arXiv:2602.01583v1 [math.AG] 2 Feb 2026

有限域上多元多项式绝对不可约性的新判据

Carlos Agrinsoni*,1,1，Heeralal Janwa[1,2],Moises Delgado[1,3]

摘要

代数簇的一项关键性质是其是否绝对不可约，也就是说，它在定义域的代数闭包上仍然不可约。判定绝对不可约性对于代数几何及其在编码理论、密码学等领域的应用都十分重要。

绝对不可约性的应用包括通过韦伊猜想界定有理点的数量，以及确立有限域上函数的例外几乎完美非线性（APN）和置换性质。本文提出了一种新的判据，用于判定有限域上由多元多项式定义的超曲面的绝对不可约性。假设首项形式无平方因子，我们的判据无需在基域或扩域中检验不可约性，只需进行多元最大公因式计算并确认其无平方因子性质。由于已知几乎所有多项式都无平方因子，因此，我们的绝对不可约性判据适用于几乎所有多元多项式。

关键词：绝对不可约性；有限域；多元多项式；次数间隙；无平方因子首型；代数几何；编码理论；密码学。

1. 引言

代数和代数几何中最重要的问题之一，是判定一个多项式是否不可约（或绝对不可约）。发展实用的判据来检验不可约性和绝对不可约性，对于纯数学和应用数学中的应用至关重要。对于

*通讯作者*Email addresses:* cagrinso@pudue.edu (CarlosAgrinsoni), heeralal.janwa@upr.edu(HeeralalJanwa)， moises.delgado@upr.edu (MoisesDelgado)[1]美国印第安纳州西拉斐特市北大学街150号，邮编47907-2067，普渡大学数学系。[2]波多黎各大学里奥彼德拉斯校区自然科学学院数学系，大学大道17号，1701室，圣胡安，波多黎各00925-2537。[3]波多黎各大学卡耶伊校区数学与物理系，安东尼奥·R·巴塞洛街205号，卡耶伊，波多黎各00736。

一元多项式，艾森斯坦判别法是检验不可约性的经典方法 [25]。这一判据已推广到利用牛顿多边形、素理想和赋值来检验多元多项式的不可约性（在某些情况下也检验其绝对不可约性）（例如，参见 [15, 47, 43]）。

绝对不可约性这一性质在数学的不同领域有许多应用，例如代数几何、组合学 [52], 编码理论[51, 35, 36], 密码学 [31], 有限几何 [32, 33], 函数域筛法 [1], 置换多项式 [46] 以及散布多项式 [11]。韦伊、Deligne 和 Bombieri 关于有理点数量及指数和的深刻结果，都要求底层代数簇是绝对不可约的（关于奇异曲线，参见 [9]）。

韦伊猜想在有理点数量和指数和的界的应用中发挥着关键作用。此外，给出有理点界的德利涅定理要求底层代数簇是绝对不可约的 [23]。将韦伊猜想推广到奇异曲线时，要求定义该奇异曲线的多项式是绝对不可约的 [9]。以下具体应用与我们的结果尤为相关。在编码理论和密码学中，通过证明由相应多元多项式定义的某个代数簇是绝对不可约的，或包含一个绝对不可约分支，在证明几乎完美非线性例外猜想方面取得了重大进展 [31]。Janwa 和 Wilson 针对单项式函数提出了这一猜想 [35] ，并取得了重大进展。他们的研究表明，现有的一种绝对不可约性检验判据十分有效，并且他们还提出了新的方法。五年后，Janwa 基于贝祖定理和交点重数提出了一个绝对不可约性判据。此后，Janwa、McGuire 和 Wilson 取得了重大进展 [36] ，基本解决了这一猜想。二十年后，Hernando 和 McGuire [32]终于证明了这一猜想。Aubry、McGuire 和 Rodier[8] 将这一猜想推广到有限域上的任意函数，并证明了相应代数簇存在一个绝对不可约因子。

本文研究由多元多项式定义的超曲面。用于检验多项式绝对不可约性的判据并不多。牛顿多边形方法以两种不同方式推广了艾森斯坦判别法：1）艾森斯坦–杜马判别法 [24, 55]；2）斯捷潘诺夫判别法（有时称为斯捷潘诺夫–施密特判别法） [48, 49, 50]。一种更一般的判据使用牛顿多面体 [27]。其他判据见[40, 53, 30, 13, 14, 45, 38, 39, 41, 44, 56, 42]。然而，在证明绝对不可约性定理时，这些算法往往并不实用。事实上，Gao 的一般判据通常并不实用，因为该算法需要判断多面体的不可分解性，而这已知是一个 NP 完全问题[27]。

我们在此提出的绝对不可约性检验，在证明 APN 猜想的重要部分时非常有效（见 [5, 7]）。我们采用的策略让人联想到 Janwa 和 Wilson [35]提出的绝对不可约性判据。Janwa、McGuire 和 Janwa 给出了一种极为有效的方法 [35, 36]，运用贝祖定理和交点重数。这种方法已被

