对于 Δ_2 和 Δ_3，我们将使用 W 的次数和高度上界：利用贝祖´定理及其算术版本 [16, 推论 2。10], 它们分别至多为 $D_W = d_F D_V$ 和 $H_W = d_F H_V + h_F D_V + n d_F D_V \ln(n+1)$。第二个量 Δ_3 最容易处理：引理 2.6 表明，我们可以取高度为 Δ_3 的 $O(n^6 D_W(D_W + H_W))$，其为 $O(n^6 d_F D_V(d_F H_V + h_F D_V + n d_F D_V \ln(n))$。

对于 Δ_2，由于 Q 在 U_0 中的次数至多为 D_W，0，由此可知 $h(\Delta_2)$ 的上界为 $\sum_{p \text{ 素数 } \le D_W} \ln(p)$。该和是狄利克雷 θ 函数 $\vartheta(D_W)$ [1, p。 22], 它满足 $\vartheta(D_W) \in O(D_W) = O(d_F D_V)$ [1, 引理 8.2.2]。 □

5 算法

5.1 几何视角

在本节中，我们描述一个（相当直接的）过程，用以计算集合 $V(F_1, \ldots, F_s)$ 的等维分量，其中多项式 F_i 的系数属于域 $\mathbb{K}$；首先用纯几何语言，然后借助它们的乔形式。

给定 $\mathbb{K}[X_1, \ldots, X_n]$ 中的 $F_1, \ldots, F_s$，我们记 $V_i = V(F_1, \ldots, F_i)$，其中 $V_0 = \mathbb{K}^n$。对于 $i = 0, \ldots, s$，我们将 V_i 的等维分解写为

$$V_i = \bigcup_{0 \le k \le n} V_{i,k},$$

对于所有 k，它都是 $V_{i,k}$ k-等维的或为空。在这种记法中，以及下文的整个论述中，我们保留所有指标 $i, k, \ldots$ 的显式形式，以便于讨论这一过程中每一步的模素数 p 约化。

对于 $i = 0, \ldots, s-1$，我们有

$$V_{i+1} = \bigcup_{0 \le k \le n} (V_{i,k} \cap V(F_{i+1}))\,.$$

对于上述的 i 和 $k = 0, \ldots, n$，我们可以写成

$$V_{i,k} = V_{i,k,\text{zero}} \cup V_{i,k,\text{proper}}, \quad \text{with} \quad V_{i,k,\text{zero}}, V_{i,k,\text{proper}} = \text{SEPARATE}(V_{i,k}, V(F_{i+1})).$$

因此，V_{i+1} 可以写成所有 $V_{i、k、\text{zero}}$（它们均为 k-等维或为空）以及所有 $V_{i、k、\text{proper}} \cap V(F_{i+1})$（它们均为 $(k-1)$-等维或为空）的并。也就是说，

$$V_{i+1} = \bigcup_{0 \le k \le n} W_{i,k}, \quad \text{with} \quad W_{i,k} = V_{i,k,\text{zero}} \cup (V_{i,k+1,\text{proper}} \cap V(F_{i+1}));$$

这里，对于 $k = n$，我们设 $V_{i,\,n+1,\,\text{proper}} = \emptyset$。每个 $W_{i,\,k}$ 均为 k-等维或为空，但族 $(W_{i,\,k})_{0\le k\le n}$ 可能不是 V_{i+1} 的等维分解，因为给定的某个 $W_{i,\,k}$ 的一些不可约分支可能是某些 $W_{i,\,k'}$, $k' > k$ 的子集。

我们再次使用 SEPARATE 运算来纠正这一点。对于 $k = 0, \dots, n$ 和 $\ell = k+1, \dots, n+1$，令 $Z_{i,k,\ell}$ 为 $W_{i,k}$ 中所有不包含于 $W_{i,\ell}, \dots, W_{i,n}$ 之并集的不可约分支的并集。特别地，我们有 $Z_{i,k,n+1} = W_{i,k}$，并且 $V_{i+1,k} = Z_{i,k,k+1}$。此外，根据定义可知，对于 $\ell = k+1, \dots, n$，我们有如下递推关系

$$Z_{i,k,\ell} = Z_{i,k,\ell+1,\text{proper}},$$

with

$$Z_{i,k,\ell+1,\text{zero}}, Z_{i,k,\ell+1,\text{proper}} = \text{SEPARATE}(Z_{i,k,\ell+1}, W_{i,\ell}).$$

由此得到我们的算法的第一个版本。

DECOMPOSITION_GEOMETRIC
INPUT: $F_1, \dots, F_s$
OUTPUT: 等维分支 $V_{s,0}, \dots, V_{s,n}$，属于 $V(F_1, \dots, F_s)$

令 $V_{0,0} = \cdots = V_{0,n-1} = \emptyset$ 和 $V_{0,n} = \mathbb{K}^n$
对于 $i = 0, \dots, s-1$ **做**
  $V_{i,n+1,\text{适当}} \leftarrow \emptyset$
  对于 $k = n, \dots, 0$ **do**
    $V_{i,k,\text{zero}}, V_{i,k,\text{proper}} \leftarrow \text{SEPARATE}(V_{i,k}, V(F_{i+1}))$
    $J_{i,k} \leftarrow V_{i,k+1,\text{proper}} \cap V(F_{i+1})$
    $W_{i,k} \leftarrow V_{i,k,\text{零}} \cup J_{i,k}$
    $Z_{i,\,k,\,n+1} \leftarrow W_{i,k}$
    对于 $\ell = n, \dots, k+1$ **执行**
      $Z_{i,\,k,\,\ell} \leftarrow \text{SEPARATE}(Z_{i,\,k,\,\ell+1},\ W_{i,\,\ell})$
    $V_{i+1,\,k} \leftarrow Z_{i,\,k,\,k+1}$
返回 $V_{s,\,0}, \dots, V_{s,\,n}$

为了将其转化为实际的算法，我们将使用上一节中介绍的乔形式上的运算。其中大多数运算都要求处于正规位置；以下性质将确保满足我们所需的所有条件。

定义 5.1。如果以下条件成立，我们称 $F_1, \dots, F_s$ 处于一般位置：对于 $i = 0, \dots, s-1$ 和 $k = 0, \dots, n$，$W_{i,\,k}$ 要么为空，要么处于正规位置。

这一性质在一般坐标下成立：稍后我们将回到这一讨论，并对变量的不良变换进行量化。

引理 5.2. 对于任意输入 $F_1, \dots, F_s$，

1. $V_{0,0}, \dots, V_{0,n}$ 均为空或处于正规位置。

此外，如果 $F_1, \dots, F_s$ 处于一般位置，则以下结论成立：

2. 对于 $i = 0, \ldots, s-1$, $k = 0, \ldots, n$ 和 $\ell = k+1, \ldots, n+1$，所有集合 $V_{i,k,\text{zero}}$, $V_{i,k,\text{proper}}$, $J_{i,k}$, $W_{i,k}$, $Z_{i,k,\ell}$ （因此 $V_{i+1,k}$）均为空或为 k-等维且处于正规位置。

