Journal of Symbolic Computation 68 (2015) 169–203

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Sparse difference resultant ☆

Wei Li, Chun-Ming Yuan, Xiao-Shan Gao

KLMM, Academy of Mathematics and Systems Science, The Chinese Academy of Sciences, Beijing 100190, China

ARTICLE INFO

Article history:
Received 24 September 2013
Accepted 13 September 2014
Available online 19 September 2014

Keywords:
Sparse difference resultant
Difference resultant
Laurent transformally essential system
Jacobi number
Transformally homogeneous polynomial
Incompleteness of projective difference space
Single exponential algorithm

ABSTRACT

In this paper, the concept of sparse difference resultant for a Laurent transformally essential system of difference polynomials is introduced and a simple criterion for the existence of sparse difference resultant is given. The concept of transformally homogenous polynomial is introduced and the sparse difference resultant is proved to be transformally homogenous. It is shown that the vanishing of the sparse difference resultant gives a necessary condition for the corresponding difference polynomial system to have non-zero solutions. Order and degree bounds for the sparse difference resultant are given. Based on these bounds, an algorithm to compute the sparse difference resultant is proposed, which is single exponential in terms of the number of variables, the Jacobi number, and the size of the Laurent transformally essential system. Furthermore, the precise order and degree, a determinant representation, and a Poisson-type product formula for the difference resultant are given.

1. Introduction

The resultant, which gives conditions for an over-determined system of polynomial equations to have common solutions, is a basic concept in algebraic geometry and a powerful tool in elimination theory (Canny, 1990; Cox et al., 1998; Eisenbud et al., 2004; Hodge and Pedoe, 1968; Jouanolou, 1991; Sturmfels, 1993). The concept of sparse resultant originated from the work of Gelfand, Kapranov, and Zelevinsky on generalized hypergeometric functions, where the central concept of $\mathcal{A}$-discriminant

☆ Partially supported by a National Key Basic Research Project of China (2011CB302400) and by grants from NSFC (60821002, 11101411).

E-mail addresses: liwei@mmrc.iss.ac.cn (W. Li), cmyuan@mmrc.iss.ac.cn (C.-M. Yuan), xgao@mmrc.iss.ac.cn (X.-S. Gao).

http://dx.doi.org/10.1016/j.jsc.2014.09.016
0747-7171/© 2014 Elsevier Ltd. All rights reserved.

is studied (Gelfand et al., 1994). Kapranov, Sturmfels, and Zelevinsky introduced the $\mathcal{A}$-resultant (Kapranov et al., 1992). Sturmfels further introduced the general mixed sparse resultant and gave a single exponential algorithm to compute the sparse resultant (Sturmfels, 1993, 1994). Canny and Emiris showed that the sparse resultant is a factor of the determinant of a Macaulay style matrix and gave an efficient algorithm to compute the sparse resultant based on this matrix representation (Emiris and Canny, 1995). A precise determinant representation for the sparse resultant was given by D'Andrea (2002). Recently, a rigorous definition for the multivariate differential resultant was presented (Gao et al., 2013) and also the theory of sparse differential resultants for Laurent differentially essential systems was developed (Li et al., 2011, 2012).

In this paper, the concept of sparse difference resultant for a Laurent transformally essential system consisting of $n+1$ Laurent difference polynomials in n difference variables is introduced and its basic properties are proved. A criterion is given to check whether a Laurent difference system is essential in terms of their supports, which is conceptually and computationally simpler than the naive approach based on the characteristic set method. The concept of transformal homogeneity is introduced and it is proved that the sparse difference resultant is transformally homogeneous. It is also shown that the sparse difference resultant is equal to the algebraic sparse resultant of a generic sparse polynomial system, and hence has a determinant representation.

It is shown that the vanishing of the sparse difference resultant gives a necessary condition for the corresponding difference polynomial system to have nonzero solutions, which is also sufficient in a certain sense. The concepts of difference projective space and transformal completeness are introduced and the projective space is shown to be not transformally complete using the sparse difference resultant for a set of specific difference polynomials. It is a classic result that the algebraic projective space is complete (Eisenbud, 1995, p. 303) and the differential projective space is not complete (Kolchin, 1974).

We give order and degree bounds for the sparse difference resultant. It is shown that the order and effective order of the sparse difference resultant can be bounded by the Jacobi number of the corresponding difference polynomial system and the degree can be bounded by a Bézout type bound. Based on these bounds, an algorithm is given to compute the sparse difference resultant. The complexity of the algorithm in the worst case is single exponential in terms of the number of variables, the degree, the Jacobi number, and the size of the Laurent transformally essential system, respectively.

For the difference resultant, which is non-sparse, more and better properties are proved including its precise order and degree, a determinant representation, and a Poisson-type product formula.