用于解决塞格雷-巴托奇猜想 [32], ，并将一般的例外 APN 猜想在奇数情形下归结为仅涉及 Gold 和 Kasami-Welch 两种情形的指数。 [35, 8] 中的判据可应用于例外 APN 猜想、塞格雷-巴托奇猜想 [32], 以及 e。Aubry、McGuire 和 Rodier [8] 通过超平面交，将这类问题从三维降至二维，从而应用于一般的例外 APN 函数猜想。

本文提出的判据是对例外 APN 猜想证明的一项重要补充，此外还有其他应用。定义代数几何码的条件之一是其基础曲线具有绝对不可约性 [34]。在有限几何中，塞格雷-巴托奇猜想是通过证明一个多元多项式在定义域上含有绝对不可约因子而得到解决的。绝对不可约性是证明置换多项式为例外置换多项式的基础

我们先前的结果见 [21, 2]。我们还证明了关于定义域上存在绝对不可约因子的结果。根据 Weil、Deligne、Bombieri 和 Lachaud-Ghorpade 的界，该因子保证有足够多的有理点（见 [8, 35]），这有助于证明塞格雷-巴托奇猜想 [32] 以及例外平面猜想 [10], 、例外 APN 函数猜想等。

本文组织如下。第2节介绍背景知识。第3节证明本文的主要结果，即给出一个绝对不可约性判据（定理 8）。第4节推广次数间隙的概念，从而帮助我们改进此前关于绝对不可约因子数量的上界。由此，我们直接证明了一类多元多项式的绝对不可约性。最后一节总结全文。

2. 背景

若多元多项式 $G(\mathbf{X})$ 在 $\mathbb{F}(\mathbf{X})$ 中定义，且对 $\mathbb{F}$ 的每个扩张域都保持不可约，则称其为绝对不可约。此外，将 $G(\mathbf{X})$ 按次数递减顺序作分次齐次分解，可得

$$G(\mathbf{X}) = G_d(\mathbf{X}) + G_{d_1}(\mathbf{X}) \cdots + G_{d_m}(\mathbf{X}), \tag{1}$$

其中， $G_{d_i}(\mathbf{X})$ 是次数为 d_i, $1 \leq i \leq m$ 且 $d > d_1 > \cdots > d_m$ 的非零齐次多项式。在本文余下部分，多项式均写成按次数递减排列的齐次形式。齐次分量$G_{d_m}(\mathbf{X}) := T_G(\mathbf{X}) := T(\mathbf{X})$ 称为 G 的**切锥** 。

最近，在 [2] 中，我们将 Aubry、McGuire 和 Rodier [8]; Ferard [26]; 以及 Delgado 和 Janwa [17, 16, 18, 20, 19, 22] 用于分解首项形式无平方因子的多项式的技巧形式化了。在这一形式体系中，我们如下引入多项式次数间隙的概念。

定义1. 设 $F(\boldsymbol{X}) \in \mathbb{F}[X_1, \ldots, X_n]$ 是一个次数为 d 且至少含有两项的多项式。我们将方程 (1)中的分解所得到的差值 $d - d_1$ 定义为次数间隙 $\gamma(F)$。如果 $F(\boldsymbol{X})$ 是齐次多项式，则将$\gamma(F)$ 定义为无穷大。

定理2（Agrinsoni、Janwa 和 Delgado [2]）。设 $F(\boldsymbol{X}) = F_d(\boldsymbol{X}) + H(\boldsymbol{X}) \in \mathbb{F}[\boldsymbol{X}]$。若 $F_d(\boldsymbol{X})$ 无平方因子，则 $F(\boldsymbol{X})$ 的每个因子的次数间隙至少为$\gamma(F(\boldsymbol{X}))$。

引理*3*（*Agrinsoni*、*Janwa* 和 *Delgado* [2]）。设 $F(X) = F_d(X) + H(X) \in \mathbb{F}[X]$。若 $F_d(X)$ 无平方因子且 $(F_d, H) = 1$，则 $F(X)$ 至多有 $\left\lfloor \frac{deg(F)}{\gamma(F)} \right\rfloor$ 个因子。

在第4节中，我们通过引入多项式的 i^{th}-次数间隙，推广了多元多项式次数间隙的概念。此外，在定理12中，我们给出了充分条件，以保证多项式的因子至少具有一个间隙，其数值与原多项式的 i^{th}-次数间隙相同。该定理推广了定理2。作为这一结果的直接推论，我们推广了引理3。引理3对首项形式无平方因子且没有齐次因子的多项式的因子个数给出了上界。

Beelen 和 Pellikaan [12] 给出了关于一类特殊三项式的绝对不可约性的一个结果。最近，我们研究了首项形式无平方因子的少形式多元多项式的绝对不可约性，见命题（4、5 和 6）。在本文中，我们在定理 8 中给出了一个用于检验绝对不可约性的通用判据。下面的命题（我们先前的结果（4、5 和 6））现在可直接由我们的定理推出。

命题4（Agrinsoni、Janwa 和 Delgado [2]）。设 $F(\boldsymbol{X}) = F_d(\boldsymbol{X}) + F_m(\boldsymbol{X}) \in \mathbb{F}[X_1, \ldots, X_n]$，其中 $\deg(F) = d$。若 $F_d(\boldsymbol{X})$ 无平方因子，且$(F_d, F_m) = 1$，则 $F(\boldsymbol{X})$ 绝对不可约。

