arXiv:2305.03906v1 [cs.SC] 6 May 2023

一般基下单变量多项式的 B´ezout 子结式

Jing Yang、Wei Yang*

SMS–HCIC–数学与物理学院，广西应用数学中心，广西民族大学，南宁 530006，中国

yangjing0930@gmail.com；

weiyang020499@163.com

摘要

子结式是计算机代数中开发各种算法的强大工具。目前，标准基（即幂基）下多项式的子结式已得到充分研究。随着保基算法日益普及，非标准基下的结式和子结式也越来越受到关注。本文提出了一般基下单变量多项式的 B´ezout 子结式公式，该公式涵盖了广泛的非标准基。具体而言，输入多项式以给定的一般基表示，所得子结式则是在同一基下的 B´ezout 型表达式。研究表明，这些子结式具有与标准基下子结式相同的基本性质。

1 引言

结式理论在计算机代数中发挥着基础性作用。鉴于其重要性，研究人员从理论和实践两个方面对结式、子结式及其变体开展了大量研究（仅举几例 $[5,7,9,10,13,17,20,21,23,24,26,27]$）。然而，大多数研究都聚焦于标准基（也称为幂基）下的多项式。具体而言，输入多项式以标准基表示，输出的子结式多项式也以标准基表示。随着保基算法在各种应用中的日益普及 $[1,8,12,15,16],$，人们对非标准基下多项式的结式和子结式越来越感兴趣（参见 $[3,6,25,28]$）。本文将研究一般基下的 B´ézout 子结式多项式（见定义 1），它涵盖了广泛的非标准基。许多著名的基都属于这一类，例如牛顿基和霍纳基；标准基也可以视为一般基的一个实例。在本文的设定中，输入多项式以一般基表示，输出的子结式多项式也以一般基表示。

通常，子结式多项式以行列式多项式的形式表示。这是因为行列式多项式是结式矩阵的子式之和，而结式矩阵具有良好的代数结构。这些结构通常会为理论发展和后续应用带来诸多便利。在本文中，我们采用这一方法。具体而言，我们将行列式多项式的概念从幂基扩展到一般基，并构造

*通讯作者。

了两个单变量多项式的子结式多项式的广义行列式多项式公式。用于构造该行列式多项式的矩阵是 B´ezout 矩阵，因此我们将所得的子结式多项式称为 B´ezout 子结式多项式。结果表明，所构造的子结式多项式具有标准基下子结式多项式的基本性质（见命题6）。

为了推导一般基下单变量多项式的 Bézout 子结式多项式公式，我们首先回顾文献 [3] 中给出的非标准基下 Bézout 矩阵的定义。由于子结式多项式的次数通常低于输入多项式，为了用给定的基表示子结式多项式，我们对非标准基施加一个自然约束，要求该基为一般基。在上述设定下，我们证明，子结式多项式可以写成非标准基下 Bézout 矩阵某个子矩阵的广义行列式多项式。

与此前其他相关工作相比，新推导出的基于一般基的单变量多项式的 B´ezout 子结式多项式公式具有以下特点。首先，它可以看作是幂基中 B´ezout 型子结式多项式的推广 [2, 22]。其次，它也是非标准基中结式的推广 [4, 14, 18,29, 30]。需要指出的是，本文的主要贡献在于从理论上验证了利用 B´ezout 矩阵在一般基中构造子结式多项式的可能性，而非提出一种高效方法来计算任意给定一般基中的子结式。事实上，几乎不可能为后者提供统一的解决方案，因为这在很大程度上取决于所选基的结构。

本文结构如下。第 2 节首先回顾 B´ézout 结式矩阵和以根定义的子结式多项式的概念，以及它们与最大公因式问题之间的内在联系。第 3 节介绍本文的主要结果（见定理 8）。第 4 节验证主定理的正确性。第 5 节对本文作总结，并给出一些进一步的评述。

2 预备知识

全文中，假设 $\mathbb{F}$ 是一个整环的分式域，$\overline{\mathbb{F}}$ 是 $\mathbb{F}$ 的代数闭包。令 $\mathbb{F}_n[x]$ 表示由 $\mathbb{F}[x]$ 中所有次数不大于 n 的多项式组成的集合。

2.1 一般基中的 B´ézout 结式

定义 1. 设 $\boldsymbol{\omega}(x) = (\omega_s, \ldots, \omega_1, \omega_0)^T$ 为 $\mathbb{F}_s[x]$ 的基，其中 ω_i 是首一的，且 $\deg \omega_i = i$。则称 $\boldsymbol{\omega}(x)$（或简称 $\boldsymbol{\omega}$）为 $\mathbb{F}_s[x]$ 的一般基。若不存在歧义，也将 $\boldsymbol{\omega}(x)$ 或 $\boldsymbol{\omega}$ 简称为一般基。

例如，标准基 $\boldsymbol{x} = (x^s, \ldots, x^1, x^0)^T$ 是 $\mathbb{F}_s[x]$ 一般基的一种特例，因为 $\deg x^i = i$。

另一种常用的一般基特例是牛顿基 $\boldsymbol{\omega}(x) = (\omega_s, \ldots, \omega_1, \omega_0)^T$，它与 $\lambda = (\lambda_s, \ldots, \lambda_1) \in \mathbb{F}^s$ 相关，其中

$$\omega_i = \begin{cases} 1, & \text{for } i = 0; \\ (x - \lambda_i)\omega_{i-1}, & \text{for } i > 0, \end{cases}$$

因为很容易验证 $\deg \omega_i = i$。本文主要研究一般基中的多项式的 B´ezout 子结式。

考虑一般基 $\boldsymbol{\omega}(x) = (\omega_n, \ldots, \omega_1, \omega_0)^T$ 中次数分别为 n 和 m 的 F、$G \in \mathbb{F}[x]$（其中 $n > m$）。更明确地说，我们假设

$$F(x) = \sum_{i=0}^{n} a_i \omega_i, \quad G(x) = \sum_{i=0}^{m} b_i \omega_i. \tag{1}$$

为了构造 $\boldsymbol{\omega}$ 中 F 和 G 的 B´ezout 矩阵，我们回顾下面这个众所周知的凯莱商。F 和 G 的凯莱商定义为

$$C(x, y) = \frac{\begin{vmatrix} F(x) & F(y) \\ G(x) & G(y) \end{vmatrix}}{x - y}.$$

注意到，两个多项式的凯莱商与用于表示输入多项式的基无关。

定义 2（B´ezout 矩阵）。设 $\boldsymbol{\omega} = (\omega_n, \ldots, \omega_1, \omega_0)^T$ 是 $\mathbb{F}_n[x]$ 的一般基，且 F、G 如（1）所示。则 F 和 G 在基 $\boldsymbol{\omega}$ 下的 B´ezout 矩阵定义为一个 $n \times n$ 矩阵 $\boldsymbol{B}_{\boldsymbol{\omega}}$，使得

$$C(x, y) = \bar{\boldsymbol{\omega}}(x)^T \cdot \boldsymbol{B}_{\boldsymbol{\omega}} \cdot \bar{\boldsymbol{\omega}}(y)$$

其中 $\bar{\boldsymbol{\omega}} = (\omega_{n-1}, \ldots, \omega_0)^T$.

注意，定义 2 中的 B´ezout 矩阵高度依赖于基。当 $\boldsymbol{\omega} = \boldsymbol{x}$, $\boldsymbol{B}_{\boldsymbol{\omega}}$ 时，它变为熟悉的标准基下的 B´ezout 矩阵，记为 $\boldsymbol{B}$。显然，$\boldsymbol{B} = \boldsymbol{U}^T \boldsymbol{B}_{\boldsymbol{\omega}} \boldsymbol{U}$，其中 $\boldsymbol{U}$ 是从基 $\bar{\boldsymbol{x}} = (x^{n-1}, \ldots, x^1, x^0)^T$ 到 $\bar{\boldsymbol{\omega}}$ 的过渡矩阵。

2.2 标准基中的子结式

在经典结式理论中，子结式扩展了结式的概念，其定义为子结式多项式的首系数；该子结式多项式可表示为输入多项式的著名西尔维斯特结式矩阵的某个子矩阵的行列式多项式。在 [22], Hou和Wang证明了，子结式多项式也可以表示为B´ézout矩阵某个子矩阵的行列式多项式。需要指出的是，在 [22] 中，用于构造B´ézout矩阵以及表述子结式多项式和子结式的基是标准基。请注意，前文讨论的结式和子结式均表示为关于 F 和 G 的系数的多项式，而它们高度依赖于所使用的基和采用的结式矩阵。在 [11, 13, 19], Hong等人以根的形式给出了子结式的一个等价定义，该定义不依赖于这两者。在剩余部分中，我们采用以根表示的子结式定义。在给出形式化定义之前，为简便起见，先介绍以下记号。

记号3.

- $\alpha_1, \ldots, \alpha_n$ *are the* n *roots of* F *over* $\overline{\mathbb{F}}$;
- $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n)$;
- $\boldsymbol{\alpha}_{ij} := (\alpha_i^j, \ldots, \alpha_i^1, \alpha_i^0)^T$;
- $\boldsymbol{V}(\boldsymbol{\alpha}) := \begin{bmatrix} \alpha_1^{n-1} & \cdots & \alpha_n^{n-1} \\ \vdots & \ddots & \vdots \\ \alpha_1^0 & \cdots & \alpha_n^0 \end{bmatrix}$;

- $\boldsymbol{x}_j := (x^j, \ldots, x^1, x^0)^T$.