Although most properties for sparse difference resultants and difference resultants are similar to their differential counterparts given in Li et al. (2012) and Gao et al. (2013), some of them are quite different in terms of descriptions and proofs due to the distinct nature of the differential and difference operators. First, the definition for the difference resultant is more subtle than the differential case as illustrated by Problem 23. Second, the criterion for Laurent transformally essential systems given in Section 3.3 is quite different and much simpler than its differential counterpart given in Li et al. (2012). Also, determinant representations for the sparse difference resultant and the difference resultant are given in Sections 5 and 7, but such a representation is still not known for differential resultants (Zhang et al., 2012; Rueda and Sendra, 2010; Rueda, 2013). Finally, there does not exist a definition for homogeneous difference polynomials, and the definition given in this paper is different from its differential counterpart (Li and Gao, 2012).

The rest of the paper is organized as follows. In Section 2, we prove some preliminary results. In Section 3, we first introduce the concepts of Laurent difference polynomials and Laurent transformally essential systems, and then define the sparse difference resultant for Laurent transformally essential systems. Basic properties of the sparse difference resultant are proved in Section 4. In Section 5, the sparse difference resultant is shown to be the algebraic sparse resultant for a certain generic polynomial system. In Section 6, we present an algorithm to compute the sparse difference resultant. In Section 7, we introduce the notion of difference resultant and prove its basic properties. In Section 8, we conclude the paper by proposing several problems for future research. An extended abstract of this paper appeared in the proceedings of ISSAC2013 (Li et al., 2013). Besides detailed proofs and further results, Section 5 is newly added.

2. Preliminaries

In this section, some basic notations and preliminary results in difference algebra will be given. For more details about difference algebra, please refer to Cohn (1965), Hrushovski (2004), Levin (2008) and Wibmer (2013).

2.1. Difference polynomial ring

An ordinary difference field $\mathcal{F}$ is a field with a third unitary operation σ satisfying that for any $a, b \in \mathcal{F}$, $\sigma(a+b) = \sigma(a) + \sigma(b)$, $\sigma(ab) = \sigma(a)\sigma(b)$, and $\sigma(a) = 0$ if and only if $a = 0$. We call σ the *transforming operator* of $\mathcal{F}$. If $a \in \mathcal{F}$, $\sigma(a)$ is called the transform of a and is denoted by $a^{(1)}$. And for $n \in \mathbb{Z}^+$, $\sigma^n(a) = \sigma^{n-1}(\sigma(a))$ is called the n-th transform of a and denoted by $a^{(n)}$, with the usual assumption $a^{(0)} = a$. By $a^{[n]}$ we mean the set $\{a, a^{(1)}, \dots, a^{(n)}\}$. If $\sigma^{-1}(a)$ is defined for each $a \in \mathcal{F}$, we say that $\mathcal{F}$ is inversive. A typical example of difference field is $\mathbb{Q}(x)$ with $\sigma(f(x)) = f(x+1)$. All difference fields in this paper are assumed to be inversive with characteristic zero.

Let S be a subset of a difference field $\mathcal{G}$ which contains $\mathcal{F}$. We will denote respectively by $\mathcal{F}[S]$, $\mathcal{F}(S)$, $\mathcal{F}\{S\}$, and $\mathcal{F}\langle S\rangle$ the smallest subring, the smallest subfield, the smallest difference subring, and the smallest difference subfield of $\mathcal{G}$ containing $\mathcal{F}$ and S. If we denote $\Theta(S) = \{\sigma^k(a) \mid k \geq 0, a \in S\}$, then we have $\mathcal{F}\{S\} = \mathcal{F}[\Theta(S)]$ and $\mathcal{F}\langle S\rangle = \mathcal{F}(\Theta(S))$.

A subset $\mathcal{S}$ of a difference extension field $\mathcal{G}$ of $\mathcal{F}$ is said to be *transformally dependent* over $\mathcal{F}$ if the set $\{\sigma^k(a) \mid a \in \mathcal{S}, k \geq 0\}$ is algebraically dependent over $\mathcal{F}$, and otherwise, it is said to be *transformally independent* over $\mathcal{F}$, or to be a family of *difference indeterminates* over $\mathcal{F}$. In the case $\mathcal{S}$ consists of only one element α, we say that α is *transformally algebraic* or *transformally transcendental* over $\mathcal{F}$, respectively. A maximal subset Ω of $\mathcal{G}$ which is transformally independent over $\mathcal{F}$ is said to be a transformal transcendence basis of $\mathcal{G}$ over $\mathcal{F}$. We use $\sigma.\mathrm{tr.deg}\,\mathcal{G}/\mathcal{F}$ to denote the *transformal transcendence degree* of $\mathcal{G}$ over $\mathcal{F}$, which is the cardinal number of Ω. Considering $\mathcal{F}$ and $\mathcal{G}$ as ordinary algebraic fields, we denote the algebraic transcendence degree of $\mathcal{G}$ over $\mathcal{F}$ by $\mathrm{tr.deg}\,\mathcal{G}/\mathcal{F}$.