证明。 第一项显然。对于第二个断言，所有关于维数的陈述都由定义成立。由一般位置假设可知，$W_{i,k}$ 处于正规位置。于是，所有集合$V_{i,k,\text{zero}}$, $J_{i,k}$ 和 $Z_{i,k,\ell}$ 都由$W_{i,k}$ 的不可约分支构成，因此它们处于正规位置（或为空集）。类似地，如果 $i > 0$，集合 $V_{i,k}$ 由 $W_{i-1,k}$ 的不可约分支构成，因此它为空或处于正规位置；根据第一项，若 $i = 0$，同样的结论也成立；无论哪种情况，$V_{i,k,\text{proper}}$也同样如此。 □

接下来，我们可以利用迄今为止介绍的乔形式运算，给出这个算法一个更具体的版本。由于它所使用的子程序可能返回未定义，因此整个过程也可能如此。

DECOMPOSITION_CHOWINPUT: $F_1, \ldots, F_s$OUTPUT: **多项式** C_s**,0, . . . ,**C_s**,**n
或未定义 1: 对于 $i = 1, \ldots, n-1$ **执行** C_0**,**$i \leftarrow$ 1**2:** C_0**,**$n \leftarrow$ **det(**$\boldsymbol{U}_0, \ldots, \boldsymbol{U}_n$**),**
其中 $\boldsymbol{U}_i = U_i$**,0, . . . ,**U_i**对所有** i**均成立 3: 对于** $i = 0, \ldots, s-1$ **执行 4:** C_i**,**
$_{n+1,\text{proper}} \leftarrow$ 1**5: 对于** $k = n, \ldots, 0$ **执行 6:** C_i**,**k**,**zero**,**C_i**,**k**,**
$_{\text{proper}} \leftarrow$ SEPARATE HYPERSURFACE CHOW**(**C_i**,**k**,** F_{i+1}**) 7:** D_i**,**
$_k \leftarrow$ INTERSECTION CHOW**(**C_i**,**$k+1$**,**proper**,** F_{i+1}**) 8:** R_i**,**$k \leftarrow$ UNION CHOW**(**C_i**,**k**,**
$_{\text{zero}}$**,**D_i**,**k**) 9:** S_i**,**k**,**$n+1 \leftarrow R_i$**,**k**10: 对于** $\ell = n, \ldots, k+1$ **执行 11:** S_i**,**k**,**
$_\ell \leftarrow$ SEPARATE CHOW**(**S_i**,**k**,**$\ell+1$**,** R_i**,**ℓ**) 12:** C_{i+1}**,**$k \leftarrow S_i$**,**k**,**$k+1$**13: 返回** C

$_{s,0}, \ldots, C_{s,n}$

下面的命题是一个常规结果：我们证明，当输入处于一般位置时，前述过程能够正确计算由算法几何版本所定义的代数集的乔形式。我们假设 $\mathbb{K}$ 具有零特征，因为这能确保满足一些假设（例如温和性），而这些假设是保证我们使用的子程序返回预期输出所必需的。

命题 5.3. 对于任意输入 $F_1, \ldots, F_s$,

1. $C_{0,0}, \ldots, C_{0,n}$ 是 $V_{0,0}, \ldots, V_{0,n}$的归一化 *Chow* 形式。

此外，若 $F_1, \ldots, F_s$ 处于一般位置且 $\mathbb{K}$ 具有零特征，则算法不会返回未定义，并且

2. for $i = 0, \ldots, s-1$, $k = 0, \ldots, n$ *and* $\ell = k+1, \ldots, n+1$,

(a) $C_{i,n+1,\text{proper}}$ 是.....的归一化 *Chow* 形式$V_{i,n+1,\text{proper}}$

(b) $C_{i,k,\mathrm{zero}}$ 是$V_{i,k,\mathrm{zero}}$的归一化 *Chow* 形式*(c)* $C_{i,k,\mathrm{proper}}$ 是$V_{i,k,\mathrm{proper}}$的归一化 *Chow* 形式*(d)* $D_{i,k}$ 是$J_{i,k}$的归一化 *Chow* 形式*(e)* $R_{i,k}$ 是$W_{i,k}$的归一化 *Chow* 形式*(f)* $S_{i,k,\ell}$ 是$Z_{i,k,\ell}$的归一化 *Chow* 形式*(g)* $C_{i+1,k}$ 是$V_{i+1,k}$的归一化 *Chow* 形式

证明。 我们通过对 i 进行归纳法证明：对于 $i=-1,\ldots\ldots,\ s-1$，断言 2g 成立，即 $C_{i+1,\,k}$是良定义的，并且是 $V_{i+1,\,k}$的归一化 Chow 形式，对所有 $k=0,\ldots\ldots,\ n$成立。我们在归纳法中建立所有其他性质。

对于 $i=-1$，我们必须证明 $C_{0,\,0},\ldots\ldots,\ C_{0,\,n}$是$V_{0,\,0},\ldots\ldots,\ V_{0,\,n}$的归一化 Chow 形式；无论是否采用一般位置假设，这一点经直接检验都是显然的，并证明了断言 1。然后，对某些 $i=0,\ldots\ldots,\ s-1$，我们假设 $C_{i,\,k}$ 是 $V_{i,\,k}$ 的归一化 Chow 形式，对所有 $k=0,\ldots\ldots,\ n$成立，并证明对所有 k，该结论对 $C_{i+1,\,k}$同样仍然成立。

- $V_{i,\,n+1,\,\text{真}}$ 为空，因此我们令 $C_{i,\,n+1,\,\text{真}}=1$，由此得到 2a。
- 对于 $k=0$、……、 n，由于$V_{i,\,k}$要么为空，要么处于正规位置（引理5.2），并结合我们对 $i-1$ 的归纳假设以及我们处于零特征这一事实，引理4.1 和4.8 给出了断言2b 和2c。
- 对于 $k=0$、……、 n, $V_{i,\,k+1,\,\text{真}}$要么为空，要么是 $(k+1)$-等维且处于正规位置（若 $k=n$，则根据定义；否则根据引理5.2 ），$C_{i,\,k+1,\,\text{真}}$是其归一化乔形式（若 $k=n$，则为断言2a ；否则为2c ），而 $J_{i,\,k}$ 要么为空，要么是 k-等维且处于正规位置（引理 5.2）。利用零特征这一假设，可以验证引理4.17 中的最后两个假设（前者由引理4.1得出，后者由第4.6小节中温和性的定义得出）。于是，引理4.17 给出断言2d，即 $D_{i,\,k}$ 是 $J_{i,\,k}$的归一化乔形式。
- 对于 $k=0,\ldots,n$，$V_{i,k,\text{零}}$ 与 $J_{i,k}$ 二者要么为空，要么为 k-等维且处于正规位置（引理 5.2 ）。利用条目 2b 和 2d，以及零特征假设（用于引理 4.1，并且因为特征二被明确排除），引理 4.2 给出断言 2e，即 $R_{i,k}$ 是 $W_{i,k}$的归一化 Chow 形式。
- 对于 $k=0,\ldots,n$，我们通过对 $\ell=n+1,\ldots,k+1$ 作递减归纳，证明 2f ($S_{i,k,\ell}$ 是 $Z_{i,k,\ell}$) 的归一化 Chow 形式。对于 $\ell=n+1$，由 2e 我们已知 $S_{i,k,n+1}=R_{i,k}$ 是 $W_{i,k}=Z_{i,k,n+1}$ 的归一化 Chow 形式。假设对于某个 $\ell\in\{k+1,\ldots,n\}$，我们知道 $S_{i,k,\ell+1}$ 是 $Z_{i,k,n+1}$ 的归一化 Chow 形式。我们还知道 $R_{i,\ell}$ 是 $W_{i,\ell}$ 的归一化 Chow 形式（再次由 2e 得出），因此，由于处于零特征下，引理 4.10 表明 $S_{i,k,\ell}$ 是 $Z_{i,k,\ell}$ 的归一化 Chow 形式。这就证明了 2f 对 ℓ 的所有取值都成立。取 $\ell=k+1$，即可得到 2g。 □