定义 4. 给定次数分别为 n 和 m 的 F、$G \in \mathbb{F}[x]$，令 a_n 为 F 的首项系数。对于 $0 \le k \le \min(m,n)$，F 和 G 关于 x 的第 k 个子结式多项式定义为

$$S_k := \frac{c \begin{vmatrix} \boldsymbol{\alpha}_{1,n-k-1} G(\alpha_1) & \cdots & \boldsymbol{\alpha}_{n,n-k-1} G(\alpha_n) & \\ \boldsymbol{\alpha}_{1,k} & \cdots & \boldsymbol{\alpha}_{n,k} & \boldsymbol{x}_k \end{vmatrix}}{|\boldsymbol{V}(\boldsymbol{\alpha})|} \tag{2}$$

其中 $c = (-1)^k a_n^{m-k}$。更明确地说，

$$S_k = \frac{c \begin{vmatrix} \alpha_1^{n-k-1} G(\alpha_1) & \cdots & \alpha_n^{n-k-1} G(\alpha_n) & \\ \vdots & \ddots & \vdots & \\ \alpha_1^0 G(\alpha_1) & \cdots & \alpha_n^0 G(\alpha_n) & \\ \alpha_1^k & \cdots & \alpha_n^k & x^k \\ \vdots & \ddots & \vdots & \vdots \\ \alpha_1^0 & \cdots & \alpha_n^0 & x^0 \end{vmatrix}}{\begin{vmatrix} \alpha_1^{n-1} & \cdots & \alpha_n^{n-1} \\ \vdots & \ddots & \vdots \\ \alpha_1^0 & \cdots & \alpha_n^0 \end{vmatrix}}.$$

S_k 在 x^k中的系数，记作 s_k，称为关于 x的 F 和 G 的第 k个子结式。

Re标记5。(2)中 S_k 的表达式应作如下理解，否则当 S_k 不是无平方因子时，分母 -ina将会为零。

(1) 将 α_1，…，α_n 视为不定元并进行精确除法，得到一个关于 α_1，…，，α_n的对称多项式。
(2) 将 α_1，…，α_n 赋值为 F的根，对该多项式求值。

以下命题揭示了子结式多项式与 F 和 G 的最大公因式之间的内在联系，并在许多计算机代数基础算法中发挥着重要作用。

命题6。给定 F、$G \in \mathbb{F}[x]$，以下两个条件等价：

1. 最大公因式(F,G) 的次数 $= k$;
2. $s_0 = \cdots = s_{k-1} = 0 \wedge s_k \neq 0$。

此外，如果 deg 最大公因式$(F,G) = k$，则有

$$\gcd(F,G) = S_k.$$

3 主要结果

为了陈述本文的主定理，我们首先将行列式多项式从标准基下的形式推广到一般基下的形式。

定义 7（广义行列式多项式）。设 $\boldsymbol{\omega}=(\omega_s,..,\omega_1,\omega_0)^T$ 是 $\mathbb{F}_s[x]$ 和 $\boldsymbol{M}\in\mathbb{F}^{(s-k)\times s}$ 的一般基，其中 $k<s$。则与 $\boldsymbol{\omega}$ 相关联的 $\boldsymbol{M}$ 的行列式多项式定义为

$$\operatorname{detp}_{\boldsymbol{\omega}}\boldsymbol{M}:=\sum_{i=0}^{k}|\hat{\boldsymbol{M}}_i|\cdot\omega_i$$

其中，$\hat{}\ \boldsymbol{M}_i$ 是由 $\boldsymbol{M}$ 的前 $s-k-1$ 列和第$(s-i)$列组成的子矩阵。

定理 8（主要结果）。假设 $\boldsymbol{\omega}=(\omega_n,..,\omega_1,\omega_0)^T$是 $\mathbb{F}_n[x]$的一般基。令 F和 G 如式（1）所示，并令 $\boldsymbol{B}_{\boldsymbol{\omega},\,k}$ 为 F 和 G 在 $\boldsymbol{\omega}$ 中的 B´ézout 矩阵删去最后 k 行后得到的子矩阵。那么对于 $0\le k\le m$,

$$S_k=c_{\boldsymbol{\omega}}\cdot\operatorname{detp}_{\boldsymbol{\omega}}\boldsymbol{B}_{\boldsymbol{\omega},k}\tag{3}$$

其中

$$c_{\boldsymbol{\omega}}=(-1)^{\binom{n-k}{2}}a_n^{m-n}.$$

式（3）给出的行列式多项式为 S_k 提供了一个等价表达式，因此本文中的行列式多项式与命题6共享。

例9。令 $\boldsymbol{\nu}=(\nu_3,\nu_2,\nu_1,\nu_0)^T$为与 $\lambda=(1,0,2)$相关联的牛顿基，即

$$\nu_0=1,\quad \nu_1=x-2,\quad \nu_2=x(x-2),\quad \nu_3=x(x-1)(x-2).$$

给定

$$\begin{aligned}F(x)&=a_3\nu_3+a_2\nu_2+a_1\nu_1+a_0\nu_0,\\ G(x)&=b_2\nu_2+b_1\nu_1+b_0\nu_0,\end{aligned}$$

其中 $a_3b_2\neq0$，我们计算 F 和 G 关于 x 的第一子结式 S_1。要求将 S_1 表示在基 $\boldsymbol{\nu}$ 中。

根据定义 2，F 和 G 在 $\boldsymbol{\nu}$ 中的 B´ezout 矩阵为

$$\boldsymbol{B}_{\boldsymbol{\nu}}=\begin{bmatrix}a_3b_2 & a_3b_1 & a_3b_0\\ a_3b_1 & P_1 & P_2\\ a_3b_0 & P_2 & P_3\end{bmatrix}$$

其中

$$\begin{aligned}P_1&=a_3b_0-a_3b_1+a_2b_1-a_1b_2,\\ P_2&=a_2b_0-a_0b_2+a_3b_0,\\ P_3&=a_1b_0+2a_2b_0+2a_3b_0-a_0b_1-2a_0b_2.\end{aligned}$$

根据定理 8，F 和 G 在 $\boldsymbol{\nu}$ 中的第一子结式为

$$S_1=c_{\boldsymbol{\nu}}\cdot\left(\begin{vmatrix}a_3b_2 & a_3b_1\\ a_3b_1 & P_1\end{vmatrix}\nu_1+\begin{vmatrix}a_3b_2 & a_3b_0\\ a_3b_1 & P_2\end{vmatrix}\nu_0\right)\tag{4}$$

其中

$$c_{\boldsymbol{\nu}}=(-1)^{\binom{3-1}{2}}a_3^{2-3}=-a_3^{-1}.$$

将 (4) 展开可得

$$S_1 = \left(a_1 b_2^2 - a_2 b_1 b_2 - a_3 b_0 b_2 + a_3 b_1^2 + a_3 b_1 b_2\right) \nu_1 + \left(a_0 b_2^2 - a_2 b_0 b_2 + a_3 b_0 b_1 - a_3 b_0 b_2\right) \nu_0. \quad (5)$$

接下来我们将验证，将 S_1 转换为标准基中的表达式后，它与 F 和 G 的第一个子结式相同。

C将 F 和 G 转换为标准基 $\boldsymbol{x} = (x^3, x^2, x^1, x^0)^T$ 中的表达式，我们得到

$$\begin{aligned} F &= a_3 x^3 + (a_2 - 3a_3)\, x^2 + (a_1 - 2a_2 + 2a_3)\, x + (a_0 - 2a_1)\,, \\ G &= b_2 x^2 + (b_1 - 2b_2)\, x + b_0 - 2b_1. \end{aligned}$$

那么， x 在基 $\boldsymbol{x} = (x^3, x^2, x^1, x^0)^T$ 下关于 F和 G 的 B ´ezout 矩阵为

$$\boldsymbol{B} = \begin{bmatrix} a_3 b_2 & a_3 b_1 - 2a_3 b_2 & a_3 b_0 - 2a_3 b_1 \\ a_3 b_1 - 2a_3 b_2 & P_4 & P_5 \\ a_3 b_0 - 2a_3 b_1 & P_5 & P_6 \end{bmatrix}$$

其中

$$\begin{aligned} P_4 &= (a_2 b_1 - a_1 b_2) + a_3 b_0 - 5\, a_3 b_1 + 4\, a_3 b_2, \\ P_5 &= (a_2 b_0 - a_0 b_2) + 2(a_1 b_2 - a_2 b_1) - 3 a_3 b_0 + 6 a_3 b_1, \\ P_6 &= (a_1 b_0 - a_0 b_1) + 2(a_0 b_2 - a_2 b_0) + 4(a_2 b_1 - a_1 b_2) + 2 a_3 b_0 - 4 a_3 b_1. \end{aligned}$$