Now suppose $\mathbb{Y} = \{y_1, y_2, \dots, y_n\}$ is a set of difference indeterminates over $\mathcal{F}$. The elements of $\mathcal{F}\{\mathbb{Y}\} = \mathcal{F}[y_j^{(k)} : j = 1, \dots, n; k \in \mathbb{N}_0]$ are called *difference polynomials* over $\mathcal{F}$ in $\mathbb{Y}$, and $\mathcal{F}\{\mathbb{Y}\}$ itself is called the *difference polynomial ring* over $\mathcal{F}$ in $\mathbb{Y}$. A *difference ideal* $\mathcal{I}$ in $\mathcal{F}\{\mathbb{Y}\}$ is an ordinary algebraic ideal which is closed under transforming, i.e. $\sigma(\mathcal{I}) \subset \mathcal{I}$. If $\mathcal{I}$ also has the property that $a^{(1)} \in \mathcal{I}$ implies that $a \in \mathcal{I}$, it is called a *reflexive difference ideal*. A prime difference ideal is a difference ideal which is prime as an ordinary algebraic polynomial ideal. For convenience, a prime difference ideal is assumed not to be the unit ideal in this paper. If S is a finite set of difference polynomials, we use (S) and $[S]$ to denote the algebraic ideal and the difference ideal in $\mathcal{F}\{\mathbb{Y}\}$ generated by S.

An n-tuple over $\mathcal{F}$ is an n-tuple of the form $\mathbf{a} = (a_1, \dots, a_n)$ where the a_i are selected from a difference extension field of $\mathcal{F}$. For a difference polynomial $f \in \mathcal{F}\{y_1, \dots, y_n\}$, $\mathbf{a}$ is called a difference zero of f if when substituting $y_i^{(j)}$ by $a_i^{(j)}$ in f, the result is 0. An n-tuple η is called a *generic zero* of a difference ideal $\mathcal{I} \subset \mathcal{F}\{\mathbb{Y}\}$ if for any polynomial $P \in \mathcal{F}\{\mathbb{Y}\}$ we have $P(\eta) = 0 \Leftrightarrow P \in \mathcal{I}$. It is well known that

Lemma 1. *(See Cohn, 1965, p. 77.) A difference ideal possesses a generic zero if and only if it is a reflexive prime difference ideal other than the unit ideal.*

Let $\mathcal{I}$ be a reflexive prime difference ideal and η a generic zero of $\mathcal{I}$. The *dimension* of $\mathcal{I}$ is defined as $\sigma.\mathrm{tr.deg}\,\mathcal{F}\langle\eta\rangle/\mathcal{F}$, denoted by $\dim(\mathcal{I})$. If $\dim(\mathcal{I}) = 0$, then $\mathrm{tr.deg}\,\mathcal{F}\langle\eta\rangle/\mathcal{F}$ is defined to be the *order* of $\mathcal{I}$, denoted by $\mathrm{ord}(\mathcal{I})$. Notice that the prime property depends on the difference ring where an ideal is defined. In the rest of the paper, to put emphasis the difference ring where difference ideals are generated, for any subset Σ, we will use $[\Sigma]_{\mathcal{F}\{\mathbb{Y}\}}$ or $[\Sigma] \cdot \mathcal{F}\{\mathbb{Y}\}$ to denote the difference ideal generated by Σ in $\mathcal{F}\{\mathbb{Y}\}$.

Given two n-tuples $\mathbf{a} = (a_1, \dots, a_n)$ and $\bar{\mathbf{a}} = (\bar{a}_1, \dots, \bar{a}_n)$ over $\mathcal{F}$, $\bar{\mathbf{a}}$ is called a *specialization* of $\mathbf{a}$ over $\mathcal{F}$, or $\mathbf{a}$ specializes to $\bar{\mathbf{a}}$, if for any difference polynomial $P \in \mathcal{F}\{\mathbb{Y}\}$, $P(\mathbf{a}) = 0$ implies that $P(\bar{\mathbf{a}}) = 0$. The following property about difference specialization will be needed in this paper.