5.2 模素数 p约化

多项式 F_1、 . . . 、 F_s 如上所述，现在我们取 $\mathbb{K} = \mathbb{Q}$，并令各个 F_i 的系数为整数；在本节中，我们仍假设这些多项式处于一般位置。

固定一个素数 p，令 $f_1, \ldots, f_s = F_1, \ldots, F_s$ 模 p。假设我们在输入 $f_1, \ldots, f_s$ 上运行过程 Decompo-sition Geometric：我们用小写字母表示它计算出的代数集（在 $\mathbb{F}_p^n$ 中），例如 $v_{i,k}$, $w_{i,k}$, $z_{i,k,\ell}$ 等。由于 Decomposition Geometric 对其输入不作任何假设，我们知道 $v_{s,0}, \ldots, v_{s,n}$ 是 $V(f_1, \ldots, f_s)$ 的等维分支。

另一方面，我们不假设 $f_1, \ldots, f_s$ 处于一般位置，因此我们无法先验地断言 Decomposition Chow 在输入 $f_1, \ldots, f_s$ 上会返回什么（输出可能未定义）。与处理 Decomposition Geometric 时一样，我们将用小写字母表示由 Decomposition Chow 在输入 $f_1, \ldots, f_s$ 上计算出的、系数属于 $\mathbb{F}_p$ 的多项式，例如 $c_{i,k}$, $d_{i,k}$ 等，前提是它们有定义。

下面的命题表明，除有限多个素数外，模 p 约化 $V(F_1, \ldots, F_s)$ 的等维分支的乔形式，得到的就是 $V(f_1, \ldots, f_s)$ 的等维分支的乔形式。

命题 5.4. 假设 $F_1, \ldots, F_s$ 处于一般位置。对于 $i = 0, \ldots, s-1$，整数

$$\Delta_i = \prod_{k=0}^{n} \left(\Delta^{\text{separate\_H}}_{V_{i,k},F_{i+1}} \Delta^{\text{intersection}}_{V_{i,k+1,\text{proper}},F_{i+1}} \Delta^{\text{union}}_{V_{i,k,\text{zero}},J_{i,k}} \prod_{\ell=k+1}^{n} \Delta^{\text{separate}}_{Z_{i,k,\ell+1},W_{i,\ell}} \right)$$

以及

$$\Delta = 2 \prod_{i=0}^{s-1} \Delta_i$$

是定义良好且非零的。若 p 不整除 Δ，则 $C_{s,0}, \ldots, C_{s,n}$ 的系数属于 $\mathbb{Z}_{(p)}$，$c_{s,0}, \ldots, c_{s,n}$ 是定义良好的，且是它们模 p 的约化，$v_{s,0}, \ldots, v_{s,n}$ 全部为空或处于正规位置，而 $c_{s,0}, \ldots, c_{s,n}$ 是它们的归一化乔形式。

本节余下部分将证明此命题。我们首先证明整数 Δ_i 定义良好且非零。对于 $i = 0, \ldots, s-1$，有如下结论：

- 对于 $k = 0, \ldots, n$, $V_{i,k}$ 根据引理 5.2，要么为空，要么是等维且处于正规位置，因此因子 $\Delta_{\text{分离 H}\, V_{i,k},F_{i+1}}$ 根据引理 4.9定义良好且非零。
- 对于 $k = 0, \ldots, n$, $V_{i,k+1,\text{proper}}$ 根据引理 5.2 再次要么为空，要么是等维且处于正规位置。此外，交 $V_{i,k+1,\text{proper}}$ 和 $V(F_{i+1})$ 是 proper，因此$\Delta_{\text{交}V_{i,k+1,\text{proper}}\, F_{i+1}}$ 根据引理 4.18定义良好且非零。
- 对于 $k = 0, \ldots, n$, $V_{i,k,\text{零}}$ 和 $J_{i,k}$ 根据引理 5.2，要么为空，要么是 k-等维且处于正规位置，因此根据引理4.3，$\Delta_{\text{并}V_{i,k,\text{零}}\, J_{i,k}}$ 定义良好且非零。
- 对于 $k = 0, \ldots, n$ 和 $\ell = k+1, \ldots, n$, $Z_{i,k,\ell+1}$ 以及 $W_{i,\ell}$，它们要么为空，要么是等维的且处于正规位置，这仍由引理 5.2 得出。由引理 4.11，$\Delta_{\text{分离}\, Z_{i,k,\ell+1},W_{i,\ell}}$ 是良定义且非零的。

由此可知，所有 Δ_i以及 Δ都是非零整数。接下来，在下文中我们将多次提及若干相关性质，为此引入以下记号。设 c是 $\mathbb{F}_p[\boldsymbol{U}_0,\dots,\boldsymbol{U}_r]$中的一个多项式，其中对于所有 i，都有$U_i = U_{i,0},\dots,U_{i,n}$；设 C属于 $\mathbb{Q}[\boldsymbol{U}_0,\dots,\boldsymbol{U}_r]$，且设 v是 $\mathbb{F}_p{}^n$中的一个代数集。如果 c, C, v具有性质 P，则称

P_1： C 的系数属于 $\mathbb{Z}_{(p)}$

P_2： $c = C$ 模 p

P_3： v 或者为空，或者是等维的 r，且处于正规位置

P_4： c 是 v 的归一化乔形式。

那么，对于 $i = 0,\dots,s$ 和 $k = 0,\dots,n$，我们要确立的关键性质如下：

A(i,k)：$c_{i,k}$ 有良好定义，并且 $(c_{i,k}, C_{i,k}, v_{i,k})$ 具有性质 P。

我们对 $i = 0,\dots,s$ 作递增归纳证明：在对 p 施加适当的整除性限制后，对于 k 的所有取值，A(i,k) 均成立。于是，取 $i = s$，我们对 p 的条件将归结为 Δ 模 $p \neq 0$，所得性质将证明该命题，因为 A(s,k) 表明，对于所有 k，$C_{s,k}$ 的系数都属于 $\mathbb{Z}_{(p)}$，$c_{s,k}$ 有定义，$c_{s,k} = C_{s,k}$ 模 p，$v_{s,k}$ 或为空或处于正规位置，而 $c_{s,k}$ 是其归一化 Chow 形式。

对于 $i = 0$，A$(0,k)$ 对 k 的所有取值均成立：P_1 和 P_2 显然成立，P_3 来自引理 1 中的第 5.2 项，而 P_4 是命题 5.3 中的第 1 项（两种情况下均应用于 $f_1,\dots,f_s$）。