Thus

$$S_1 = c_{\boldsymbol{x}} \left(\begin{vmatrix} a_3 b_2 & a_3 b_1 - 2a_3 b_2 \\ a_3 b_1 - 2a_3 b_2 & P_4 \end{vmatrix} x^1 + \begin{vmatrix} a_3 b_2 & a_3 b_0 - 2a_3 b_1 \\ a_3 b_1 - 2a_3 b_2 & P_5 \end{vmatrix} x^0 \right) \quad (6)$$

其中再次有 $c_{\boldsymbol{x}} = -a_3^{-1}$。(6) 的展开式为

$$\begin{aligned} S_1 = &\left(a_1 b_2^2 - a_2 b_1 b_2 - a_3 b_0 b_2 + a_3 b_1^2 + a_3 b_1 b_2\right) x + \\ &\left(a_0 b_2^2 - 2\, a_1 b_2^2 - a_2 b_0 b_2 + 2\, a_2 b_1 b_2 + a_3 b_0 b_1 + a_3 b_0 b_2 - 2\, a_3 b_1^2 - 2\, a_3 b_1 b_2\right), \end{aligned}$$

这正是以标准基重新表述后（5）中的 S_1 。

4 主要结果的证明

在详细介绍证明之前，我们先简要概述证明思路。第一步，将以根表示的 S_k 从幂基转换为一般基。接着，将一般基中的 S_k 从关于根的多项式转换为关于系数的行列式。最后，我们证明关于系数的行列式可以写成定理 8 给出的广义行列式多项式。

4.1 将以根表示的 S_k 从标准基转换为一般基

显然，根据（2）定义的关于 x 的 F 和 G 的子结式 S_k 并不取决于 F 和 G 所表示时采用的基。然而，仔细观察（2）中的表达式可以发现，标准基实际上出现在 S_k 中。更具体地说， S_k 中行列式的元素具有 x^i $(0 \le i \le k)$ 的形式，或者是在 F 的根处对 x^i $(0 \le i \le k)$ 和 $x^i g(x)$（$0 \le i \le n-k-1$）进行求值。在这个意义上，我们可以说 S_k 是用标准基表示的。在本小节中，我们将把以标准基表示的关于根的 S_k 转换为一般基表示。为简单起见，我们引入以下记号。

记号 10。

- $\boldsymbol{\omega}(x) := (\omega_n, \ldots, \omega_1, \omega_0)^T$ *is a general basis of* $\mathbb{F}_n[x]$;
- $\boldsymbol{\omega}_j(x) := (\omega_j, \ldots, \omega_1, \omega_0)^T$ *for* $0 \le j < n$;
- $\boldsymbol{W}(\boldsymbol{\alpha}) := \begin{bmatrix} \omega_{n-1}(\alpha_1) & \cdots & \omega_{n-1}(\alpha_n) \\ \vdots & \ddots & \vdots \\ \omega_0(\alpha_1) & \cdots & \omega_0(\alpha_n) \end{bmatrix}$.

引理 11. 设 F、$G \in \mathbb{F}[x]$ 满足 deg $F = n$。则对于 $k \le n$，有

$$S_k = \frac{c \cdot \begin{vmatrix} \boldsymbol{\omega}_{n-k-1}(\alpha_1)G(\alpha_1) & \cdots & \boldsymbol{\omega}_{n-k-1}(\alpha_n)G(\alpha_n) \\ \boldsymbol{\omega}_k(\alpha_1) & \cdots & \boldsymbol{\omega}_k(\alpha_n) \quad \boldsymbol{\omega}_k \end{vmatrix}}{|\boldsymbol{W}(\boldsymbol{\alpha})|} \tag{7}$$

其中 c 与定义 4 中相同，即 $c = (-1)^k a_n^{m-k}$。

证明。我们将分别比较（2）和（7）中的分母与分子，并证明它们等价，从而证明该引理。证明稍长，因此我们将其分成若干步骤。

（i）证明（2）和（7）中的分母等价。

（a）设 $\boldsymbol{U}$ 为从 $\bar{\boldsymbol{x}} = (x^{n-1}, \ldots, x^0)^T$ 到 $\bar{\boldsymbol{\omega}} = (\omega_{n-1}, \ldots, \omega_0)^T$ 的过渡矩阵，即 $\bar{\boldsymbol{x}} = \boldsymbol{U}\bar{\boldsymbol{\omega}}$。

因此，对于 $i = 1, \ldots, n$, $\bar{\boldsymbol{x}}(\alpha_i) = \boldsymbol{U}\bar{\boldsymbol{\omega}}(\alpha_i)$。更明确地说，我们有

$$\boldsymbol{U} = \begin{bmatrix} 1 & \cdots & \cdot \\ & \ddots & \vdots \\ & & 1 \end{bmatrix}.$$

换言之，U 是一个单位上三角矩阵。

(b) 因此

$$\begin{aligned} \boldsymbol{V}(\boldsymbol{\alpha}) &= \begin{bmatrix} \bar{\boldsymbol{x}}(\alpha_1) & \cdots & \bar{\boldsymbol{x}}(\alpha_n) \end{bmatrix} \\ &= \begin{bmatrix} \boldsymbol{U}\bar{\boldsymbol{\omega}}(\alpha_1) & \cdots & \boldsymbol{U}\bar{\boldsymbol{\omega}}(\alpha_n) \end{bmatrix} \\ &= \boldsymbol{U} \begin{bmatrix} \bar{\boldsymbol{\omega}}(\alpha_1) & \cdots & \bar{\boldsymbol{\omega}}(\alpha_n) \end{bmatrix} \\ &= \boldsymbol{U}\boldsymbol{W}(\boldsymbol{\alpha}) \end{aligned}$$

(c) 对上述等式两边取行列式，得到 $|\boldsymbol{V}(\boldsymbol{\alpha})| = |\boldsymbol{U}| \cdot |\boldsymbol{W}(\boldsymbol{\alpha})|$.

(d) 由于 $\boldsymbol{U}$ 是单位上三角矩阵，$|\boldsymbol{U}| = 1$，这意味着

$$|\boldsymbol{V}(\boldsymbol{\alpha})| = |\boldsymbol{W}(\boldsymbol{\alpha})|. \tag{8}$$

(ii) 证明 (2) 和 (7) 中分子的等价性。

(a) 令 $\boldsymbol{U}_j$ 为从 $\boldsymbol{U}$ 中选取最后 j 行和最后 j 列得到的子矩阵。则 $\boldsymbol{U}_j$ 是从 $\mathbb{F}_{j-1}[x]$ 的基 $\boldsymbol{x}_{j-1}$ 到 $\boldsymbol{\omega}_{j-1}(x)$ 的过渡矩阵，即 $\boldsymbol{x}_{j-1}(x) = \boldsymbol{U}_j\boldsymbol{\omega}_{j-1}(x)$。

(b) 由此可得

$$\begin{aligned}&\left[\begin{array}{cccc}\boldsymbol{x}_k(\alpha_1) & \cdots & \boldsymbol{x}_k(\alpha_n) & \boldsymbol{x}_k\end{array}\right]\\=&\left[\begin{array}{cccc}\boldsymbol{U}_{k+1}\boldsymbol{\omega}_k(\alpha_1) & \cdots & \boldsymbol{U}_{k+1}\boldsymbol{\omega}_k(\alpha_n) & \boldsymbol{U}_{k+1}\boldsymbol{\omega}_k(x)\end{array}\right]\\=&\boldsymbol{U}_{k+1}\left[\begin{array}{cccc}\boldsymbol{\omega}_k(\alpha_1) & \cdots & \boldsymbol{\omega}_k(\alpha_n) & \boldsymbol{\omega}_k(x)\end{array}\right].\end{aligned}$$

(c) 以相同的方式，我们推导出以下结果:

$$\begin{aligned}&\left[\begin{array}{cccc}\boldsymbol{\alpha}_{1,n-k-1}G(\alpha_1) & \cdots & \boldsymbol{\alpha}_{n,n-k-1}G(\alpha_n)\end{array}\right]\\=&\boldsymbol{U}_{n-k}\left[\begin{array}{cccc}\boldsymbol{\omega}_{n-k-1}(\alpha_1)G(\alpha_1) & \cdots & \boldsymbol{\omega}_{n-k-1}(\alpha_n)G(\alpha_n) & \boldsymbol{0}_{(n-k)\times 1}\end{array}\right].\end{aligned}$$

(d) 将 (ii.b) 和 (ii.c) 中得到的表达式组合起来，我们得到

$$\begin{aligned}&\left[\begin{array}{cccc}\boldsymbol{\alpha}_{1,n-k-1}G(\alpha_1) & \cdots & \boldsymbol{\alpha}_{n,n-k-1}G(\alpha_n) & \\ \boldsymbol{\alpha}_{1,k} & \cdots & \boldsymbol{\alpha}_{n,k} & \boldsymbol{x}_k\end{array}\right]\\=&\left[\begin{array}{c}\boldsymbol{U}_{n-k}\left[\begin{array}{cccc}\boldsymbol{\omega}_{n-k-1}(\alpha_1)G(\alpha_1) & \cdots & \boldsymbol{\omega}_{n-k-1}(\alpha_n)G(\alpha_n) & \end{array}\right]\\ \boldsymbol{U}_{k+1}\left[\begin{array}{cccc}\boldsymbol{\omega}_k(\alpha_1) & \cdots & \boldsymbol{\omega}_k(\alpha_n) & \boldsymbol{\omega}_k(x)\end{array}\right]\end{array}\right]\\=&\begin{bmatrix}\boldsymbol{U}_{n-k} & \\ & \boldsymbol{U}_{k+1}\end{bmatrix}\cdot\left[\begin{array}{cccc}\boldsymbol{\omega}_{n-k-1}(\alpha_1)G(\alpha_1) & \cdots & \boldsymbol{\omega}_{n-k-1}(\alpha_n)G(\alpha_n) & \\ \boldsymbol{\omega}_k(\alpha_1) & \cdots & \boldsymbol{\omega}_k(\alpha_n) & \boldsymbol{\omega}_k(x)\end{array}\right].\end{aligned}$$