Lemma 2. *Let $P_i(\mathbb{U}, \mathbb{Y}) \in \mathcal{F}\langle\mathbb{Y}\rangle\{\mathbb{U}\}$ $(i = 1, \dots, m)$ where $\mathbb{U} = (u_1, \dots, u_r)$ is a set of difference indeterminates. If $P_i(\mathbb{U}, \mathbb{Y})$ $(i = 1, \dots, m)$ are transformally dependent over $\mathcal{F}\langle\mathbb{U}\rangle$, then for any difference specialization $\mathbb{U}$ to $\overline{\mathbb{U}} \subset \mathcal{F}$, $P_i(\overline{\mathbb{U}}, \mathbb{Y})$ $(i = 1, \dots, m)$ are transformally dependent over $\mathcal{F}$.*

Proof. It suffices to show the case $r = 1$. Denote $u = u_1$. Since $P_i(u, \mathbb{Y})$ $(i = 1, \dots, m)$ are transformally dependent over $\mathcal{F}\langle u\rangle$, there exist natural numbers s and l such that $\mathbb{P}_i^{(k)}(u, \mathbb{Y})$ $(k \le s)$ are algebraically dependent over $\mathcal{F}(u^{(k)} \mid k \le s + l)$. When u specializes to $\bar{u} \in \mathcal{F}$, $u^{(k)}$ $(k \ge 0)$ are correspondingly algebraically specialized to $\bar{u}^{(k)} \in \mathcal{F}$. By Wu (2003, p. 161), $\mathbb{P}_i^{(k)}(\bar{u}, \mathbb{Y})$ $(k \le s)$ are algebraically dependent over $\mathcal{F}$. Thus, $P_i(\bar{u}, \mathbb{Y})$ $(i = 1, \dots, m)$ are transformally dependent over $\mathcal{F}$. □

2.2. Characteristic set for a difference polynomial system

In this section, we give several preliminary results about the characteristic set for a difference polynomial system. For details on difference characteristic set methods, please refer to Gao et al. (2009).

Let f be a difference polynomial in $\mathcal{F}\{\mathbb{Y}\}$. The order of f w.r.t. y_i is defined to be the greatest number k such that $y_i^{(k)}$ appears effectively in f, denoted by $\mathrm{ord}(f, y_i)$. The *order* of f is defined to be $\max_i \mathrm{ord}(f, y_i)$, that is, $\mathrm{ord}(f) = \max_i \mathrm{ord}(f, y_i)$. The *least order* of f w.r.t. y_i is $\mathrm{Lord}(f, y_i) = \min\{k \mid \deg(f, y_i^{(k)}) > 0\}$ and the *effective order* of f w.r.t. y_i is $\mathrm{Eord}(f, y_i) = \mathrm{ord}(f, y_i) - \mathrm{Lord}(f, y_i)$. And if y_i does not appear in f, then we set $\mathrm{ord}(f, y_i) = \mathrm{Eord}(f, y_i) = -\infty$.

A *ranking* $\mathscr{R}$ is a total order over $\Theta(\mathbb{Y}) = \{\sigma^k(y_i) \mid 1 \le i \le n, k \ge 0\}$, which satisfies the following properties:

1) $\sigma(\theta) > \theta$ for each $\theta \in \Theta(\mathbb{Y})$.
2) $\theta_1 > \theta_2 \Longrightarrow \sigma(\theta_1) > \sigma(\theta_2)$ for $\theta_1, \theta_2 \in \Theta(\mathbb{Y})$.

Let f be a difference polynomial in $\mathcal{F}\{\mathbb{Y}\}$ and $\mathscr{R}$ a ranking endowed on it. The greatest $y_j^{(k)}$ w.r.t. $\mathscr{R}$ which appears effectively in f is called the *leader* of f, denoted by $\mathrm{ld}(f)$ and y_j is called the *leading variable* of f, denoted by $\mathrm{lvar}(f) = y_j$. The leading coefficient of f as a univariate polynomial in $\mathrm{ld}(f)$ is called the *initial* of f and is denoted by I_f.

Let f and g be two difference polynomials in $\mathcal{F}\{\mathbb{Y}\}$ with $\mathrm{ld}(f) = y_j^{(k)}$. We say g is of higher rank than f if either $\mathrm{ld}(g) > y_j^{(k)}$, or $\mathrm{ld}(g) = y_j^{(k)}$ and $\deg(g, y_j^{(k)}) > \deg(f, y_j^{(k)})$. And g is said to be *reduced* w.r.t. f if $\deg(g, y_j^{(k+l)}) < \deg(f, y_j^{(k)})$ for all $l \in \mathbb{N}_0$.

A finite chain of nonzero difference polynomials $\mathcal{A} = A_1, \dots, A_m$ is said to be an *ascending chain* if

1) $m = 1$ and $A_1 \ne 0$ or
2) $m > 1$, $A_j > A_i$ and A_j is reduced w.r.t. A_i for $1 \le i < j \le m$.