该命题对首项形式无平方因子时的广义二项式给出了完整刻画。

命题5（Agrinsoni、Janwa 和 Delgado [3]）。设 $F(X) = F_d(X) + F_{d-e}(X) + F_a(X) \in \mathbb{F}[X]$，其中 $d - e > a$。若 $F_d(X)$ 无平方因子，$(F_d, F_{d-e}, F_a) = 1$，且对于某个 $m \in \mathbb{Z}$，$a \neq d - me$，则 $F(X)$ 是绝对不可约的。

命题 *6*（*Agrinsoni*、*Janwa* 和 *Delgado* [4]）。设 $F(X) = F_d(X) + F_{d-\gamma_1}(X) + F_{d-\gamma_2}(X) + F_{d-\gamma_3}(X) \in \mathbb{F}[X]$。设 $F_d(X)$ 无平方因子，且 $(F_d, F_{d-\gamma_1}, F_{d-\gamma_2}, F_{d-\gamma_3}) = 1$。若 $\gamma_3 \notin$ 张成空间$_{\mathbb{N}}\{\gamma_1, \gamma_2\}$，则 $F(X)$ 是绝对不可约的。

本文表明，还有更多首项形式无平方因子的多元多项式是绝对不可约的。以下结果表明，我们的判据对几乎所有多元多项式都成立。

命题 7（Gao 和 Lauder [28]）。大多数多元多项式都无平方因子。

3. 新结果

在本文余下部分，我们假设 $0 \in \mathbb{N}$。

定理 8。设 $F(\boldsymbol{X}) = F_d(\boldsymbol{X}) + F_{d-\gamma_1}(\boldsymbol{X}) + \cdots + F_{d-\gamma_m}(\boldsymbol{X}) \in \mathbb{F}[\boldsymbol{X}]$。设$F_d(\boldsymbol{X})$无平方因子，且$(F_d, F_{d-\gamma_1}, \ldots, F_{d-\gamma_m}) = 1$。若 $\gamma_m \notin$ 张成空间$_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}$，则 $F(\boldsymbol{X})$ 是绝对不可约的。

Proof. 反设

$$F = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0), \tag{2}$$

其中 P_i （分别为 Q_j）是次数为 i （分别为 j）的型或零。现在

$$F_d = P_s Q_t. \tag{3}$$

令 $k \notin$ 张成空间$_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}$ **和** $0 < k < \gamma_m$。

在公式（2）的展开式中比较次数为 $d-k$ 的项，可得如下结果。

$$F_{d-k} = 0 = \sum_{i=0}^{k} P_{s-i} Q_{t-k+i} =$$

$$P_s Q_{t-k} + \sum_{\substack{i \notin \mathrm{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}, \\ 0<i<k}} P_{s-i} Q_{t-k+i} + P_{s-k} Q_t + \sum_{\substack{i \in \mathrm{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}, \\ 0<i<k}} P_{s-i} Q_{t-k+i}. \tag{4}$$

断言： 公式（4）可改写为

$$F_{d-k} = 0 = P_s Q_{t-k} + P_{s-k} Q_t, \tag{5}$$

对所有 $0 < k < \gamma_m$ 均成立。

为了证明该断言，只需证明

$$\sum_{\substack{i \notin \mathrm{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}, \\ 0<i<k}} P_{s-i} Q_{t-k+i} = 0, \tag{6}$$

and

$$\sum_{\substack{i \in \mathrm{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}, \\ 0<i<k}} P_{s-i} Q_{t-k+i} = 0. \tag{7}$$

第一部分：为导出矛盾，假设方程 (6)中的等号不成立，即它是 $\neq 0$。

设 $A = \{j \mid P_{s-j} \neq 0, j \notin$ 张成空间$_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}, \quad 0 < j < k\}$。根据我们的假设， $A \neq \emptyset$。然后，根据良序原理，存在一个极小元 $a \in A$。比较次数为 $d - a$ 的项，得到:

$$F_{d-a} = 0 = \sum_{i=0}^{a} P_{s-i} Q_{t-a+i} =$$

$$P_s Q_{t-a} + \sum_{i \notin \mathrm{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\},\ 0<i<a} P_{s-i} Q_{t-a+i} + P_{s-a} Q_t + \sum_{i \in \mathrm{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\},\ 0<i<a} P_{s-i} Q_{t-a+i}. \tag{8}$$

由 a 的极小性， $\sum_{i \notin \text{张成空间}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\},\ 0<i<a} P_{s-i} Q_{t-a+i} = 0$，因为对于所有 $i \in \{j \mid j \notin$ 张成空间$_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}, \quad 0 < j < a\}$，都有 $P_{s-i} = 0$。

断言：

$$\sum_{\substack{i \in \mathrm{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\} \\ 0<i<a}} P_{s-i} Q_{t-a+i} = 0. \tag{9}$$