(e) 对两边取行列式，得到

$$\begin{aligned}&\left|\begin{array}{cccc}\boldsymbol{\alpha}_{1,n-k-1}G(\alpha_1) & \cdots & \boldsymbol{\alpha}_{n,n-k-1}G(\alpha_n) & \\ \boldsymbol{\alpha}_{1,k} & \cdots & \boldsymbol{\alpha}_{n,k} & \boldsymbol{x}_k\end{array}\right|\\=&\begin{vmatrix}\boldsymbol{U}_{n-k} & \\ & \boldsymbol{U}_{k+1}\end{vmatrix}\cdot\left|\begin{array}{cccc}\boldsymbol{\omega}_{n-k-1}(\alpha_1)G(\alpha_1) & \cdots & \boldsymbol{\omega}_{n-k-1}(\alpha_n)G(\alpha_n) & \\ \boldsymbol{\omega}_k(\alpha_1) & \cdots & \boldsymbol{\omega}_k(\alpha_n) & \boldsymbol{\omega}_k(x)\end{array}\right|.\end{aligned}$$

(f) 由于 $\boldsymbol{U}$ 是单位上三角矩阵， $\boldsymbol{U}_{n-k}$ 和 $\boldsymbol{U}_{k+1}$ 也都是。因此 $|\boldsymbol{U}_{n-k}|=|\boldsymbol{U}_{k+1}|=1$，这意味着

$$\begin{aligned}&\left|\begin{array}{cccc}\boldsymbol{\alpha}_{1,n-k-1}G(\alpha_1) & \cdots & \boldsymbol{\alpha}_{n,n-k-1}G(\alpha_n) & \\ \boldsymbol{\alpha}_{1,k} & \cdots & \boldsymbol{\alpha}_{n,k} & \boldsymbol{x}_k\end{array}\right|\\=&\left|\begin{array}{cccc}\boldsymbol{\omega}_{n-k-1}(\alpha_1)G(\alpha_1) & \cdots & \boldsymbol{\omega}_{n-k-1}(\alpha_n)G(\alpha_n) & \\ \boldsymbol{\omega}_k(\alpha_1) & \cdots & \boldsymbol{\omega}_k(\alpha_n) & \boldsymbol{\omega}_k(x)\end{array}\right|.\end{aligned}\tag{9}$$

(iii) 结合 (8) 和 (9)，我们得到

$$S_k=\frac{c\cdot\left|\begin{array}{cccc}\boldsymbol{\omega}_{n-k-1}(\alpha_1)G(\alpha_1) & \cdots & \boldsymbol{\omega}_{n-k-1}(\alpha_n)G(\alpha_n) & \\ \boldsymbol{\omega}_k(\alpha_1) & \cdots & \boldsymbol{\omega}_k(\alpha_n) & \boldsymbol{\omega}_k(x)\end{array}\right|}{|\boldsymbol{W}(\boldsymbol{\alpha})|}$$

其中 $c=(-1)^k a_n^{m-k}$。

□

注12。 S_k 在（7）中的表达式应按照注5所述的相同方式理解，否则当 F 不是无平方因子时，分母将变为零。

4.2 将一般基中的 S_k 从根的表达式转换为系数的表达式

下面的引理 13 使我们能够将 S_k 根的表达式转换为用一般基表示的输入多项式系数的表达式。它推广了 Li 针对标准基下的子结式多项式 [24]所提出的思想。

引理 13. 给定 $\mathbb{F}_n[x]$ 的一般基 $\boldsymbol{\omega}=(\omega_n,\ldots,\omega_1,\omega_0)^T$，以及如 (1) 中的 F, G，令 $\boldsymbol{B}_{\boldsymbol{\omega}}$ 为 F 和 G 关于 $\boldsymbol{\omega}$ 中的 x 的 B ´ézout 矩阵，且令 $_k$, $_k$ 为从 $\boldsymbol{B}_{\boldsymbol{\omega}}$ 中删去最后 k 行得到的子矩阵。那么

$$S_k = c_{\boldsymbol{\omega}} \cdot \begin{vmatrix} \boldsymbol{B}_{\boldsymbol{\omega},k} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{vmatrix}$$

其中

- $c_{\boldsymbol{\omega}} = (-1)^{\binom{n-k}{2}} a_n^{m-n}$,
- *and*

$$\boldsymbol{X}_{\boldsymbol{\omega},k} = \begin{bmatrix} -1 & & \omega_k/\omega_0 \\ & \ddots & \vdots \\ & -1 & \omega_1/\omega_0 \end{bmatrix}_{k\times n}. \tag{10}$$

在证明引理 13 之前，我们需要先验证以下引理 14 和引理 15，它们概括了引理 13 的关键要素。

引理 14. 给定如 (1) 中的 F, G，其中 $\boldsymbol{\omega}=(\omega_n,\ldots,\omega_1,\omega_0)^T$ 是 $\mathbb{F}_n[x]$ 的一般基，令

- $\boldsymbol{B}_{\boldsymbol{\omega}}$ 为 F 和 G 关于 $\boldsymbol{\omega}$ 中的 x 的 B ´ézout 矩阵,
- $\bar{\boldsymbol{\omega}}=(\omega_{n-1},\ldots,\omega_1,\omega_0)^T$，并且
- $\alpha_1,\ldots,\alpha_n$ 是 F在 $\overline{\mathbb{F}}$上的 n 根。

Then

$$\boldsymbol{B}_{\boldsymbol{\omega}} \cdot \begin{bmatrix} \bar{\boldsymbol{\omega}}(\alpha_1) & \cdots & \bar{\boldsymbol{\omega}}(\alpha_n) \end{bmatrix} = a_n \boldsymbol{U}^T \boldsymbol{T} \boldsymbol{U} \begin{bmatrix} \bar{\boldsymbol{\omega}}(\alpha_1) G(\alpha_1) & \cdots & \bar{\boldsymbol{\omega}}(\alpha_n) G(\alpha_n) \end{bmatrix}$$

其中， $\boldsymbol{U}$ 是从 $\bar{\boldsymbol{x}}$到 $\bar{\boldsymbol{\omega}}$ 的过渡矩阵，并且

$$\boldsymbol{T} = \begin{bmatrix} & & & (-1)^0 e_0 \\ & & (-1)^2 e_0 & (-1)^1 e_1 \\ & \iddots & \vdots & \vdots \\ (-1)^{2(n-1)} e_0 & \cdots & \cdots & (-1)^{n-1} e_{n-1} \end{bmatrix}.$$

证明。证明过程较长，将分为几个步骤。

(i) 令

$$C(x,y) = \frac{\begin{vmatrix} F(x) & F(y) \\ G(x) & G(y) \end{vmatrix}}{x-y}. \tag{11}$$

根据定义 2， $\boldsymbol{B}_{\boldsymbol{\omega}}$ 满足

$$C(x,y) = \bar{\boldsymbol{\omega}}(x)^T \cdot \boldsymbol{B}_{\boldsymbol{\omega}} \cdot \bar{\boldsymbol{\omega}}(y) \tag{12}$$

（ii）由于对于 $i=1$，……，n，$F(\alpha_i)=0$，将 $y=\alpha_i$ 代入（12），可得

$$C(x,\alpha_i)=\bar{\boldsymbol{\omega}}(x)^T\cdot\boldsymbol{B}_{\boldsymbol{\omega}}\cdot\bar{\boldsymbol{\omega}}(\alpha_i). \tag{13}$$

(iii) 另一方面，由（11）可得

$$C\left(x,\alpha_i\right)=\frac{F\left(x\right)G\left(\alpha_i\right)}{x-\alpha_i}=a_n\prod_{\substack{j=1\\ j\neq i}}^{n}\left(x-\alpha_j\right)G\left(\alpha_i\right).$$

(iv) 令 $e_j^{(i)}$ 表示 $\alpha_1,\ldots,\alpha_{i-1},\alpha_{i+1},\ldots,\alpha_n$ 中的第 j 个初等对称多项式[1]（其中 $e_0^{(i)}:=1$）。那么

$$\begin{aligned}C\left(x,\alpha_i\right)&=a_n\left(\sum_{j=0}^{n-1}(-1)^j e_j^{(i)}x^{n-1-j}\right)G(\alpha_i)\\&=a_n\begin{bmatrix}x^{n-1}&\cdots&x^0\end{bmatrix}\begin{bmatrix}(-1)^0e_0^{(i)}\\ \vdots\\ (-1)^{n-1}e_{n-1}^{(i)}\end{bmatrix}G(\alpha_i)\\&=a_n\bar{\boldsymbol{x}}^T\begin{bmatrix}(-1)^0e_0^{(i)}\\ \vdots\\ (-1)^{n-1}e_{n-1}^{(i)}\end{bmatrix}G(\alpha_i).\end{aligned}$$