现在假设，对于某个 i，其中 i 属于 $0,\dots,s-1$，我们已经证明了所有 A(i,k)，$k = 0,\dots,n$。以下假设 p 不整除 $2\Delta_i$，并证明对于 $k = 0,\dots,n$，所有 A$(i+1,k)$ 均成立。

1. 在第 4 步，$v_{i,\,n+1,\,\text{proper}}$ 为空，$c_{i,\,n+1,\,\text{proper}} = 1$（作为一个系数取自 $\mathbb{F}_p$ 的多项式），且 $C_{i,\,n+1,\,\text{proper}} = 1$（作为一个系数取自 $\mathbb{Q}$的多项式），因此三元组（$c_{i,\,n+1,\,\text{proper}}$，$C_{i,\,n+1,\,\text{proper}}$，$v_{i,\,n+1,\,\text{proper}}$）具有性质 P。

2. 取 k，使其属于 0，……，n。在 $\mathbb{F}_p$ 上，我们有

$$v_{i,k,\text{zero}}, v_{i,k,\text{proper}} = \textsc{Separate}(v_{i,k}, V(f_{i+1})) \tag{7}$$

$$c_{i,k,\text{zero}}, c_{i,k,\text{proper}} = \textsc{Separate\_Hypersurface\_Chow}(c_{i,k}, f_{i+1})$$

（除非该函数调用返回未定义），而且以下结论在 $\mathbb{Q}$上成立：

$$C_{i,k,\text{zero}}, C_{i,k,\text{proper}} = \textsc{Separate\_Hypersurface\_Chow}(C_{i,k}, F_{i+1}).$$

根据命题 5.3 可知 $C_{i,\,k} = C_{V_{i,\,k}}$，并且根据 A$(i,\ k)$ 的第一项和第二项，它在 $\mathbb{Z}_{(p)}$ 中的系数为 $c_{i,\,k} = C_{i,\,k}$ 模 p。然后，利用上述定义，并且由于 p 不整除 $\Delta^{\text{separate H}}_{V_{i\,k}\,F_{i+1}}{}_{,\,,}$，由引理 4.9 得到以下性质：

- $C_{i,k,\text{zero}}$ and $C_{i,k,\text{proper}}$ have coefficients in $\mathbb{Z}_{(p)}$.

- $c_{i,\ k,\ \text{零}}$ $c_{i,\ k,\ \text{适当的}}$ 均定义良好，且分别等于 $C_{i,\ k,\ \text{零}}$ 模 p，$C_{i,\ k,\ \text{适当的}}$ 模 p。
- 最大公因式$(c_{i,k}, \partial c_{i,j}/\partial U_{0,0}) = 1$。

另一方面，由于 $v_{i,k}$ 要么为空，要么处于正规位置，而 $c_{i,k}$ 是其归一化乔形式（两者也由 $\mathsf{A}(i,k$给出），并利用上面列出的第三项，引理 4.8 可知，$c_{i,k,\text{zero}}$ 和 $c_{i,k,\text{proper}}$ 分别是$v_{i,k,\text{zero}}$ 和$v_{i,k,\text{proper}}$的归一化乔形式。

这证明，对于所有 k 属于 $0, \ldots, n$，$(c_{i,k,\text{proper}}, C_{i,k,\text{proper}}, v_{i,k,\text{proper}})$ 和 $(c_{i,k,\text{zero}}, C_{i,k,\text{zero}}, v_{i,k,\text{zero}})$ 都具有性质 P。

3. 取 k 属于 $0, \ldots, n$。在 $\mathbb{F}_p$ 上，我们有

$$j_{i,k} = v_{i,k+1,\text{proper}} \cap V(f_{i+1})$$

$$d_{i,k} = \textsc{Intersection\_Chow}(c_{i,k+1,\text{proper}}, f_{i+1})$$

（除非 函数调用返回未定义），而在 $\mathbb{Q}$上，以下结论成立：

$$D_{i,k} = \textsc{Intersection\_Chow}(C_{i,k+1,\text{proper}}, F_{i+1}).$$

回想一下，$C_{i,k+1,\text{proper}}$ 和$D_{i,k}$ 是$V_{i,k+1,\text{proper}}$ 和$J_{i,k} = V_{i,k+1,\text{proper}} \cap V(F_{i+1})$的归一化乔形式（命题 5.3）。我们还知道，$C_{i,k+1,\text{proper}}$ 的系数属于 $\mathbb{Z}_{(p)}$，且$c_{i,k+1,\text{proper}} = C_{i,k+1,\text{proper}}$ 模 p （若 $k = n$，则为本证明中的第 1 项；否则为第 2 项）。接着，由于我们假设 p 不整除$\Delta^{\text{intersection}}_{V_i\ k+1}$，$_{,\text{proper},F_{i+1}}$，由引理 4.18 可得：

- $D_{i,\ k}$ 的系数属于 $\mathbb{Z}_{(p)}$。
- $d_{i,\ k}$ 是良定义的，且模 p等于$D_{i,\ k}$。
- $\gcd(c_{i,\ k+1,\ \text{真}}\ \partial c_{i,\ k+1,\ \text{真}}/\partial U_{0,\ 0}) = 1$。
- $\textsc{Degree_}d\textsc{_Chow_form}(c_{i,\ k+1,\ \text{真}}\ f_{i+1})$是驯顺的。

另一方面，我们知道 $v_{i,k+1,\text{proper}}$ 为空集或处于正规位置（若 $k = n$，则由第 1 项可知；否则由第 2 项可知），$v_{i,k+1,\text{proper}} \cap V(f_{i+1})$ 为空集或为 k-等维（若 $k = n$，则由第 1 项可知；否则由索引 $k+1$ 处的等式 (7) 可知），而且 $c_{i,k+1,\text{proper}}$ 是 $v_{i,k+1,\text{proper}}$ 的归一化乔形式（同样由第 1 项和第 2 项可知）。利用上面列出的第 3 项和第 4 项，引理4.17表明 $d_{i,k}$ 是 $j_{i,k}$ 的一个乔形式。

我们知道 $D_{i,k}$ 已规范化，因此其模 p 约化 $d_{i,k}$ 也已规范化。这意味着 $j_{i,k}$ 若非空集，则处于正规位置；而 $d_{i,k}$ 是其归一化乔形式。换言之，$(d_{i,k}, D_{i,k}, j_{i,k})$ 具有性质 P。

4. 取 k 属于 0、.....、n。在 $\mathbb{F}_p$ 上，我们有

$$w_{i,k} = v_{i,k,\text{zero}} \cup j_{i,k}$$

$$r_{i,k} = \textsc{Union\_Chow}(c_{i,k,\text{zero}}, d_{i,k})$$

（除非函数调用返回未定义），而在 $\mathbb{Q}$ 上，我们有

$$R_{i,k} = \textsc{Union\_Chow}(C_{i,k,\text{zero}}, D_{i,k}).$$

回忆一下，$C_{i,k,\text{zero}}$ 是$V_{i,k,\text{zero}}$ 的归一化乔形式，而$D_{i,k}$ 是$J_{i,k}$ 的规范化乔形式（命题 5.3）。我们还知道，$C_{i,k,\text{zero}}$ 的系数属于$\mathbb{Z}_{(p)}$，且$c_{i,k,\text{zero}} = C_{i,k,\text{zero}}$ 模 p （本证明中的第 2 项）；类似地，$D_{i,k,\text{zero}}$ 的系数属于 $\mathbb{Z}_{(p)}$，且$d_{i,k,\text{zero}} = D_{i,k,\text{zero}}$ 模 p （本证明中的第 3 项）。接着，由于我们假设 p 不整除$\Delta^{\text{union}}_{V_{i\,k}}$，$_{,\text{zero},J_{i,k}}$，根据引理 4.3 可得以下性质：