反设方程（9）中的等式不成立。设 $B = \{j \mid Q_{t-a+j} \neq 0, j \in$ 张成空间$_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}\ 0 < j < a\}$。根据假设， $B \neq \emptyset$。然后，由于 B 是一个有限集，存在一个极大元 $b \in B$。注意， $a - b \notin$ 张成空间$_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}$。比较次数为 $d - a + b$ 的项，得到:

$$F_{d-a+b} = 0 = \sum_{i=0}^{a-b} P_{s-i} Q_{t-a+b+i} =$$

$$P_s Q_{t-a+b} + \sum_{\substack{i \notin \mathrm{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}, \\ 0<i<a-b}} P_{s-i} Q_{t-a+b+i} + P_{s-a+b} Q_t + \sum_{\substack{i \in \mathrm{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}, \\ 0<i<a-b}} P_{s-i} Q_{t-a+b+i}. \tag{10}$$

注意到

1. $\sum_{i \notin \text{张成空间}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\},\ 0<i<a-b} P_{s-i} Q_{t-b+i} = 0$，因为对于所有 $P_{s-i} = 0$， $i \in \{j \mid j \notin$ 张成空间$_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}, \quad 0 < j < a - b\}$，由 a 的极小性可知；2. $\sum_{i \in \text{张成空间}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\},\ 0<i<a-b} P_{s-i} Q_{t-a+b+i} = 0$，因为对于所有 $Q_{t-a+b+i} = 0$， $i \in \{j \mid j \in$ 张成空间$_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}$, $0 < j < a - b\}$，由 b 的极大性可知。

因此，方程（10）可改写如下

$$F_{d-a+b} = 0 = P_s Q_{t-a+b} + P_{s-a+b} Q_t.$$

这意味着 $P_s Q_{t-a+b} = -P_{s-a+b} Q_t$。因此， $P_s \mid P_{s-a+b} Q_t$ 和 $Q_t \mid P_s Q_{t-a+b}$。根据方程（3）以及 $F_d(\mathbf{X})$ 的无平方因子性，我们有 $(P_s, \ Q_t) = 1$。因此，由两个整除关系可得 $P_s \mid P_{s-a+b}$，并且 $Q_t \mid Q_{t-a+b}$。于是，$P_{s-a+b} = Q_{t-a+b} = 0$。这就产生了矛盾。因此，方程（9）为零。

现在，方程（8）可改写为

$$F_{d-a} = P_s Q_{t-a} + P_{s-a} Q_t.$$

这意味着 $P_s Q_{t-a} = -P_{s-a} Q_t$。因此， $P_{s-a} = Q_{t-a} = 0$。这是一个矛盾。因此，方程（6）等于零。

第二部分。假设方程（7）中的等式不成立，以导出矛盾。

令 $C = \{j \mid Q_{t-k+j} \neq 0, j \in \text{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\},\ 0 < j < k\}$。根据我们的假设， $C \neq \emptyset$。那么，由于 C 是一个有限集，存在一个极大元$c \in C$。比较次数为 $d-k+c$ 的项，我们得到:

$$F_{d-k+c} = 0 = \sum_{i=0}^{k-c} P_{s-i} Q_{t-k+c+i} =$$

$$P_s Q_{t-k+c} + \sum_{\substack{i \notin \text{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}, \\ 0<i<k-c}} P_{s-i} Q_{t-k+c+i} + P_{s-k+c} Q_t + \sum_{\substack{i \in \text{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}, \\ 0<i<b}} P_{s-i} Q_{t-k+c+i}. \tag{11}$$

注意
1. $\sum_{i \notin \text{张成空间}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\},\ 0<i<k-c} P_{s-i} Q_{t-k+c+i} = 0$ ，因为对于所有 $i \in \{j \mid j \notin \text{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\},\ 0 < j < k-c\}$ ，根据方程（6）的证明; 以及 2. $\sum_{i \in \text{张成空间}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\},\ 0<i<b} P_{s-i} Q_{t-k+c+i} = 0$，因为对于所有 $i \in \{j \mid j \in \text{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\},\ 0 < j < b\}$ ，根据 c的极大性。

因此，方程 (11) 可改写为

$$F_{d-k+c} = 0 = P_s Q_{t-k+c} + P_{s-k+c} Q_t.$$

这意味着 $P_s Q_{t-k+c} = -P_{s-k+c} Q_t$。因此， $P_{s-k+c} = Q_{t-k+c} = 0$。这是一个矛盾。因此，方程 (7) 等于零。因此，方程 (5) 成立。这意味着 $P_s Q_{t-k} = -P_{s-k} Q_t$。

因此，对于所有 $k \notin$ 张成空间$_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}$和$0 < k < \gamma_m$**，** $P_{s-k} = Q_{t-k} = 0$。

因此，对次数为 $d - \gamma_m$ 的形式进行比较，我们得到

$$F_{d-\gamma_m} = \sum_{i=0}^{d-\gamma_m} P_{s-i} Q_{t-\gamma_m+i} =$$

$$P_s Q_{t-\gamma_m} + \sum_{\substack{i \notin \text{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}, \\ 0<i<\gamma_m}} P_{s-i} Q_{t-\gamma_m+i} + P_{s-\gamma_m} Q_t + \sum_{\substack{i \in \text{span}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}, \\ 0<i<\gamma_m}} P_{s-i} Q_{t-\gamma_m+i}. \tag{12}$$