(v) 由于 $\bar{\boldsymbol{x}}=\boldsymbol{U}\bar{\boldsymbol{\omega}}$，我们有

$$C\left(x,\alpha_i\right)=a_n\bar{\boldsymbol{\omega}}^T\boldsymbol{U}^T\begin{bmatrix}(-1)^0e_0^{(i)}\\ \vdots\\ (-1)^{n-1}e_{n-1}^{(i)}\end{bmatrix}G(\alpha_i)=a_n\bar{\boldsymbol{\omega}}^T\boldsymbol{U}^T\begin{bmatrix}(-1)^0e_0^{(i)}G(\alpha_i)\\ \vdots\\ (-1)^{n-1}e_{n-1}^{(i)}G(\alpha_i)\end{bmatrix}. \tag{14}$$

(vi) 比较（13）和（14）中 $C(x,\alpha_i)$ 的系数，我们得到

$$\boldsymbol{B}_{\boldsymbol{\omega}}\bar{\boldsymbol{\omega}}(\alpha_i)=a_n\boldsymbol{U}^T\begin{bmatrix}e_0^{(i)}G(\alpha_i)\\ \vdots\\ (-1)^{n-1}e_{n-1}^{(i)}G(\alpha_i)\end{bmatrix}.$$

(vii) 将 $\boldsymbol{B}_{\boldsymbol{\omega}}\bar{\boldsymbol{\omega}}(\alpha_i)$（$i=1,\ldots,n$）水平排列成一个矩阵，我们得到

$$\begin{aligned}&\begin{bmatrix}\boldsymbol{B}_{\boldsymbol{\omega}}\bar{\boldsymbol{\omega}}(\alpha_1)&\cdots&\boldsymbol{B}_{\boldsymbol{\omega}}\bar{\boldsymbol{\omega}}(\alpha_n)\end{bmatrix}\\&=\begin{bmatrix}a_n\boldsymbol{U}^T\begin{bmatrix}e_0^{(1)}G(\alpha_1)\\ \vdots\\ (-1)^{n-1}e_{n-1}^{(1)}G(\alpha_1)\end{bmatrix}&\cdots&a_n\boldsymbol{U}^T\begin{bmatrix}e_0^{(n)}G(\alpha_n)\\ \vdots\\ (-1)^{n-1}e_{n-1}^{(n)}G(\alpha_n)\end{bmatrix}\end{bmatrix}\end{aligned}$$

[1] 第 k 个初等对称多项式（变量为 $x_1,x_2,\ldots,x_n$）定义为 $\sigma_k=\sum_{1\le i_1<\cdots<i_k\le n}x_{i_1}\cdots x_{i_k}$。$\{i_1,\ldots,i_k\}\subset\{1,\ldots,n\}$

$$
\begin{aligned}
=&a_n\boldsymbol{U}^T\begin{bmatrix}(-1)^0e_0^{(1)}G(\alpha_1) & \cdots & (-1)^0e_0^{(n)}G(\alpha_n)\\ \vdots & \ddots & \vdots\\ (-1)^{n-1}e_{n-1}^{(1)}G(\alpha_1) & \cdots & (-1)^{n-1}e_{n-1}^{(n)}G(\alpha_n)\end{bmatrix}\\
=&a_n\boldsymbol{U}^T\begin{bmatrix}(-1)^0e_0^{(1)} & \cdots & (-1)^0e_0^{(n)}\\ \vdots & \ddots & \vdots\\ (-1)^{n-1}e_{n-1}^{(1)} & \cdots & (-1)^{n-1}e_{n-1}^{(n)}\end{bmatrix}\begin{bmatrix}G(\alpha_1) & & \\ & \ddots & \\ & & G(\alpha_n)\end{bmatrix}\\
=&a_n\boldsymbol{U}^T\begin{bmatrix}(-1)^0 & & \\ & \ddots & \\ & & (-1)^{n-1}\end{bmatrix}\begin{bmatrix}e_0^{(1)} & \cdots & e_0^{(n)}\\ \vdots & \ddots & \vdots\\ e_{n-1}^{(1)} & \cdots & e_{n-1}^{(n)}\end{bmatrix}\begin{bmatrix}G(\alpha_1) & & \\ & \ddots & \\ & & G(\alpha_n)\end{bmatrix}. \qquad (15)
\end{aligned}
$$

(viii) 回顾 [21, 引理 35], 其指出了这一点。

$$
e_j^{(i)}=\sum_{k=0}^{j}(-1)^k e_{j-k}\alpha_i^k=\begin{bmatrix}0\cdots 0 & (-1)^j e_0\cdots(-1)^0e_j\end{bmatrix}\bar{\boldsymbol{x}}(\alpha_i)
$$

其中 e_j 表示 $\alpha_1,\ldots,\alpha_n$ 中的第 j 个初等对称多项式（其中 $e_0:=1$）.
因此,

$$
\begin{aligned}
&\begin{bmatrix}(-1)^0 & & \\ & \ddots & \\ & & (-1)^{n-1}\end{bmatrix}\begin{bmatrix}e_0^{(1)} & \cdots & e_0^{(n)}\\ \vdots & \ddots & \vdots\\ e_{n-1}^{(1)} & \cdots & e_{n-1}^{(n)}\end{bmatrix}\\
=&\begin{bmatrix}(-1)^0 & & \\ & \ddots & \\ & & (-1)^{n-1}\end{bmatrix}\begin{bmatrix}& & & (-1)^0e_0\\ & & (-1)^1e_0 & (-1)^0e_1\\ & \iddots & \vdots & \vdots\\ (-1)^{n-1}e_0 & \cdots & \cdots & (-1)^0e_{n-1}\end{bmatrix}\cdot\begin{bmatrix}\bar{\boldsymbol{x}}(\alpha_1)\cdots\bar{\boldsymbol{x}}(\alpha_n)\end{bmatrix}\\
=&\boldsymbol{T}\begin{bmatrix}\bar{\boldsymbol{x}}(\alpha_1) & \cdots & \bar{\boldsymbol{x}}(\alpha_n)\end{bmatrix} \qquad (16)
\end{aligned}
$$

其中

$$
\boldsymbol{T}=\begin{bmatrix}& & & (-1)^0e_0\\ & & (-1)^2e_0 & (-1)^1e_1\\ & \iddots & \vdots & \vdots\\ (-1)^{2(n-1)}e_0 & \cdots & \cdots & (-1)^{n-1}e_{n-1}\end{bmatrix}.
$$

(ix) 将 (16) 代入 (15) 立即得到

$$
\begin{aligned}
&\boldsymbol{B}_{\boldsymbol{\omega}}\begin{bmatrix}\bar{\boldsymbol{\omega}}(\alpha_1) & \cdots & \bar{\boldsymbol{\omega}}(\alpha_n)\end{bmatrix}\\
=&\begin{bmatrix}\boldsymbol{B}_{\boldsymbol{\omega}}\bar{\boldsymbol{\omega}}(\alpha_1) & \cdots & \boldsymbol{B}_{\boldsymbol{\omega}}\bar{\boldsymbol{\omega}}(\alpha_n)\end{bmatrix}\\
=&a_n\boldsymbol{U}^T\boldsymbol{T}\begin{bmatrix}\bar{\boldsymbol{x}}(\alpha_1) & \cdots & \bar{\boldsymbol{x}}(\alpha_n)\end{bmatrix}\begin{bmatrix}G(\alpha_1) & & \\ & \ddots & \\ & & G(\alpha_n)\end{bmatrix}\\
=&a_n\boldsymbol{U}^T\boldsymbol{T}\begin{bmatrix}\bar{\boldsymbol{x}}(\alpha_1)G(\alpha_1) & \cdots & \bar{\boldsymbol{x}}(\alpha_n)G(\alpha_n)\end{bmatrix}\\
=&a_n\boldsymbol{U}^T\boldsymbol{T}\boldsymbol{U}\begin{bmatrix}\bar{\boldsymbol{\omega}}(\alpha_1)G(\alpha_1) & \cdots & \bar{\boldsymbol{\omega}}(\alpha_n)G(\alpha_n)\end{bmatrix}.
\end{aligned}
$$

□

引理 15. 设 $\boldsymbol{M} \in \mathbb{F}_{(n-k)\times n}$ with $k < n$ and $\bar{\boldsymbol{\omega}} = (\omega_{n-1}, \ldots, \omega_1, \omega_0)^T$ 是 $\mathbb{F}_{n-1}[x]$ 的一般基。给定 $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n) \in \overline{\mathbb{F}}^n$，我们有

$$\left| \begin{array}{c} \boldsymbol{M} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{array} \right| = \frac{(-1)^k \left| \begin{array}{ccc|c} & \boldsymbol{MW}(\boldsymbol{\beta}) & & \\ \hline \boldsymbol{\omega}_k(\beta_1) & \cdots & \boldsymbol{\omega}_k(\beta_n) & \boldsymbol{\omega}_k \end{array} \right|}{|\boldsymbol{W}(\boldsymbol{\beta})|} \tag{17}$$