Let $\mathcal{A} = A_1, A_2, \dots, A_t$ be an ascending chain and f an arbitrary difference polynomial. Then there exists an algorithm, which reduces f w.r.t. $\mathcal{A}$ to a polynomial r that is reduced w.r.t. $\mathcal{A}$, satisfying the relation

$$\prod_{i=1}^{t}\prod_{k=0}^{d_i}\big(\sigma^k(\mathrm{I}_{A_i})\big)^{e_{ik}} \cdot f \equiv r, \mathrm{mod}[\mathcal{A}],$$

where the d_i, e_{ik} are nonnegative integers. The difference polynomial r is called the *difference remainder* of f w.r.t. $\mathcal{A}$ (Gao et al., 2009).

Let $\mathcal{A}$ be an ascending chain. Denote $\mathbb{I}_{\mathcal{A}}$ to be the minimal multiplicative set containing the initials of elements of $\mathcal{A}$ and their transforms. The *saturation ideal* of $\mathcal{A}$ is defined as

$$\mathrm{sat}(\mathcal{A}) = [\mathcal{A}] : \mathbb{I}_{\mathcal{A}} = \big\{p : \exists h \in \mathbb{I}_{\mathcal{A}}, hp \in [A]\big\}.$$

And the *algebraic saturation ideal* of $\mathcal{A}$ is $\text{asat}(\mathcal{A}) = (\mathcal{A}) : \text{I}_{\mathcal{A}}$, where $\text{I}_{\mathcal{A}}$ is the minimal multiplicative set containing the initials of elements of $\mathcal{A}$.

An ascending chain $\mathcal{C}$ contained in a difference polynomial set $\mathcal{S}$ is said to be a *characteristic set* of $\mathcal{S}$, if $\mathcal{S}$ does not contain any nonzero element reduced w.r.t. $\mathcal{C}$. A characteristic set $\mathcal{C}$ of a difference ideal $\mathcal{J}$ reduces all elements of $\mathcal{J}$ to zero.

Let $\mathcal{A}$ be a characteristic set of a reflexive prime difference ideal $\mathcal{I}$. We rewrite $\mathcal{A}$ in the following form

$$\mathcal{A} = \begin{cases} A_{11}, \ldots, A_{1k_1} \\ \cdots \\ A_{p1}, \ldots, A_{pk_p} \end{cases} \tag{1}$$

where $\text{lvar}(A_{ij}) = y_{c_i}$ for $j = 1, \ldots, k_i$ and $\text{ord}(A_{ij}, y_{c_i}) < \text{ord}(A_{il}, y_{c_i})$ for $j < l$. In terms of a characteristic set of the above form, p is equal to the *codimension* of $\mathcal{I}$, that is $n - \dim(\mathcal{I})$. Unlike the differential case, here even though $\mathcal{I}$ is of codimension one, there may be more than one difference polynomial in a characteristic set of $\mathcal{I}$ as shown by the following example.

Example 3. Let $A_{11} = (y_1^{(1)})^2 + y_1^2 + 1$, $A_{12} = y_1^{(2)} - y_1$. Then $\mathcal{I} = [A_{11}, \mathcal{A}_{12}]$ is a reflexive prime difference ideal whose characteristic set is $\mathcal{A} = A_{11}, A_{12}$ and $\mathcal{I} = \text{sat}(\mathcal{A})$ (Gao et al., 2009). Note that $[A_{11}]$ is not a prime difference ideal, because $\sigma(A_{11}) - A_{11} = (y_1^{(2)} - y_1)(y_1^{(2)} + y_1) \in [A_{11}]$ and both $y_1^{(2)} - y_1$ and $y_1^{(2)} + y_1$ are not in $[A_{11}]$.

Now we proceed to show that given a reflexive prime difference ideal, a property of uniqueness still exists among all its characteristic sets under different rankings. First of all, several algebraic results will be needed.

Let $\mathcal{B} = B_1, \ldots, B_m$ be an algebraic triangular set in $\mathcal{F}[x_1, \ldots, x_n]$ with $\text{lvar}(B_i) = y_i$ and $U = \{x_1, \ldots, x_n\} \backslash \{y_1, \ldots, y_m\}$ the parametric set of $\mathcal{B}$. We assume $U < y_1 < y_2 < \cdots < y_m$. A polynomial f is said to be invertible w.r.t. $\mathcal{B}$ if $(f, B_1, \ldots, B_s) \cap \mathcal{F}[U] \neq \{0\}$ where $\text{lvar}(f) = \text{lvar}(B_s)$. We call $\mathcal{B}$ a *regular chain* if for each $i > 1$, the initial of B_i is invertible w.r.t. $B_1, \ldots, B_{i-1}$. For a regular chain $\mathcal{B}$, we say that f is invertible w.r.t. $\text{asat}(\mathcal{B})$ if $(f, \text{asat}(\mathcal{B})) \cap \mathcal{F}[U] \neq \{0\}$. The next two lemmas give basic properties of regular chains which will be used later.