- $R_{i,\,k}$ 的系数属于 $\mathbb{Z}_{(p)}$。
- $r_{i,\,k}$ 定义良好，且模 p与$R_{i,\,k}$ 相等。
- 最大公因式$(c_{i,\,k,\,\text{零}}\ \partial c_{i,\,k,\,\text{零}}/\partial U_{0,\,0}) =$最大公因式$(d_{i,\,k,}\ \partial d_{i,\,k}/\partial U_{0,\,0}) = 1$。

另一方面，我们知道 $v_{i,\,k,\,\text{zero}}$ 为空或处于正规位置，并且 $c_{i,\,k,\,\text{zero}}$ 是其归一化 Chow 形式（第 2 项）；类似地，$j_{i,\,k}$ 为空或处于正规位置，并且 $d_{i,\,k}$ 是其归一化 Chow 形式（前一项）。这两个集合的维数均为 k （若非空）。这尤其表明 $w_{i,\,k}$ 为空或处于正规位置。由于 p 是奇数，结合上面列出的第三项， 引理 4.2表明 $r_{i,\,k}$ 是 $w_{i,\,k}$的归一化 Chow 形式。换言之，$(r_{i,\,k},\ R_{i,\,k},\ w_{i,\,k})$具有性质 P。

5. 再次取 k，其中取值于 $0, \ldots, n$。我们有 $s_{i,k,n+1} = r_{i,k}$, $S_{i,k,n+1} = R_{i,k}$ 以及 $z_{i,k,n+1} = w_{i,k}$。由于 $(r_{i,k}, R_{i,k}, w_{i,j})$具有性质 P，我们推知 $(s_{i,k,n+1}, S_{i,k,n+1}, z_{i,k,n+1})$也具有性质 P。接着，对于 $\ell = n, \ldots, k+1$，假设 $(s_{i,k,\ell+1}, S_{i,k,\ell+1}, z_{i,k,\ell+1})$具有性质 P，我们证明 $(s_{i,k,\ell}, S_{i,k,\ell}, z_{i,k,\ell})$也具有性质 P。

在 $\mathbb{F}_p$上，我们有

$$_{-}, z_{i,k,\ell} \leftarrow \textsc{Separate}(z_{i,k,\ell+1}, w_{i,\ell}),$$

and

$$_{-}, s_{i,k,\ell} \leftarrow \textsc{Separate\_Chow}(s_{i,k,\ell+1}, r_{i,\ell})$$

（除非函数调用返回未定义），而在 $\mathbb{Q}$上，以下结论成立：

$$_{-}, S_{i,k,\ell} \leftarrow \textsc{Separate\_Chow}(S_{i,k,\ell+1}, R_{i,\ell}).$$

回想一下，$S_{i、\,k、\,\ell+1}$ 以及$R_{i、\,\ell}$ 分别是$Z_{i、\,k、\,\ell+1}$ 以及$W_{i、\,\ell}$ 的归一化 Chow 形式（命题 5.3）。这两个多项式的系数都属于 $\mathbb{Z}_{(p)}$ （前者由归纳假设得出，后者由第 4项得出），它们模 p 的约化分别为$s_{i、\,k、\,\ell+1}$ 以及$r_{i、\,\ell}$ （理由相同）。然后，由于我们假设 p 不整除$\Delta^{\text{separate}}_{Z_{i\,k\,\ell+1}}$，$W_{i、\,\ell}$，根据引理 4.11，我们得到以下性质：

- $S_{i,\,k,\,\ell}$ 的系数属于 $\mathbb{Z}_{(p)}$。

- $s_{i,\ k,\ \ell}$ 定义良好，且模 p等于$S_{i,\ k,\ \ell}$。
- 最大公因式$(s_{i,\ k,\ \ell+1},\ \partial s_{i,\ k,\ \ell+1}/\partial U_{0,\ 0}) = 1$。

另一方面，我们知道 $z_{i,\ k,\ \ell+1}$ 和 $w_{i,\ \ell}$ 要么为空，要么处于正规位置；前者根据归纳假设，后者根据第4项。我们还知道 $s_{i,\ k,\ \ell+1}$ 和$r_{i,\ \ell}$ 是它们的归一化乔形式（理由相同）。利用上面列出的第三项，引理 4.10 表明，$z_{i,\ k,\ \ell}$ 要么为空，要么处于正规位置，且$s_{i,\ k,\ \ell}$ 是其归一化乔形式。

换句话说，$(s_{i,\ k,\ \ell},\ S_{i,\ k,\ \ell},\ z_{i,\ k,\ \ell})$具有性质 P。这就确立了我们的归纳性质；取 $\ell = k+1$，可知 $(c_{i+1,\ k},\ C_{i+1,\ k},\ v_{i+1,\ k})$具有性质 P。进而，这就确立了 A$(i+1,\ k)$，并完成了证明。

5.3 定量方面及主定理的证明

我们以主定理的证明结束本节。设给定 $F_1 \ldots,\ F_s$，它们的系数为整数，次数至多为 $d \geq 1$，高度至多为 $h \geq 1$。我们不假设它们处于一般位置。与之前一样，我们将通过对 F_1，...，F_s 应用算法 Decomposition Geometric 得到的代数集称为 $V_{i,\ k}$，$J_{i,\ k}$，$W_{i,\ k}$，...。

引理 *5.5.* 假设所有 F_i 的系数均为整数，次数至多为 $d \geq 1$，高度至多为 $h \geq 1$。那么，对于 $i = 0$，...，$s-1$ 和 $k = 0$，...，n，所有代数集 $V_{i、\ k、}$ $V_{i、\ k、\ \text{zero}、}$ $V_{i、\ k、\ \text{proper}、}$ $V_{i、\ n+1、\ \text{proper}、}$ $J_{i、\ k、}$ $W_{i、\ k}$ 以及 $V_{i+1、\ k} = Z_{i、\ k、\ k+1、\ \ldots、\ Z_{i、\ k、\ n+1}}$ 的次数至多为 D，高度至多为 H，其中 D 和 H 由下式给出

$$D = 2d^{n+1} \in O(d^{n+1})$$

and

$$H = 5hnd^{n+1}\ln(n+1) \in O(nhd^{n+1}\ln(n)).$$

证明。对于 $i = 0, \ldots, s$ 和 $k = 0, \ldots, n$，$V_{i,k}$ 的次数至多为 d^n，高度至多为 $d^n(nh + 2n\ln(n+1))$：次数上界来自 [14, 命题 2.3],，高度上界来自 [16, 推论 2.10]。若我们只考虑 $i = 0, \ldots, s-1$，则 $V_{i,k,\text{zero}}$ 和 $V_{i,k,\text{proper}}$ 也满足相同的界，因为它们的不可约分支是 $V_{i,k}$ 的不可约分支；$V_{i,n+1,\text{proper}} = \emptyset$ 也同样如此。由此可得，$J_{i,k} = V_{i,k+1,\text{proper}} \cap V(F_{i+1})$ 的次数至多为 d^{n+1}，其高度至多为 $d^n h + d^{n+1}(nh + 2n\ln(n+1)) + d^{n+1}\ln(n+1)$（参见相同文献）。最后，由可加性，$W_{i,k} = V_{i,k,\text{zero}} \cup J_{i,k}$ 的次数和高度分别至多为

$$D = 2d^{n+1} \in O(d^{n+1})$$

and

$$H = 5hnd^{n+1}\ln(n+1) \in O(nhd^{n+1}\ln(n)).$$

对于 $\ell = k+1, \ldots, n$，代数集 $Z_{i,k,\ell+1}$ 具有相同的次数和高度界，因为它们的不可约分支也是 $W_{i,k}$ 的不可约分支。 □