现在 $\sum_{i \notin \text{张成空间}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\},\ 0<i<\gamma_m} P_{s-i} Q_{t-\gamma_m+i} = 0$，因为 $P_{s-i} = 0$ 对于每个$i \in \{j \mid j \notin$ 张成空间$_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\},\ 0 < j < \gamma_m\}$和$\sum_{i \in \text{张成空间}_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\},\ 0<i<\gamma_m} P_{s-i} Q_{t-\gamma_m+i} = 0$，因为 $Q_{t-\gamma_m+i} = 0$ 对于每个

$i \in \{j \mid j \in$ 张成空间$_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}, \quad 0 < j < \gamma_m\}$。因此，方程可以简化为 (12)

$$F_{d-\gamma_m} = P_s Q_{t-\gamma_m} + P_{s-\gamma_m} Q_t. \tag{13}$$

F(**X**) 的切锥是 P 与 Q 的切锥之积（因为多项式的最低次型等于其因子的最低次型之积）。因此，存在 b', c' 使得

$$F_{d-\gamma_m} = P_{s-b'} Q_{t-c'}, \tag{14}$$

并且 $P_{s-i} = 0$ 对于 $i > b'$，而 $Q_{t-j} = 0$ 对于 $j > c'$。

由于 $F_{d-\gamma_m}$(**X**) 是 F(**X**) 的切锥，因此它是 P 和 Q 的切锥之积。因此，$P_{s-\gamma_m} = 0$ 或 $Q_{t-\gamma_m} = 0$。若 $P_{s-\gamma_m} = 0$，则根据方程 (13)，P(**X**) 的切锥为 P_s。这与 $(F_d, F_{d-\gamma_1}, \ldots\ldots, F_{d-\gamma_m}) = 1$ 矛盾。类似地，若 $Q_{t-\gamma_m} = 0$，则根据方程 (13)，Q(**X**) 的切锥为 Q_t。这与 $(F_d, F_{d-\gamma_1}, \ldots\ldots, F_{d-\gamma_m}) = 1$ 矛盾。

作为该定理证明的直接推论，我们得出以下引理。

引理*9*。设 $F(X) = F_d(X) + F_{d-\gamma_1}(X) + \cdots + F_{d-\gamma_m}(X) \in \mathbb{F}[X]$。设 $F_d(X)$ 无平方因子，且 $(F_d, F_{d-\gamma_1}, \ldots, F_{d-\gamma_m}) = 1$。若 $\gamma_i \notin$ 张成空间$_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{i-1}\}$且 $F(X) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0)$，则 $F_{d-\gamma_i} = P_s Q_{t-\gamma_i} + P_{s-\gamma_i} Q_t$

引理*10*。设 $F(X) = F_d(X) + F_{d-\gamma_1}(X) + \cdots + F_{d-\gamma_m}(X) \in \mathbb{F}[X]$。设$F_d(X)$ 无平方因子，且 $(F_d, F_{d-\gamma_1}, \ldots, F_{d-\gamma_m}) = 1$。若 $k \notin$ 张成空间$_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{m-1}\}, 0 < k < \gamma_m$，且 $F(X) = (P_s + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0)$，则 $F_{d-k} = P_s Q_{t-k} + P_{s-k} Q_t$

4. 次数间隙概念的推广以及绝对不可约因子个数的改进的上界

定义11. 设 $F(\boldsymbol{X}) = F_d(\boldsymbol{X}) + F_{d-\gamma_1}(\boldsymbol{X}) + \cdots + F_{d-\gamma_m}(\boldsymbol{X}) \in \mathbb{F}[\boldsymbol{X}]$ 与$F_d(\boldsymbol{X})$ 是无平方因子的。我们将 i^{th}-次数间隙 $\gamma_i(F)$ 定义为 $d - \gamma_i$。若 $F(\boldsymbol{X})$包含少于 i 个形式，则 $\gamma_i(F)$ 定义为无穷大。

定理*12.* 设 $F(X) = F_d(X) + F_{d-\gamma_1} + F_{d-\gamma_2}(X) + \cdots + F_{d-\gamma_m}(X) \in \mathbb{F}[X]$。设 $k \in \{1, 2, \ldots, m\}$ 使得 $\gamma_k \notin$ 张成空间$_{\mathbb{N}}\{\gamma_1, \gamma_2, \ldots, \gamma_{k-1}\}$ 且 $(F_d, F_{d-\gamma_k}) = 1$。若 $P(X) \mid F(X)$，且 $F_d(X)$ 是无平方因子的，则 $deg(P) \geq \gamma_k$。

Proof. 令 F(**X**) $= (P_S + P_{s-1} + \cdots + P_0)(Q_t + Q_{t-1} + \cdots + Q_0)$，其中 P_i（分别为 Q_j）是次数为 i（分别为 j）的型或零。于是

$$F_d = P_s Q_t$$

其中 $(P_s, Q_t) = 1$。根据定理 8 对 $i \notin \text{span}_{\mathbb{N}}\{\gamma_1, \ldots, \gamma_{k-1}\}, i < \gamma_k$ 的证明，我们有

$$F_{d-i} = P_s Q_{t-i} + P_{s-i} Q_t.$$

由于 $F_{d-i} = 0$,

$$P_s Q_{t-k} = P_{s-k} Q_t.$$

因此，$P_s \mid P_{s-i}$ 和 $Q_t \mid Q_{t-i}$，于是对于所有 $i \notin$，$P_{s-i} = Q_{t-i} = 0$ 张成空间$_{\mathbb{N}}\{\gamma_1, \ldots, \gamma_{k-1}\}$，$i < \gamma_k$。