Lemma 4. *Let $\mathcal{B}$ be a regular chain in $\mathcal{F}[x_1, \ldots, x_n]$. If $\sqrt{\text{asat}(\mathcal{B})} = \bigcap_{i=1}^m \mathcal{P}_i$ is an irredundant prime decomposition of $\sqrt{\text{asat}(\mathcal{B})}$, then a polynomial f is invertible w.r.t. $\text{asat}(\mathcal{B})$ if and only if $f \notin \mathcal{P}_i$ for all $i = 1, \ldots, m$.*

Proof. Since $\sqrt{\text{asat}(\mathcal{B})} = \bigcap_{i=1}^m \mathcal{P}_i$ is an irredundant prime decomposition of $\sqrt{\text{asat}(\mathcal{B})}$, U is a parametric set of $\mathcal{P}_i$ for each i by Gao and Chou (1993). And for prime ideals $\mathcal{P}_i$, $f \notin \mathcal{P}_i$ if and only if $(f, \mathcal{P}_i) \cap \mathcal{F}[U] \neq \{0\}$. If f is invertible w.r.t. $\text{asat}(\mathcal{B})$, $\{0\} \neq (f, \text{asat}(\mathcal{B})) \cap \mathcal{F}[U] \subset (f, \mathcal{P}_i) \cap \mathcal{F}[U]$. Thus, $f \notin \mathcal{P}_i$ for each i. For the other side, suppose $f \notin \mathcal{P}_i$ for all i, then there exist nonzero polynomials $h_i(U)$ such that $h_i(U) \in (f, \mathcal{P}_i)$. Thus, there exists $t \in \mathbb{N}$ such that $(\prod_{i=1}^m h_i(U))^t \in (f, \text{asat}(\mathcal{B}))$. So f is invertible w.r.t. $\text{asat}(\mathcal{B})$. □

Lemma 5. *(See Bouziane et al., 2001.) Let $\mathcal{B}$ be a regular chain in $\mathcal{F}[x_1, \ldots, x_n]$ and U the parametric set of $\mathcal{B}$. Let $f \in \mathcal{F}[x_1, \ldots, x_n]$ and L in $\mathcal{F}[U] \backslash \{0\}$ such that $Lf \in (\mathcal{B})$. Then $f \in \text{asat}(\mathcal{B})$.*

Lemma 6. *Let A be an irreducible difference polynomial in $\mathcal{F}\{\mathbb{Y}\}$ with $\deg(A, y_{i_0}) > 0$ for some i_0. If f is invertible w.r.t. $A^{[k]} = A, A^{(1)}, \ldots, A^{(k)}$ under some ranking $\mathscr{R}$, then $\sigma(f)$ is invertible w.r.t. $A^{[k+1]}$. In particular, $A^{[k]}$ is a regular chain for any $k \geq 0$.*

Proof. Suppose $\text{ld}(A) = y_l^{(s)}$. Let $U = \Theta(\mathbb{Y}) \backslash \{y_l^{(k)} \mid k \geq s\}$. Two cases will be considered.

i) $f \in \mathcal{F}[U]$. If $\sigma(f) \in \mathcal{F}[U]$, it is trivial. Otherwise, $\deg(\sigma(f), y_l^{(s)}) > 0$. Let R be the resultant of $\sigma(f)$ and A w.r.t. $y_l^{(s)}$. Then $R \neq 0$, for if not, A divides $\sigma(f)$, a contradiction to $\deg(A, y_{i_0}) > 0$. So $(\sigma(f), A) \cap \mathcal{F}[U] \neq \{0\}$ and $\sigma(f)$ is invertible w.r.t. $A^{[k+1]}$.

ii) $f \notin \mathcal{F}[U]$. Since f is invertible w.r.t. $A^{[k]}$, there exist $0 \neq h(U) \in \mathcal{F}[U]$ such that $h(U) \in (f, A^{[k]})$. So $\sigma(h(U)) \in (\sigma(f), A^{[k+1]})$. By i), $\sigma(h(U))$ is invertible w.r.t. $A^{[k+1]}$. So $\sigma(f)$ is also invertible w.r.t. $A^{[k+1]}$.

Since I_A is invertible w.r.t. A, it follows that $A^{[k]}$ is a regular chain. □

The following result is crucial to define sparse difference resultant.