为了应用上一节的结果，我们需要一般位置多项式；这可以通过应用一次系数为整数且高度受控的变量替换来实现（关于零点定理恒等式的讨论，请参见 [16, 第 4] 节，其中包含启发本讨论的论证）。

对于可逆的 $n \times n$ 矩阵 $\boldsymbol{A}$ 以及 F 中的多项式 $\mathbb{Q}[X_1, \ldots, X_n]$，记作 $F^{\boldsymbol{A}} = F(\boldsymbol{AX})$，其中 $\boldsymbol{X}$ 是一个列向量，其条目为 X_1、……、X_n。如果 V 是一个代数集，则将 $V^{\boldsymbol{A}}$ 定义为所有多项式 $F^{\boldsymbol{A}}$（其中 F 属于 $I(V)$）的零点集；等价地，$V^{\boldsymbol{A}}$ 是在映射 $\boldsymbol{x} \mapsto \boldsymbol{A}^{-1}\boldsymbol{x}$ 下 V 的像。特别地，对 $F_1^{\boldsymbol{A}}$、……、$F_s^{\boldsymbol{A}}$ 应用算法 Decomposition Geometric 所得的代数集，恰好是 $V_{i\,k}^{\boldsymbol{A}}$、$J_{i\,,k}^{\boldsymbol{A}}$、$W_{i\,,k}^{\boldsymbol{A}}$，等等。

引理 5.6。 存在 $\boldsymbol{B} \in \mathbb{Z}^{n\times n}$，使得以下结论成立：

- $\boldsymbol{B}$ 的高度为 $O(n\ln(d))$。
- $\boldsymbol{B}$ 在 $\mathbb{Q}^{n\times n}$ 中可逆，其逆称为 $\boldsymbol{A}$。
- $F_1^{\boldsymbol{A}}$、……、$F_s^{\boldsymbol{A}}$ 处于一般位置。

证明。对于 $i = 0$、……、$s-1$ 以及 $k = 0$、……、n，$W_{i,\,k}$ 是 k-等维的（或为空），其次数至多为 $D = 2d^{n+1}$。由于零维集合总处于正规位置，我们可以假设 $k \geq 1$。

如果 $W_{i,\,k}$ 为空，则唯一的约束是 $\boldsymbol{B}$ 可逆（因为这样一来，当 $\boldsymbol{A} = \boldsymbol{B}^{-1}$、$W_{i\,,k}^{\boldsymbol{A}}$ 也为空）。在这种情况下，我们定义 $G_{i,\,k} = 1$。

否则，如果 $W_{i,\,k}$ 非空，则有理数域 [16]中的命题 4.5 证明了存在一个非零多项式 $G_{i,\,k}$ 属于 $\mathbb{Q}[\boldsymbol{U}_1, \ldots, \boldsymbol{U}_k]$（其中 $\boldsymbol{U}_i = U_{i,\,0}$、……、$U_{i,\,n}$ 对所有 i 均成立），其总次数至多为 $2nD^2$，并且如果 $G_{i,\,k}(b_{1,\,0}$、……、$b_{k,\,n}) \neq 0$，

$$W_{i,k} \cap V(b_{1,0} + b_{1,1}X_1 + \cdots + b_{1,n}X_n, \ldots, b_{k,0} + b_{k,1}X_1 + \cdots + b_{k,n}X_n)$$

的基数为 $\deg(W_{i,k})$。

然后我们选取整数 $b_{1,0}, \ldots, b_{n,n}$，使得对所有 $k = 1, \ldots, n$ 都有 $G_{i,k}(b_{1,0}, \ldots, b_{k,n}) \neq 0$，并且矩阵 $\boldsymbol{B} = [b_{k,j}]_{1\leq k,j\leq n}$ 可逆。若令 $\boldsymbol{A} = \boldsymbol{B}^{-1}$，则对所有 $j = 1, \ldots, n$，$V(b_{j,0} + b_{j,1}X_1 + \cdots + b_{j,n}X_n)^{\boldsymbol{A}} = V(X_j + b_{j,0})$。由此可得，对 $k = 1, \ldots, n$，

$$\begin{aligned} W_{i,k}^{\boldsymbol{A}} \cap V(b_{1,0} + b_{1,1}X_1 + \cdots + b_{1,n}X_n, \ldots, b_{k,0} + b_{k,1}X_1 + \cdots + b_{k,n}X_n)^{\boldsymbol{A}} \\ = W_{i,k}^{\boldsymbol{A}} \cap V(X_1 + b_{1,0}, \ldots, X_k + b_{k,0}). \end{aligned}$$

我们对 $b_{k,j}$ 的假设表明（若 $W_{i,k}$ 非空），该集合是有限的，次数为 $\deg(W_{i,k}) = \deg(W_{i\,,k}^{\boldsymbol{A}})$，因此由引理 3.7，$W_{i\,,k}^{\boldsymbol{A}}$ 处于正规位置。

接下来需要给出 $\boldsymbol{B}$ 高度的上界。$\boldsymbol{B}$ 上的约束表明，$b_{k,j}$ 不应使一个次数至多为 $2n^2D^2 + n \leq 3n^2D^2 \leq 12n^2d^{2n+2}$ 的非零多项式相消，因此根据 De Millo-Lipton-Schwartz-Zippel 引理，我们可以找到合适的 $b_{k,j}$，使其高度至多为 $\ln(12n^2d^{2n+2}) \in O(n\ln(d))$。

□

按前一个引理中的方式固定 $\boldsymbol{B}$ 和 $\boldsymbol{A}$，并令 δ 为 $\boldsymbol{B}$ 的行列式；这是一个高度为 $O(n^2\ln(d))$ 的非零整数，我们可以写作 $\boldsymbol{A}=\boldsymbol{A}'/\delta$，其中 $\boldsymbol{A}'$ 的各项也是高度为 $O(n^2\ln(d))$ 的整数。

定义 $G_1,\ldots,G_s$，使其满足 $G_i=\delta_i F_i^{\boldsymbol{A}}$，其中 δ_i 是 $F_i^{\boldsymbol{A}}$ 的最小分母（这是 δ 某个幂的因子）。由此可得，$G_1,\ldots,G_s$ 是 $\mathbb{Z}[X_1,\ldots,X_n]$ 中的一般位置多项式，其次数至多为 d，高度为 $O(h')$，且 $h'=h+n^2d\ln(d)$；后者可通过将 F_i 齐次化，在 $(\boldsymbol{A}'\boldsymbol{X})1,\ldots,(\boldsymbol{A}'\boldsymbol{X})_n$，$\delta$ 处求值，并应用引理 1.2.1]得出。