考虑次数为 $d - \gamma_k$ 的齐次形式。

$$F_{d-\gamma_k} = \sum_{i=0}^{\gamma_k} P_{s-i} Q_{t-\gamma_k+i} =$$

$$P_s Q_{t-\gamma_k} + \sum_{\substack{i \notin \text{span}_{\mathbb{N}}(\gamma_1, \ldots \gamma_{k-1}), \\ 0<i<\gamma_k}} P_{s-i} Q_{t-\gamma_k+i} + P_{s-\gamma_k} Q_t + \sum_{\substack{i \in \text{span}_{\mathbb{N}}(\gamma_1, \ldots \gamma_{k-1}), \\ 0<i<\gamma_k}} P_{s-i} Q_{t-\gamma_k+i}. \tag{15}$$

注意，根据定理 8 的证明:

1. $\sum_{\substack{i \notin \text{span}_{\mathbb{N}}(\gamma_1, \ldots \gamma_{k-1}), \\ 0<i<\gamma_k}} P_{s-i} Q_{t-k+i} = 0$ as $P_{s-i} = 0$ for all $i \notin \text{span}_{\mathbb{N}}(\gamma_1, \ldots \gamma_{k-1})$, $0 < i < \gamma_k$.
2. $\sum_{\substack{i \in \text{span}_{\mathbb{N}}(\gamma_1, \ldots \gamma_{k-1}), \\ 0<i<\gamma_k}} P_{s-i} Q_{t-\gamma_k+i} = 0$ as $Q_{t-\gamma_k+i} = 0$ for all $i \in \text{span}_{\mathbb{N}}(\gamma_1, \ldots \gamma_{k-1})$, $0 < i < \gamma_k$.

因此，我们可以将方程（15）改写为

$$F_{d-\gamma_k} = P_s Q_{s-\gamma_k} + P_{s-\gamma_k} Q_t. \tag{16}$$

由于 $(F_d,\ F_{d-\gamma_k}) = 1$，$Q_{t-\gamma_k} \neq 0$ 和 $P_{s-\gamma_k} \neq 0$。因此，$s - \gamma_k \geq 0$，于是$s = \deg(P) \geq \gamma_k$。

注 13. 该定理的一个直接推论是，如果 $P(X) = P_s + P_{s-1} + \cdots + P_0$ 是 $F(X)$的一个因子，那么 $P_{s-\gamma_k} \neq 0$，其中 k 是定理*12*中的一个。

推论 14. 设 $F(\boldsymbol{X}) = F_d(\boldsymbol{X}) + F_{d-\gamma_1}(\boldsymbol{X}) + \cdots + F_{d-\gamma_m}(\boldsymbol{X}) \in \mathbb{F}[\boldsymbol{X}]$。设 $k \in \{1, \ldots, m\}$ 为满足定理*12*条件的最大 k。如果F_d无平方因子，那么 $F(\boldsymbol{X})$ 至多有 $\left\lfloor \deg\left(\frac{F}{\gamma_k}\right) \right\rfloor$ 个因子。

推论 15. 设 $F(\boldsymbol{X}) = F_d(\boldsymbol{X}) + F_{d-\gamma_1}(\boldsymbol{X}) + \cdots + F_{d-\gamma_m}(\boldsymbol{X}) \in \mathbb{F}[\boldsymbol{X}]$。设$k \in \{1, \ldots, m\}$ 为满足定理*12*条件的最大 k。如果F_d 无平方因子且 $\gamma_m < 2\gamma_k$，那么 $F(\boldsymbol{X})$ 是绝对不可约的。

Proof. 假设 $F(\mathbf{X}) = P(\mathbf{X}) Q(\mathbf{X})$。那么根据注 13，我们有$P_{s-\gamma_k} \neq 0$和 $Q_{t-k} \neq 0$。因此，$\deg(T_F) = d - \gamma_m \leq \deg(P_{s-\gamma_k} * Q_{t-\gamma_k}) = s - \gamma_k + t - \gamma_k = d - 2\gamma_k$。因此，$\gamma_m \geq 2\gamma_k$ 矛盾。

5. 结论

多元多项式的绝对不可约性检验在数论和代数几何中非常重要。

本文给出了绝对不可约性判据：在首项形式无平方因子的前提下，无需检验多项式在基域或扩张域上是否不可约。我们需要进行多元最大公因式计算，并要求多项式具有无平方因子的性质。对于二元多项式，这两个条件可归结为对首项齐次形式对应的单变量多项式进行不可约性检验。有限域上的不可约性检验已有快速算法。因此，我们得到了有限域上曲线的快速绝对不可约性判据。鉴于有限域上的曲线在编码理论、密码学和组合学中有诸多应用，我们给出的绝对不可约性判据具有重要的应用价值。

事实上，我们已将该判据用于证明 APN 多项式和例外多项式的绝对不可约性。因此，我们在解决 Agrinsoni、Janwa 和 Delgado [6] 中的例外 APN 猜想方面取得了进展。