Theorem 7. *Let $\mathcal{I}$ be a reflexive prime difference ideal of codimension one in $\mathcal{F}\{\mathbb{Y}\}$. The first element in any characteristic set of $\mathcal{I}$ w.r.t. any ranking, when taken irreducible, is unique up to a factor in $\mathcal{F}$.*

Proof. Write any ascending chain in form (1). Let $\mathcal{A} = A_{11}, \ldots, A_{1m}$ be a characteristic set of $\mathcal{I}$ w.r.t. some ranking $\mathscr{R}$ with A_{11} irreducible. Suppose $\mathrm{lvar}(A_{1i}) = y_1$. Given another characteristic set $\mathcal{B} = B_{11}, \ldots, B_{1l}$ of $\mathcal{I}$ w.r.t. some other ranking $\mathscr{R}'$ (B_{11} is irreducible), we need to show that there exists $c \in \mathcal{F}$ such that $B_{11} = c \cdot A_{11}$. If $\mathrm{lvar}(B_{11}) = y_1$, B_{11} and A_{11} should have the same orders in y_1. Since both of them are irreducible polynomials, $B_{11} = c \cdot A_{11}$ for some $c \in \mathcal{F}$ follows. So it suffices to prove the case $\mathrm{lvar}(B_{11}) \neq y_1$. Suppose $\mathrm{lvar}(B_{11}) = y_2$. Clearly, a transform of y_2 appears effectively in A_{11} for $\mathcal{B}$ reduces A_{11} to 0. And since $\mathcal{I}$ is reflexive, there exists some i_0 such that $\deg(A_{11}, y_{i_0}) > 0$.

Suppose $\mathrm{ord}(A_{11}, y_2) = o_2$. Take another ranking under which $y_2^{(o_2)}$ is the leader of A_{11} and we use $\widetilde{A}_{11}$ to distinguish it from the A_{11} under $\mathscr{R}$. By Lemma 6, for each k, $A_{11}^{[k]}$ and $\widetilde{A}_{11}^{[k]}$ are regular chains.

Now we claim that $\mathrm{asat}(A_{11}^{[k]}) = \mathrm{asat}(\widetilde{A}_{11}^{[k]})$ for each k. On the one hand, for any polynomial $f \in \mathrm{asat}(A_{11}^{[k]})$, we have $(\prod_{i=0}^{k} \sigma^i(\mathrm{I}_{A_{11}}))^a f \in (A_{11}^{[k]})$. Since $\mathrm{I}_{A_{11}}$ is invertible w.r.t. $\widetilde{A}_{11}$, by Lemma 6, $(\prod_{i=0}^{k} \sigma^i(\mathrm{I}_{A_{11}}))^a$ is invertible w.r.t. $\widetilde{A}_{11}^{[k]}$. Denote the parameters of $\widetilde{A}_{11}^{[k]}$ by $\widetilde{U}$. So there exists a nonzero polynomial $h(\widetilde{U})$ such that $h(\widetilde{U}) \in ((\prod_{i=0}^{k} \sigma^i(\mathrm{I}_{A_{11}}))^a, \widetilde{A}_{11}^{[k]})$. Thus, $h(\widetilde{U}) f \in (\widetilde{A}_{11}^{[k]})$. Since $\widetilde{A}_{11}^{[k]}$ is a regular chain, by Lemma 5, $f \in \mathrm{asat}(\widetilde{A}_{11}^{[k]})$. So $\mathrm{asat}(A_{11}^{[k]}) \subseteq \mathrm{asat}(\widetilde{A}_{11}^{[k]})$. Similarly, we can show that $\mathrm{asat}(\widetilde{A}_{11}^{[k]}) \subseteq \mathrm{asat}(A_{11}^{[k]})$. Thus, $\mathrm{asat}(A_{11}^{[k]}) = \mathrm{asat}(\widetilde{A}_{11}^{[k]})$.

Suppose $\mathrm{ord}(B_{11}, y_2) = o_2'$. Clearly, $o_2 \geq o_2'$. We now proceed to show that it is impossible for $o_2 > o_2'$. Suppose the contrary, i.e. $o_2 > o_2'$. Then B_{11} is invertible w.r.t. $\mathrm{asat}(\widetilde{A}_{11}^{[k]})$. Suppose $\sqrt{\mathrm{asat}(\widetilde{A}_{11}^{[k]})} = \bigcap_{i=1}^{t} \mathcal{P}_i$ is an irredundant prime decomposition. By Lemma 4, $B_{11} \notin \mathcal{P}_i$ for each i. Since $\mathrm{asat}(A_{11}^{[k]}) = \mathrm{asat}(\widetilde{A}_{11}^{[k]})$, using Lemma 4 again, B_{11} is invertible w.r.t. $\mathrm{asat}(A_{11}^{[k]})$. Thus, there exists a nonzero difference polynomial H with $\mathrm{ord}(H, y_1) < \mathrm{ord}(A_{11}, y_1)$ such that $H \in (B_{11}, \mathrm{asat}(A_{11}^{[k]})) \subset \mathcal{I}$, which is a contradiction. Thus, $o_2 = o_2'$. Since $\mathcal{B}$ reduces A_{11} to zero and A_{11} is irreducible, there exists $c \in \mathcal{F}$ such that $B_{11} = c \cdot A_{11}$. □

3. Sparse difference resultants

In this section, the concepts of Laurent difference polynomial and Laurent transformally essential system are first introduced, and then the sparse difference resultant for Laurent transformally essential systems is defined. A criterion for a Laurent polynomial system to be Laurent transformally essential in terms of the support of the given system is also given.