其中 $\boldsymbol{W}(\boldsymbol{\beta}) = \left[\bar{\boldsymbol{\omega}}(\beta_1) \cdots \bar{\boldsymbol{\omega}}(\beta_n)\right]$ 和 $\boldsymbol{\omega}_k = (\omega_k, \ldots, \omega_1, \omega_0)^T$。

证明。我们先回顾以下事实:

$$\left| \begin{array}{c} \boldsymbol{M} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{array} \right| \cdot |\boldsymbol{W}(\boldsymbol{\beta})| = \left| \begin{array}{c} M\boldsymbol{W}(\boldsymbol{\beta}) \\ \boldsymbol{X}_{\boldsymbol{\omega},k}\boldsymbol{W}(\boldsymbol{\beta}) \end{array} \right|.$$

Th然后我们考虑下方的矩阵乘积，并进行如下乘法

$$\begin{aligned} \boldsymbol{X}_{\boldsymbol{\omega},k}\boldsymbol{W}(\boldsymbol{\beta}) &= \begin{bmatrix} -1 & & \omega_k \\ & \ddots & \vdots \\ & -1 & \omega_1 \end{bmatrix} \begin{bmatrix} \omega_{n-1}(\beta_1) & \cdots & \omega_{n-1}(\beta_n) \\ \vdots & \ddots & \vdots \\ \omega_0(\beta_1) & \cdots & \omega_0(\beta_n) \end{bmatrix} \\ &= \begin{bmatrix} \omega_k\omega_0(\beta_1) - \omega_k(\beta_1) & \cdots & \omega_k\omega_0(\beta_n) - \omega_k(\beta_n) \\ \vdots & \ddots & \vdots \\ \omega_1\omega_0(\beta_1) - \omega_1(\beta_1) & \cdots & \omega_1\omega_0(\beta_n) - \omega_1(\beta_n) \end{bmatrix}. \end{aligned}$$

对等式两边取行列式，得到

$$\begin{aligned} &\left| \begin{array}{c} \boldsymbol{M} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{array} \right| \cdot |\boldsymbol{W}(\boldsymbol{\beta})| \\ &= \left| \begin{array}{ccc} & \boldsymbol{MW}(\boldsymbol{\beta}) & \\ \hline \omega_k\omega_0(\beta_1) - \omega_k(\beta_1) & \cdots & \omega_k\omega_0(\beta_n) - \omega_k(\beta_n) \\ \vdots & \ddots & \vdots \\ \omega_1\omega_0(\beta_1) - \omega_1(\beta_1) & \cdots & \omega_1\omega_0(\beta_n) - \omega_1(\beta_n) \end{array} \right| \\ &= \left| \begin{array}{ccc|c} & \boldsymbol{MW}(\boldsymbol{\beta}) & & \\ \hline \omega_k\omega_0(\beta_1) - \omega_k(\beta_1) & \cdots & \omega_k\omega_0(\beta_n) - \omega_k(\beta_n) & \\ \vdots & \ddots & \vdots & \\ \omega_1\omega_0(\beta_1) - \omega_1(\beta_1) & \cdots & \omega_1\omega_0(\beta_n) - \omega_1(\beta_n) & \\ \omega_0(\beta_1) & \cdots & \omega_0(\beta_n) & 1 \end{array} \right|. \end{aligned}$$

将第 $(n-i+1)$ 行减去第 $(n+1)$ 行乘以 ω_i，其中 $i = 1, \ldots, k$，得到

$$\left| \begin{array}{c} \boldsymbol{M} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{array} \right| \cdot |\boldsymbol{W}(\boldsymbol{\beta})| = \left| \begin{array}{ccc|c} & \boldsymbol{MW}(\boldsymbol{\beta}) & & \\ \hline -\omega_k(\beta_1) & \cdots & -\omega_k(\beta_n) & -\omega_k \\ \vdots & \ddots & \vdots & \vdots \\ -\omega_1(\beta_1) & \cdots & -\omega_1(\beta_n) & -\omega_1 \\ \omega_0(\beta_1) & \cdots & \omega_0(\beta_n) & 1 \end{array} \right|.$$

将最后 $k+1$ 行（最后一行除外）中的 -1 提取出来，并令最后一列中的 1 为 ω_0，即可得到：

$$\begin{vmatrix} \boldsymbol{M} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{vmatrix} \cdot |\boldsymbol{W}(\boldsymbol{\beta})| = (-1)^k \left| \begin{array}{ccc|c} \boldsymbol{M}\boldsymbol{W}(\boldsymbol{\beta}) & & & \\ \hline \boldsymbol{\omega}_k(\beta_1) & \cdots & \boldsymbol{\omega}_k(\beta_n) & \boldsymbol{\omega}_k \end{array} \right|$$

这等价于我们想要的结果。 □

注释 16. 右侧 (17) 中的表达式应按照注5中 S_k 的表达式的解释方式来理解：

(1) 将 $\beta_1, \ldots, \beta_n$ 视为不定元并进行精确除法，结果得到一个关于 $\beta_1, \ldots, , \beta_n$ 的对称多项式。

(2) 将 $\beta_1, \ldots, \beta_n$ 赋予 $\mathbb{F}$ 中的一些特定值，对该多项式求值。

否则，当 $\beta_i = \beta_j$ 取某个 $i \neq j$ 时，分母将为零。

现在我们可以证明引理 13 了。

证明。证明过程稍长，将分为几个步骤。

(i) 将 $\boldsymbol{M}$ 和 $\boldsymbol{\beta}$ 特化为 $\boldsymbol{B}_{\boldsymbol{\omega},\,k}$ 和 $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$，其中 α_i 是 F 在 $\overline{\mathbb{F}}$ 上的根，我们得到

$$\begin{vmatrix} \boldsymbol{B}_{\boldsymbol{\omega},k} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{vmatrix} \cdot |\boldsymbol{W}(\boldsymbol{\alpha})| = (-1)^k \left| \begin{array}{ccc|c} \boldsymbol{B}_{\boldsymbol{\omega},k}\boldsymbol{W}(\boldsymbol{\alpha}) & & & \\ \hline \boldsymbol{\omega}_k(\alpha_1) & \cdots & \boldsymbol{\omega}_k(\alpha_n) & \boldsymbol{\omega}_k \end{array} \right|. \tag{18}$$

(ii) 接下来，我们继续化简 $\boldsymbol{B}_{\boldsymbol{\omega},\,k}\boldsymbol{W}(\boldsymbol{\alpha})$。

(a) 由于 $\boldsymbol{B}_{\boldsymbol{\omega},\,k} = \begin{bmatrix} \boldsymbol{I}_{n-k} & \boldsymbol{0}_{(n-k)\times k} \end{bmatrix} \boldsymbol{B}_{\boldsymbol{\omega}}$，其中 $\boldsymbol{I}_{n-k}$ 是 $n-k$ 阶单位矩阵，根据引理 14,

$$\begin{aligned} \boldsymbol{B}_{\boldsymbol{\omega},k}\boldsymbol{W}(\boldsymbol{\alpha}) &= \begin{bmatrix} \boldsymbol{I}_{n-k} & \boldsymbol{0}_{(n-k)\times k} \end{bmatrix} \boldsymbol{B}_{\boldsymbol{\omega}}\boldsymbol{W}(\boldsymbol{\alpha}) \\ &= a_n \begin{bmatrix} \boldsymbol{I}_{n-k} & \boldsymbol{0}_{(n-k)\times k} \end{bmatrix} \boldsymbol{U}^T\boldsymbol{T}\boldsymbol{U} \cdot \begin{bmatrix} \bar{\boldsymbol{\omega}}(\alpha_1)G(\alpha_1) & \cdots & \bar{\boldsymbol{\omega}}(\alpha_n)G(\alpha_n) \end{bmatrix}. \end{aligned}$$

(b) 注意，$\boldsymbol{U}$ 是单位上三角矩阵，因此 $\boldsymbol{U}^T$ 是单位下三角矩阵。此外，$\boldsymbol{T}$ 是单位反下三角矩阵。因此，我们可以按以下方式将它们分块：

$$\boldsymbol{U} = \begin{bmatrix} \boldsymbol{U}_1 & * \\ & * \end{bmatrix}, \quad \boldsymbol{U}^T = \begin{bmatrix} * & \\ * & \boldsymbol{U}_2 \end{bmatrix}, \quad \boldsymbol{T} = \begin{bmatrix} & \boldsymbol{T}_1 \\ * & * \end{bmatrix}, \tag{19}$$

其中 $\boldsymbol{U}_1$、$\boldsymbol{U}_2$、$\boldsymbol{T}_1 \in \mathbb{F}^{(n-k)\times(n-k)}$。由此可得

$$\begin{aligned} & \begin{bmatrix} \boldsymbol{I}_{n-k} & \boldsymbol{0}_{(n-k)\times k} \end{bmatrix} \boldsymbol{U}^T\boldsymbol{T}\boldsymbol{U} \\ = & \begin{bmatrix} \boldsymbol{I}_{n-k} & \boldsymbol{0}_{(n-k)\times k} \end{bmatrix} \begin{bmatrix} * & \\ * & \boldsymbol{U}_2 \end{bmatrix} \begin{bmatrix} & \boldsymbol{T}_1 \\ * & * \end{bmatrix} \begin{bmatrix} \boldsymbol{U}_1 & * \\ & * \end{bmatrix} \\ = & \begin{bmatrix} \boldsymbol{0}_{(n-k)\times k} & \boldsymbol{U}_2\boldsymbol{T}_1\boldsymbol{U}_1 \end{bmatrix}. \end{aligned}$$