还要注意，对 $G_1,\ldots,G_s$ 应用算法 Decomposition Geome-tric 得到的代数集仍然是 $V_{i\,k}^{\boldsymbol{A}},,J_i^{\boldsymbol{A}},_k,W_i^{\boldsymbol{A}},_k,\ldots$ 由于所有 $V_{i,k},J_{i,k},W_{i,k},\ldots$ 的次数至多为 D，且高度至多为 H（定义见引理 5.5），而 $\boldsymbol{B}=\boldsymbol{A}^{-1}$ 的所有项的高度为 $O(n\ln(d))$，由文献 [16] 中的引理 2.6 可知，所有 $V_{i\,k}^{\boldsymbol{A}},,J_i^{\boldsymbol{A}},_k,W_i^{\boldsymbol{A}},_k,\ldots$ 的高度均为 $O(H')$，且 $H'=H+n^2D\ln(d)$。它们的次数仍有上界 D。

设 Δ 为将命题 5.4 应用于 G_1，……，G_s 所得的非零整数，并设 $\Delta'=\delta\Delta$。由引理 4.9、4.18、4.3 与 4.11，我们得到相应的高度界：

$$
\begin{aligned}
h(\Delta^{\text{separate\_H}}_{V_{i,k}^{\boldsymbol{A}},G_{i+1}}) &\in O(n^6D(d\ln(d)+h'+dH'+dD))\\
h(\Delta^{\text{intersection}}_{V_{i,k+1,\text{proper}}^{\boldsymbol{A}},G_{i+1}}) &\in O(n^6d^2DH'+n^6dh'D^2+n^7d^2D^2\ln(n))\\
h(\Delta^{\text{union}}_{V_{i,k,\text{zero}}^{\boldsymbol{A}},J_{i,k}^{\boldsymbol{A}}}) &\in O(n^6D(H'+D))\\
h(\Delta^{\text{separate}}_{Z_{i,k,\ell+1}^{\boldsymbol{A}},W_{i,\ell}^{\boldsymbol{A}}}) &\in O(n^6D^2(H'+D)).
\end{aligned}
$$

指标 i 有 s 个取值需要考虑，k 有 n 个取值，而 ℓ 至多有 n 个取值。为得到 Δ 的高度的总体上界，我们将它们全部纳入考虑，并使用不等式 $D\geq d$、$H'\geq h$、$H'\geq h'$。由此得到

$$h(\Delta)\in O(n^{10}s(d^2DH'+dh'D^2+d^2D^2+D^3+D^2H')).$$

利用 D 与 H 的上界，我们得到

$$h(\Delta)\in O(n^{13}shd^{3n+3}\ln(nd))\subset O(n^{14}shd^{3n+4}).$$

Δ' 的高度具有相同的渐近界。

最后，设 p 为不整除 Δ' 的素数，并称 Φ_0，……，Φ_n 为 $V(G_1$，……，$G_s)=V(F_1$，……，$F_s)^{\boldsymbol{A}}$ 的等维分支的归一化 Chow 形式。于是，由命题 5.4 可知，若对所有 i 令 $g_i=G_i$ 模 p，则 Φ_0，……，Φ_n 的系数均属于 $\mathbb{Z}_{(p)}$，$V(g_1$，……，$g_s)$ 的等维分支均处于正规位置，且 φ_0，……，$\varphi_n=\Phi_0$，……，Φ_n 模 p 是这些等维分支的归一化 Chow 形式。由于 δ 模 p 不消失，故 $V(g_1$，……，$g_s)=V(f_1$，……，$f_s)^{\boldsymbol{a}}$，其中对所有 i 有 $f_i=F_i$ 模 p，且 $\boldsymbol{a}=\boldsymbol{A}$ 模 p。

Let $\widetilde{\boldsymbol{A}}=[1]\oplus\boldsymbol{A}^T$，并令 $\widetilde{\boldsymbol{a}}$ 为其模 p 的约化。于是我们可以定义以下多项式：

- 对于 $i=0,\ \ldots,\ n$，令 $C_i=\Phi_i^{\widetilde{A}^{\oplus i+1}}$，其中 $\widetilde{\boldsymbol{A}}^{\oplus i+1}=\widetilde{\boldsymbol{A}}\oplus\cdots\oplus\widetilde{\boldsymbol{A}}$（$i+1$ 次）作用于 Φ_i 中由 $n+1$ 个变量组成的 $i+1$ 个块。因此，$C_0,\ \ldots,\ C_n$ 是 $V(F_1,\ \ldots,\ F_s)$ 的等维分支 $V_0,\ \ldots,\ V_n$ 的乔形式，且其系数仍属于 $\mathbb{Z}_{(p)}$；此外，对于所有 i，我们都可以写成 $C_i=C_{\text{本原}\,i}\ \ /\alpha_i$，其中某个整数为 α_i，而 $C_{\text{本原}\,i}$ 是 V_i 的本原肖氏形式（请回忆，这些形式仅在符号上有差异）。
- 类似地，对于 $i=0,\ldots,n$，我们令 $c_i=\varphi_i^{\widetilde{\boldsymbol{a}}^{\oplus i+1}}$，并且如上有 $\widetilde{\boldsymbol{a}}^{\oplus i+1}=\widetilde{\boldsymbol{a}}\oplus\cdots\oplus\widetilde{\boldsymbol{a}}$。由于$\varphi_i$是 $V(f_1,\ldots,f_s)$[a]的第 i 个等维分支的乔形式，因此如上所述，c_i 是 $V(f_1,\ldots,f_s)$ 的第 i 个等维分支 v_i 的乔形式。

由于 $c_i=C_i$ 模 p，前面的讨论得出 $C_i^{\text{primitive}}$ 模 $p=\alpha_i c_i$。另一方面，所有 α_i 模 p 均非零，因此 $\alpha_i c_i$ 是 v_i 的乔形式，对所有 i均成立。这意味着，只要 p 不整除 Δ'，定理 1.1 的结论就成立。

6 实验

为便于阅读，定理1.1的主要结果及其推导过程中的中间步骤，均以渐近记号给出高度上界。虽然可以为所有这些步骤推导出不等式，但编写并手动检查这些不等式很快就会变得复杂。因此，我们编写了一个 Maple 脚本，按照证明的整体结构计算实际上界。这里我们给出若干示例中的数值。

如引言中所述，D'Andrea 等人在 [7] 中给出了一个与主定理中的界类似的界，适用于已知解的数量有限的方程组 $\mathbb{C}^n$（特别是，如果给定方程的数量 s 小于 n，则这些方程组无解）。我们将此界记为 A，并将其与上一节中根据 Δ'导出的界进行比较，后者记为 B。对于每组参数（$n,\ s,\ d,\ h$），我们计算 A和 B的数值，并报告比值 B/A 以作比较。所有实验均在 Maple 中完成（参见代码库）。