正如我们所引述的，几乎所有多项式都已知是无平方因子的；我们的绝对不可约性判据适用于几乎所有多元多项式。我们通过反例证明，我们的判据已是最优的。

现有判据，例如 Stepanov 给出的判据 [49, 50], ，仅适用于非常特定类型的多项式（例如，库默尔扩张）。Gao 的一般判据通常并不实用，因为该算法要求多面体具有不可分解性，而这一问题已知是 NP 完全的 [27]。

参考文献

[1] L. M. Adleman. 函数域筛法。载于算法数论（伊萨卡，纽约州，*1994*），第877卷*Lecture Notes in Comput. Sci.*，第108–121页。施普林格，柏林，1994年。[2] C. Agrinsoni、H. Janwa 和 M. Delgado. 多元多项式的新绝对不可约性检验准则与因式分解。载于：Hoffman 等（编），组合学、图论与计算。*SEICCGTC 2021*，Springer Proc. Math. Stat.，第448卷，施普林格，Cham，2024年。[3] C. Agrinsoni、H. Janwa 和 M. Delgado. 有限域上多元多项式的新绝对不可约性准则。载于：Heuss 等（编），组合学、图论与计算。*SEICCGTC 2022*，Springer Proc. Math. Stat.，第462卷，施普林格，Cham，2024年。[4] C. Agrinsoni、H. Janwa 和 M. Delgado. 有限域上广义四项式绝对不可约性的新准则。载于：Hoffman 等（编），组合学、图论与计算。*SEICCGTC 2024*，Springer Proc. Math. Stat.，施普林格，Cham，2026年4月。

[5] C. Agrinsoni、H. Janwa 和 M. Delgado，《Gold 次数情形下例外 APN 猜想的解决》，Designs, Codes and Cryptography 1–20，2025年。[6] C. Agrinsoni、H. Janwa 和 M. Delgado，朝着解决 Kasami–Welch 次数情形下的例外 APN 猜想迈进，*Journal of Algebra andIts Applications*，第24卷，第10期，文章编号2541029，第2481–2495页，2025年。doi：https://doi.org/10.1142/S0219498825410291 0.1142/S0219498825410291。[7] C. Agrinsoni、H. Janwa 和 M. Delgado，解决例外几乎完美非线性猜想的进展：偶数情形。预印本，拟投稿。[8] Y. Aubry、G. McGuire 和 F. Rodier. 若干个并非无限多次为 APN 的新函数。载于*Finite Fields: Theory and Applications*，Contemp. Math. 518，第23–31页，AMS，2010年。[9] Y. Aubry 和 M. Perret. 奇异曲线的韦伊定理。载于*Arithmetic,Geometry and Coding Theory*，第1–7页，de Gruyter，1996年。[10] D. Bartoli 和 K.-U. Schmidt. 特征二有限域上的低次数平面多项式。*Journal of Algebra*，535：541–555，2019年。[11] D. Bartoli 和 M. Montanucci. 朝着例外散布多项式的完整分类迈进。*arXiv:1905.11390*，2019年。[12] P. Beelen 和 R. Pellikaan. 具有许多有理点的平面曲线的牛顿多边形。*Designs, Codes and Cryptography*，21：41–67，2000年。[13] E. R. Berlekamp. 有限域上的多项式因式分解。*Bell SystemTech. J.*，46：1853–1859，1967年。[14] E. R. Berlekamp. 大有限域上的多项式因式分解。*Math.Comp.*，24：713–735，1970年。[15] J. W. S. Cassels. *Local Fields*。剑桥大学出版社，1986年。[16] M. Delgado 和 H. Janwa. APN 函数猜想及绝对不可约多项式方面的进展。*arXiv:1602.02576*，2016年。[17] Moises Delgado 和 Heeralal Janwa. 关于 $\mathbb{P}^3$ 中广义费马簇超平面截面的绝对不可约性，以及例外 APN 函数猜想：Kasami-Welch 次数情形。*arXiv* 预印本 *arXiv:1612.05997*，2016年。[18] Mois´es Delgado 和 Heeralal Janwa. 关于 Gold 次数情形下例外 APN 猜想的完成及绝对不可约多项式。*Congr. Numer.*，第229卷，第135–142页，2017年。