(c) 因此，

$$\boldsymbol{B}_{\boldsymbol{\omega},k}\boldsymbol{\omega}(\boldsymbol{\alpha}) = a_n \begin{bmatrix} \boldsymbol{0}_{(n-k)\times k} & \boldsymbol{U}_2\boldsymbol{T}_1\boldsymbol{U}_1 \end{bmatrix} \cdot \begin{bmatrix} \bar{\boldsymbol{\omega}}(\alpha_1)G(\alpha_1) & \cdots & \bar{\boldsymbol{\omega}}(\alpha_n)G(\alpha_n) \end{bmatrix}.$$

(d) 现在我们将矩阵分块

$$\left[\bar{\boldsymbol{\omega}}(\alpha_1)G(\alpha_1)\ \cdots\ \bar{\boldsymbol{\omega}}(\alpha_n)G(\alpha_n)\right]$$

分成两个块，其中上块由 k 行组成，下块由 $(n-k)$ 行组成。完成矩阵乘法后，我们得到

$$\boldsymbol{B}_{\boldsymbol{\omega},k}\boldsymbol{W}(\boldsymbol{\alpha}) = a_n\boldsymbol{U}_2\boldsymbol{T}_1\boldsymbol{U}_1 \cdot \left[\boldsymbol{\omega}_{n-k-1}(\alpha_1)G(\alpha_1)\cdots\boldsymbol{\omega}_{n-k-1}(\alpha_n)G(\alpha_n)\right]$$

（e）因此，

$$\left[\begin{array}{ccc|c} & \boldsymbol{B}_{\boldsymbol{\omega},k}\boldsymbol{W}(\boldsymbol{\alpha}) & & \\ \hline \boldsymbol{\omega}_k(\alpha_1) & \cdots & \boldsymbol{\omega}_k(\alpha_n) & \boldsymbol{\omega}_k \end{array}\right]$$

$$= \begin{bmatrix} a_n\boldsymbol{U}_2\boldsymbol{T}_1\boldsymbol{U}_1 & \\ & \boldsymbol{I}_{k+1} \end{bmatrix} \cdot \left[\begin{array}{ccc|c} \boldsymbol{\omega}_{n-k-1}(\alpha_1)G(\alpha_1) & \cdots & \boldsymbol{\omega}_{n-k-1}(\alpha_n)G(\alpha_n) & \\ \hline \boldsymbol{\omega}_k(\alpha_1) & \cdots & \boldsymbol{\omega}_k(\alpha_n) & \boldsymbol{\omega}_k \end{array}\right]$$

其中，$\boldsymbol{I}_{k+1}$ 是 $k+1$ 阶单位矩阵。

（iii）当前步骤旨在计算上述矩阵的行列式，该行列式与引理 11 中的 S_k 密切相关。

（a）回顾引理 11，并将其转换为

$$S_k = c \cdot \begin{vmatrix} \boldsymbol{\omega}_{n-k-1}(\alpha_1)G(\alpha_1)\cdots\boldsymbol{\omega}_{n-k-1}(\alpha_n)G(\alpha_n) & \\ \boldsymbol{\omega}_k(\alpha_1) \quad\quad \cdots\boldsymbol{\omega}_k(\alpha_n) & \boldsymbol{\omega}_k \end{vmatrix} / |\boldsymbol{W}(\boldsymbol{\alpha})|$$

（b）根据（ii.e），

$$\begin{vmatrix} \boldsymbol{\omega}_{n-k-1}(\alpha_1)G(\alpha_1)\cdots\boldsymbol{\omega}_{n-k-1}(\alpha_n)G(\alpha_n) & \\ \boldsymbol{\omega}_k(\alpha_1) \quad\quad \cdots\boldsymbol{\omega}_k(\alpha_n) & \boldsymbol{\omega}_k \end{vmatrix} = \frac{\left|\begin{array}{ccc|c} & \boldsymbol{B}_{\boldsymbol{\omega},k}\boldsymbol{W}(\boldsymbol{\alpha}) & & \\ \hline \boldsymbol{\omega}_k(\alpha_1) & \cdots & \boldsymbol{\omega}_k(\alpha_n) & \boldsymbol{\omega}_k \end{array}\right|}{\begin{vmatrix} a_n\boldsymbol{U}_2\boldsymbol{T}_1\boldsymbol{U}_1 & \\ & \boldsymbol{I}_{k+1} \end{vmatrix}}$$

(c) 将引理 15 中的 M 和 $\boldsymbol{\beta}$ 分别用 $\boldsymbol{B}_{\boldsymbol{\omega},k}$ 和 $\boldsymbol{\alpha}$ 进行特化，我们得到

$$\left|\begin{array}{ccc|c} & \boldsymbol{B}_{\boldsymbol{\omega},k}\boldsymbol{W}(\boldsymbol{\alpha}) & & \\ \hline \boldsymbol{\omega}_k(\alpha_1) & \cdots & \boldsymbol{\omega}_k(\alpha_n) & \boldsymbol{\omega}_k \end{array}\right| = (-1)^k \left|\begin{array}{c} \boldsymbol{B}_{\boldsymbol{\omega},k} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{array}\right| |\boldsymbol{W}(\boldsymbol{\alpha})|.$$

(d) 综合 (iii.a)–(iii.c)，即可得到

$$S_k = \frac{c}{(-1)^k|a_n\boldsymbol{U}_2\boldsymbol{T}_1\boldsymbol{U}_1|} \cdot \left|\begin{array}{c} \boldsymbol{B}_{\boldsymbol{\omega},k} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{array}\right|.$$

(iv) 在最后一步中，我们将求出上面所得行列式前面的系数。

(a) 回顾一下，$\boldsymbol{U}$ 是单位上三角，$\boldsymbol{T}$ 是单位反向上三角。因此，$\boldsymbol{U}_1$ 和 $\boldsymbol{U}_2$ 都是单位上三角，而 $\boldsymbol{T}_1$ 是单位反下三角。此外，这三个矩阵的阶数都是 $n-k$。因此，

$$|a_n\boldsymbol{U}_2\boldsymbol{T}_1\boldsymbol{U}_1| = a_n^{n-k}|\boldsymbol{U}_2| \cdot |\boldsymbol{T}_1| \cdot |\boldsymbol{U}_1| = a_n^{n-k} \cdot (-1)^{\sum_{i=1}^{n-k}(i+1)} = (-1)^{\binom{n-k}{2}} \cdot a_n^{n-k},$$

这表明

$$S_k = (-1)^{k+\binom{n-k}{2}} c a_n^{k-n} \left|\begin{array}{c} \boldsymbol{B}_{\boldsymbol{\omega},k} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{array}\right|.$$

(b) 我们继续化简下方等式中的常数因子。

$$(-1)^{k+\binom{n-k}{2}} c a_n^{k-n} = (-1)^{k+\binom{n-k}{2}} \cdot (-1)^k a_n^{m-k} a_n^{k-n} = (-1)^{\binom{n-k}{2}} a_n^{m-n}.$$

(c) 总之，我们有

$$S_k = (-1)^{\binom{n-k}{2}} a_n^{m-n} \cdot \begin{vmatrix} \boldsymbol{B}_{\boldsymbol{\omega},k} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{vmatrix}.$$

□

4.3 将一般基中的 S_k 从单个行列式转换为行列式多项式

在本小节中，我们证明一个比所需结果更一般的结论。提出这个更一般的结论，是希望它在其他场合也能派上用场。

引理 17. 给定 $\boldsymbol{\omega} = (\omega_n, \ldots, \omega_1, \omega_0)^T$，它是 $\mathbb{F}_n[x]$ 的一般基，且 $\boldsymbol{M} \in \mathbb{F}^{(n-k)\times n}$，其中 $k < n$，令 $\boldsymbol{X}_{\boldsymbol{\omega},\,k}$ 如 (10) 中所示。则

$$\operatorname{detp}_{\boldsymbol{\omega}} \boldsymbol{M} = \begin{vmatrix} \boldsymbol{M} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{vmatrix}.$$

证明. 记 $\boldsymbol{M}$ 的第 i 列为 $\boldsymbol{M}_i$。则

$$\begin{vmatrix} \boldsymbol{M} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{vmatrix} = \begin{vmatrix} \boldsymbol{M}_1 & \cdots & \boldsymbol{M}_{n-k} & \cdots & \cdots & \boldsymbol{M}_n \\ & & -1 & & & \omega_k \\ & & & \ddots & & \vdots \\ & & & & -1 & \omega_1 \end{vmatrix}$$

将第 $(n-i)$ 列乘以 ω_i，对 $i = 1, \ldots, k$，再加到最后一列，得到

$$\begin{vmatrix} \boldsymbol{M} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{vmatrix} = \begin{vmatrix} \boldsymbol{M}_1 & \cdots & \boldsymbol{M}_{n-k} & \cdots & \cdots & \sum_{i=1}^{k} \boldsymbol{M}_{n-i}\omega_i + \boldsymbol{M}_n \\ & & -1 & & & 0 \\ & & & \ddots & & \vdots \\ & & & & -1 & 0 \end{vmatrix}.$$