我们逐一考察各个参数，每次改变一个参数，同时固定其余参数。表1中，我们考察 n，同时固定 $s=5$、$d=2$和 $h=10$。随着 n增大，界的增长速度比其他参数增大时更快。表2中，我们考察 s，同时固定 $n=5$、$d=2$和 $h=10$。表3中，我们考察 d，同时固定$n=3$、$s=5$和 $h=10$。最后，表4中，我们考察 h，同时固定 $n=3$、$s=5$和 $d=3$。

两篇论文中的界都涉及一个主导项 d^{3n}，乘以一个关于 nds 的多项式量，并且关于 h 呈线性，因此不出所料，对变量数 n 的依赖最为显著。在测试的示例中，B 的范围从约 10^6（当 n 较小时）到约 10^{61}（当 n 最大时）；而 s、d 和 h 的增加带来的变化则较为温和。在所有实验中，比例 B/A 约在 10^2 和 10^{11} 之间变化。

´**致谢**。Eric Schost 感谢加拿大自然科学与工程研究委员会（NSERC）通过探索性研究资助提供支持。Jesse Elliott 感谢 Inria 通过 OURAGAN 项目团队提供支持。

n	A	B	B/A
1	1.9921×10^{4}	3.4824×10^{6}	1.7481×10^{2}
2	2.3695×10^{5}	4.3930×10^{8}	1.8540×10^{3}
5	2.5031×10^{8}	3.3880×10^{13}	1.3535×10^{5}
10	1.5907×10^{13}	1.2561×10^{20}	7.8968×10^{6}
20	3.5113×10^{22}	2.2805×10^{31}	6.4947×10^{8}
50	1.1769×10^{50}	3.4204×10^{61}	2.9063×10^{11}

表1：变量数 n 的扫描。其余参数固定为 $s=5$,$d=2$, $h=10$。

s	A	B	B/A
2	2.0540×10^{8}	1.3552×10^{13}	6.5979×10^{4}
5	2.5031×10^{8}	3.3880×10^{13}	1.3535×10^{5}
10	2.8429×10^{8}	6.7760×10^{13}	2.3834×10^{5}
20	3.1827×10^{8}	1.3552×10^{14}	4.2580×10^{5}
50	3.6319×10^{8}	3.3880×10^{14}	9.3284×10^{5}
100	3.9717×10^{8}	6.7760×10^{14}	1.7061×10^{6}

表2：方程数量 s 的变化。其余参数固定为 $n=5$,$d=2$, $h=10$。

d	A	B	B/A
2	2.5455×10^{6}	2.6014×10^{10}	1.0219×10^{4}
3	2.0926×10^{8}	2.8950×10^{12}	1.3835×10^{4}
5	5.5270×10^{10}	1.3592×10^{15}	2.4593×10^{4}
10	1.0949×10^{14}	6.0890×10^{18}	5.5611×10^{4}
20	2.2045×10^{17}	2.7274×10^{22}	1.2372×10^{5}

表3：次数 d 的变化。其余参数固定为 $n=3$, $s=5$,$h=10$。

h	A	B	B/A
1	1.8959×10^{8}	1.6600×10^{12}	8.7556×10^{3}
2	1.9178×10^{8}	1.7972×10^{12}	9.3713×10^{3}
5	1.9833×10^{8}	2.2089×10^{12}	1.1137×10^{4}
10	2.0926×10^{8}	2.8950×10^{12}	1.3835×10^{4}
100	4.0589×10^{8}	1.5245×10^{13}	3.7559×10^{4}

表4：系数高度 h 的变化。其余参数固定为 $n=3$,$s=5$, $d=3$。

参考文献

[1] E. Bach 和 J. Shallit。算法数论；第一卷：高效算法。麻省理工学院出版社，1996年。

[2] Cristina Blanco、Gabriela Jeronimo 和 Pablo Solern´o。计算光滑仿射代数簇理想的生成元。《符号计算杂志》，38(1):843–872，2004年。[3] J. B¨ohm、W. Decker、C. Fieker 和 G. Pfister。坏素数在有理重构中的应用。《数学计算》，84:3013–3027，2012年。[4] D. Boyd。多变量多项式的克罗内克定理与莱默问题。《数论杂志》，13(1):116–121，1981年。[5] John Dalbec 和 Bernd Sturmfels。乔形式导论，第37–58页。施普林格荷兰，多德雷赫特，1995年。[6] M. Levent Dogan、Alperen A. Erg¨ur 和 Elias Tsigaridas。乔形式与赫尔维茨形式的复杂度。《*ACM*计算机代数通讯》，57(4):167–199，2024年3月。[7] C. D'Andrea、A. Ostafe、I. Shparlinski 和 M. Sombra。多项式方程组与代数动力系统的模素数约化。《美国数学会汇刊》，371(2):1169–1198，2019年。[8] J. Elliott 和 ´E. Schost。中国剩余定理纠错码的一些应用。载于*ISSAC'25*。ACM，2025年。[9] Jesse Elliott。可行性、连通性与 2^a-同源计算的复杂度。博士论文，滑铁卢大学，2025年。[10] Jesse Elliott 和 ´Eric Schost。中国剩余定理纠错码的一些应用。载于*SCSS 2024*：第十届国际软件科学符号计算研讨会，CEUR-WS.org，日本东京，2024年8月。CEUR研讨会论文集。[11] J. von zur Gathen 和 J. Gerhard。《现代计算机代数》。剑桥大学出版社，剑桥，第三版，2013 年。[12] I. M. Gelfand、M. M. Kapranov 和 A. V. Zelevinsky。判别式、结式与多维行列式。《数学：理论与应用》。波士顿 Birkh¨auser 公司，马萨诸塞州波士顿，1994年。[13] J. Heintz。代数闭域中的可定义性与快速量词消去。《理论计算机科学》，24(3):239–277，1983年。[14] J. Heintz 和 C. P. Schnorr。检验易于计算的多项式（扩展摘要）。载于*STOC*，第262–272页。ACM，1980年。[15] Gabriela Jeronimo、Teresa Krick、Juan Sabia 和 Martin Sombra。乔形式的计算复杂度。《计算数学基础》，4(1):41–117，2004年。

[16] T. Krick、L. M. Pardo 和 M. Sombra。算术零点定理的精确估计。《杜克数学杂志》，109:521–598，2001年。[17] L. Kronecker。《代数数论基础》。Journal für die reine und angewandte Mathematik，92:1–122，1882年。[18] S. Lang。《丢番图几何基础》。施普林格出版社，纽约，1983年。[19] F. Macaulay。《模系统代数理论》。剑桥大学出版社，1916年。[20] H. Matsumura。《交换环论》。剑桥高等数学研究丛书。剑桥大学出版社，1986年。[21] James S. Milne。《代数几何》（v6.1），2024年。网址：www.jmilne.org/math/。[22] D. Mumford。《代数几何 I：复射影簇》。数学经典丛书。施普林格出版社，1976年。[23] C. Pernet。《高性能可靠代数计算》。博士后资格论文，格勒诺布尔第一约瑟夫·傅里叶大学，2014年11月。[24] P. Philippon。《代数独立性判据》。《高等科学研究所数学出版物》，64:5–52，1986年。[25] P. Philippon。《论替代高度 III》。《纯粹与应用数学杂志》，74(4):345–365，1995年。[26] Stacks 项目作者。《Stacks 项目》。 https://stacks.math.columbia.edu，2025年。