[19] Delgado M., Janwa H.,《广义费马簇的分解：对应于 Kasami-Welch 函数的 P^3》，Congr. Numer.，第 232 卷，页码 101–111，2020年。[20] Moises Delgado 和 Heeralal Janwa，《关于 APN 函数猜想与多项式绝对不可约性的研究》。Des. Codes Cryptogr.，页码 617–627，2017年。[21] M. Delgado 和 H. Janwa，《Gold 次数情形下例外 APN 猜想的完成》。Congr. Numer.，229:135–142，2017年。[22] M. Delgado 和 H. Janwa，《关于例外 APN 函数猜想的一些新结果》。Adv. Math. Co mmun.，页码 389–396，2017年。[23] P. Deligne，《Weil 猜想 I》，Publ. Math. IHES 43 (1974)，273–307。[24] G. Dumas，《关于有理数系数多项式不可约性的若干情形》，J. Math. Pures Appl. 2 (1906)，191–258。.[25] G. Eisenstein，《关于整 lemniscate 的分割所满足方程的不可约性及其他一些性质》，J. Reine Angew. Math. 39 (1850)，160–179。[26] E. F´erard，《一类无限多次不具几乎完美非线性性质的 Kasami 函数》。载于 Contemp. Math. 686，页码 45–63，AMS，2017年。[27] S. Gao，《通过牛顿多面体判定多项式的绝对不可约性》。Jour- nal of Algebra，237:501–520，2001。[28] S. Gao 和 A. Lauder，《有限域上通过亨泽尔提升进行二元多项式因式分解》。Mathematics of Computation，71(240):1663–1676，2002。[29] S. Gao，《通过偏微分方程分解多元多项式》。Math. Comp.，72:801–822，2003。[30] J. Heintz 和 M. Sieveking，《多项式的绝对素性可在关于变量数的随机多项式时间内判定》。载于《自动机、语言与编程》（阿科，1981），Lecture Notes in Comput. Sci. 第 115 卷，页码 16–28。施普林格，柏林-纽约，1981年。[31] F. Hernando 和 G. McGuire，《关于例外数序列猜想的证明：循环码与 APN 函数的分类》，J. Algebra 343 (2011)，78–92。[32] F. Hernando 和 G. McGuire，《Segre 和 Bartocci 关于单项式超卵形猜想的证明》，Des. Codes Cryptogr. 65 (2012)，275–289。[33] J. W. P. Hirschfeld，《有限域上的射影几何》，Oxford Mathematical Monographs，牛津大学出版社，1979年。

[34] T. Høholdt、J. H. Van Lint 和 R. Pellikaan。《代数几何码》。Handbook of coding theory，1(Part 1):871–961，1998。[35] H. Janwa 和 R. M. Wilson，《特征为 2 时 P^3 中的费马簇超平面截面及其在循环码中的应用》，载于 AAECC 1993，Lecture Notes in Comput. Sci.，第 673 卷，施普林格，1993年，180–194。[36] H. Janwa、G. McGuire 和 R. M. Wilson，《双纠错循环码与 GF(2) 上的绝对不可约多项式》，J. Algebra 178 (1995)，665–676。[37] D. Jedlicka，《对无限多个 n，GF(2^n) 上的 APN单项式》。Finite Fields Appl.，13(4):1006–1028，2007。[38] E. Kaltofen，《从多元到二元整系数多项式分解的多项式归约》。载于第十四届 ACM 计算理论年度研讨会论文集，页码 261–266，1982。[39] E. Kaltofen，《从二元到一元整系数多项式分解的多项式时间归约》。载于第二十三届计算机科学基础年度研讨会（伊利诺伊州芝加哥，1982），页码 57–64。IEEE，纽约，1982。[40] E. Kaltofen，《快速并行绝对不可约性检验》，J. Symbolic Com- put. 1 (1985)，57–67。[41] E. Kaltofen，《从多元到二元及一元整系数多项式分解的多项式时间归约》。SIAM J. Comput.，14(2):469–489，1985。[42]E. Kaltofen，《有效的诺特不可约形式及其应用》，J. Comput. System Sci. 50 (1995)，274–295。[43] S. K. Khanduja 和 J. Saha，《关于艾森斯坦不可约性判据的一种推广》，Mathematika 44 (1997)，第 1 期，37–41。[44] A. K. Lenstra，《有限域上的多元多项式分解》。J. Comput. System Sci.，30(2):235–248，1985。[45] A. K. Lenstra、H. W. Lenstra 和 L. Lov´asz，《有理数系数多项式的因式分解》，Math. Ann. 261 (1982)，515–534。[46] R. Lidl 和 H. Niederreiter，《有限域》，数学及其应用百科全书，第 20 卷，Addison–Wesley，1983年。[47] S. MacLane，《用素理想表述的 Sch¨onemann–Eisenstein 不可约性判据》，Trans. Amer. Math. Soc. 43 (1938)，226–239。[48] W. Schmidt，《有限域上的方程：初等方法》。Kendrick Press，希伯城，UT，第二版，2004年。

[49] S. A. Stepanov. 二元同余. 苏联科学院数学系列学报, 36:683–711, 1972年.
[50] S. A. Stepanov. 有限域上代数曲线的有理点. 载于解析数论当前问题, 1974年.[51]H. Stichtenoth, 代数函数域与编码, Universitext, 施普林格, 1993年.[52] T. Sz˝onyi, 代数曲线在有限几何和组合学中的若干应用，载于《组合学综述，*1997*》, 伦敦数学学会讲义系列，第241卷，剑桥大学出版社，1997年，197–236.[53] J. von zur Gathen. 多元多项式的不可约性. 计算机与系统科学杂志, 31(2):225–264, 1985年。专刊：第二十四届计算机科学基础年会（图森，亚利桑那州，1983年）.[54] J. von zur Gathen and J. Gerhard. 现代计算机代数. 剑桥大学出版社，2013年.[55] D. Wan，多项式的最小多项式与克洛斯特曼和的互异性，有限域及其应用1 (1995年), 189–203.[56] P. J. Weinberger. 求多项式因子的个数. 算法杂志, 5(2):180–186, 1984年。