注意，对于 $i = 0,\ 1 \ldots, k-1$ 和 $\omega_0 = 1$，右侧行列式的第 $(n-i)$ 行中只有一个非零项。因此，展开后得到

$$\begin{vmatrix} \boldsymbol{M} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{vmatrix} = \begin{vmatrix} \boldsymbol{M}_1 & \cdots & \boldsymbol{M}_{n-k-1} & \sum_{i=0}^{k} \boldsymbol{M}_{n-i}\omega_i \end{vmatrix}.$$

继续化简行列式，我们得到

$$\begin{aligned} \begin{vmatrix} \boldsymbol{M} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{vmatrix} &= \sum_{i=0}^{k} \begin{vmatrix} \boldsymbol{M}_1 & \cdots & \boldsymbol{M}_{n-k-1} & \boldsymbol{M}_{n-i}\omega_i \end{vmatrix} \\ &= \sum_{i=0}^{k} \begin{vmatrix} \boldsymbol{M}_1 & \cdots & \boldsymbol{M}_{n-k-1} & \boldsymbol{M}_{n-i} \end{vmatrix} \omega_i \end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=0}^{k} \left|\hat{\boldsymbol{M}}_i\right| \omega_i \\
&= \operatorname{detp}_{\boldsymbol{\omega}} \boldsymbol{M},
\end{aligned}
$$

这与我们所需的结果等价。 □

在引理 13 中将 $\boldsymbol{B}_{\boldsymbol{\omega},k}$ 特化到引理 17 的 $\boldsymbol{M}$ 后，我们立即得到以下结果。

推论 18. 给定 (1) 中的 $\boldsymbol{\omega}$ 一般基 $\mathbb{F}_n[x]$、F 和 G，设 $\boldsymbol{B}_{\boldsymbol{\omega},k}$ 是 F 和 G 关于基 $\boldsymbol{\omega}$ 中的 x 的 B´ézout 矩阵删去最后 k 行后得到的子矩阵，且 $\boldsymbol{X}_{\boldsymbol{\omega},k}$ 如 (10) 所示。那么

$$
\begin{vmatrix} \boldsymbol{B}_{\boldsymbol{\omega},k} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{vmatrix} = \operatorname{detp}_{\boldsymbol{\omega}} \boldsymbol{B}_{\boldsymbol{\omega},k}. \tag{20}
$$

4.4 定理 8 的证明

现在我们可以证明主定理（即定理 8）了。

证明. 根据引理 13，我们有

$$
S_k = c_{\boldsymbol{\omega}} \cdot \begin{vmatrix} \boldsymbol{B}_{\boldsymbol{\omega},k} \\ \boldsymbol{X}_{\boldsymbol{\omega},k} \end{vmatrix}.
$$

将 (20) 代入上式，得到

$$
S_k = c_{\boldsymbol{\omega}} \cdot \operatorname{detp}_{\boldsymbol{\omega}} \boldsymbol{B}_{\boldsymbol{\omega},k}.
$$

其中 $c_{\boldsymbol{\omega}} = (-1)\binom{n-k}{2} a_n^{m-n}$，由此完成证明。 □

5 结论与展望

本文提出了一种方法，借助非标准基下的 B´ezout 矩阵，构造以一般基表示的单变量多项式的 B´ezout 型子结式多项式。尽管基发生了变化，但子结式的基本性质仍得以保留。本研究的动机在于观察到，以一般基表示的多项式的 B´ezout 矩阵通常比将多项式转换为标准基后得到的 B´ezout 矩阵更为简单（见例 9），所得的子结式多项式也具有同样的特点。一般基下 B´ezout 矩阵的简洁表达式对于探索一般基下子结式所蕴含的优美隐藏结构可能非常有帮助。然而，为了找到一种高效计算一般基下结式矩阵和子结式多项式的方法，有必要充分利用给定基的结构，这将成为下一阶段需要研究的关键问题。

另一个相关问题是，如何设计算法来计算其他基下的多项式的子结式多项式，这些基具有与一般基相似的性质（例如伯恩斯坦基 [6]）。这一问题也值得在未来进一步研究。

致谢。本研究得到国家自然科学基金委员会项目（项目编号：12261010和11801101）以及广西民族大学2022年科研培育项目（项目编号：2022MDKJ001）的资助。

参考文献

[1] A. Amiraslani、D. A. Aruliah和Robert M. Corless. 广义伴随矩阵铅笔的瑞利商迭代. 预印本，2006年。[2] Fran¸cois Ap´ery和Jean-Pierre Jouanolou. 结式与子结式：消元——单变量情形——附订正习题. Hermann，2006年。[3] Dhavide Aruliah、Robert Corless、Laureano Gonz´alez-Vega和Azar Shakoori. 二元张量积拉格朗日基中贝祖矩阵的几何应用. 2007年1月。[4] S Barnett. 切比雪夫多项式的贝祖矩阵. 布拉德福德大学数学科学学院，1987年。[5] Stephen Barnett. 多个多项式的最大公因式. 载于《剑桥哲学学会数学学报》，第70卷，第263–268页。剑桥大学出版社，1971年。[6] Dario A Bini和Luca Gemignani. 伯恩斯坦-贝祖矩阵. 《理论计算机科学》，315(2-3):319–333，2004年。[7] Alin Bostan、Carlos D'Andrea、Teresa Krick、Agnes Szanto和Marcelo Valdettaro. 重根情形下的子结式：一个极端情形. 《线性代数及其应用》，529:185–198，2017年。[8] Jes´us M Carnicer和Juan Manuel Pena. 保形表示与伯恩斯坦基的最优性. 《计算数学进展》，1(2):173–196，1993年。[9] George E Collins. 子结式与约化多项式余序列. 《美国计算机协会杂志》，14(1):128–142，1967年。[10] David A Cox和Carlos D'Andrea. 子结式与形状引理. arXiv:2112.10306，2021年。[11] Carlos D'Andrea、Teresa Krick和Agnes Szanto. 根上的多元子结式. 《代数杂志》，302(1):16–36，2006年。[12] J. Delgado和J. M. Pe˜na. 一种具有线性复杂度求值算法的保形表示. 《计算机辅助几何设计》，20(1):1–10，2003年。[13] Gema M Diaz-Toca和Laureano Gonzalez-Vega. 子结式的若干新表达式及其应用. 《工程、通信与计算中的应用代数》，15(3):233–266，2004年。[14] Gema Mar´ıa D´ıaz-Toca和Mario Fioravanti. 任意基下贝祖矩阵的零空间与最大公因式. 载于2014年计算代数与应用会议论文集（EACA' 2014），2014年。[15] Rida T Farouki和VT Rajan. 伯恩斯坦形式中多项式的数值条件. 《计算机辅助几何设计》，4(3):191–216，1987年。[16] T. N. T. Goodman和H. B. Said. 广义巴尔基的保形性质. 《计算机辅助几何设计》，8(2):115–121，1991年。

[17] Chung-Jen Ho.《代数计算专题：子结式、最大公因式、因式分解与素理想分解》。博士论文，美国，1989年。[18] H. Hong。《根中的子结式》。载于第八届计算机代数应用国际会议（ACA'2002）论文集。沃洛斯，希腊，2002年。[19] Hoon Hong。《根中的子结式》。技术报告，数学系。北卡罗来纳州立大学，1999年。[20] Hoon Hong 和 Jing Yang。单变量多项式重数结构的一个条件。《符号计算杂志》，104:523–538，2021年。[21]Hoon Hong 和 Jing Yang。多个单变量多项式的子结式。arXiv:2112.15370，2021年。[22] Xiaorong Hou 和 Dongming Wang。带有 B´ézout 矩阵的子结式。载于《计算机数学》，第19–28页。世界科学出版社，2000年。[23] Alain Lascoux 和 Piotr Pragacz。子结式的双重西尔维斯特和与多重舒尔函数。《符号计算杂志》，35(6):689–710，2003年。[24] Yong-Bin Li。构造子结式的新方法。《应用数学与计算》，183(1):471–476，2006年。[25] Ana Marco 和 Jos´e-Javier Mart´ínez。伯恩斯坦–贝祖矩阵与曲线隐式化。《理论计算机科学》，377(1-3):65–72，2007年。[26] Sylvester。关于两个有理整函数的合消关系理论，其中包括对斯图姆函数理论及最大代数公因式理论的应用。《哲学汇刊》，143:407–548，1853年。[27] Akira Terui。递归多项式余式序列及其子结式。《代数杂志》，320(2):633–659，2008年。[28] Weidong Wang 和 Jing Yang。牛顿基下多个单变量多项式的广义伴随子结式。arXiv:2212.03422，2022年。[29] H. Wu、X. Wu 和 Z.H. Yang。关于一般基下多项式贝祖矩阵的更多讨论。《线性代数电子杂志》，21:14，2010年。[30] Z.H. Yang。一般基下的多项式贝祖矩阵。《线性代数及其应用》，331(1):165–179，2001年。