3.1. Laurent difference polynomials

Let $\mathcal{F}$ be an ordinary difference field with a transforming operator σ and $\mathcal{F}\{\mathbb{Y}\}$ the ring of difference polynomials in the difference indeterminates $\mathbb{Y} = \{y_1, \ldots, y_n\}$. Before defining sparse difference resultants, we first introduce the concept of Laurent difference polynomial.

Definition 8. A Laurent difference monomial of order s is a Laurent monomial in variables $\mathbb{Y}^{[s]} = (y_i^{(k)})_{1 \leq i \leq n; 0 \leq k \leq s}$. More precisely, it has the form $\prod_{i=1}^{n} \prod_{k=0}^{s} (y_i^{(k)})^{m_{ik}}$ where m_{ik} are integers which can be negative. A *Laurent difference polynomial* over $\mathcal{F}$ is a finite linear combination of Laurent difference monomials with coefficients in $\mathcal{F}$.

Clearly, the collection of all Laurent difference polynomials forms a commutative difference ring under the obvious sum, product, and the usual transforming operator σ, where all Laurent difference monomials are invertible. We denote the difference ring of Laurent difference polynomials with coefficients in $\mathcal{F}$ by $\mathcal{F}\{y_1, y_1^{-1}, \ldots, y_n, y_n^{-1}\}$, or simply by $\mathcal{F}\{\mathbb{Y}^{\pm}\}$.

Definition 9. For each Laurent difference polynomial $F \in \mathcal{F}\{\mathbb{Y}^{\pm}\}$, there exists a unique Laurent difference monomial M such that 1) $M \cdot F \in \mathcal{F}\{\mathbb{Y}\}$ and 2) for any Laurent difference monomial T with $T \cdot F \in \mathcal{F}\{\mathbb{Y}\}$, $T \cdot F$ is divisible by $M \cdot F$ as polynomials. This $M \cdot F$ is defined to be the *normal form* of F, denoted by $\mathrm{N}(F)$. The order and degree of $\mathrm{N}(F)$ is defined to be the *order* and *degree* of F, denoted by $\mathrm{ord}(F)$ and $\deg(F)$.

In the following, we consider zeros for Laurent difference polynomials.

Definition 10. Let F be a Laurent difference polynomial in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$. An n-tuple $(a_1, \ldots, a_n)$ over $\mathcal{F}$ with each $a_i \neq 0$ is said to be a *nonzero difference solution* of F if $F(a_1, \ldots, a_n) = 0$.

For an ideal $\mathcal{I} \subset \mathcal{F}\{\mathbb{Y}^{\pm}\}$, the difference zero set of $\mathcal{I}$ is the set of common nonzero difference zeros of all Laurent difference polynomials in $\mathcal{I}$. We will see later in Example 40, how nonzero difference solutions are naturally related with the sparse difference resultant.

3.2. Definition of sparse difference resultants

In this section, the definition of the sparse difference resultant will be given. Similar to the study of sparse resultants and sparse differential resultants, we first define sparse difference resultants for Laurent difference polynomials whose coefficients are difference indeterminates. Then the sparse difference resultant for a given Laurent difference polynomial system with concrete coefficients is the value that the generic resultant takes for the coefficients of the given system.

Suppose $\mathcal{A}_i = \{M_{i0}, M_{i1}, \ldots, M_{il_i}\}$ $(i = 0, 1, \ldots, n)$ are finite sets of Laurent difference monomials in $\mathbb{Y}$. Consider $n+1$ *generic Laurent difference polynomials* defined over $\mathcal{A}_0, \ldots, \mathcal{A}_n$:

$$\mathbb{P}_i = \sum_{k=0}^{l_i} u_{ik} M_{ik} \quad (i = 0, \ldots, n), \tag{2}$$

where all the u_{ik} are transformally independent over the rational number field $\mathbb{Q}$. Denote

$$\mathbf{u}_i = (u_{i0}, u_{i1}, \ldots, u_{il_i}), \quad i = 0, \ldots, n, \quad \text{and} \quad \mathbf{u} = \bigcup_{i=0}^{n} \mathbf{u}_i \backslash \{u_{i0}\}. \tag{3}$$

The number $l_i + 1$ is called the *size* of $\mathbb{P}_i$ and $\mathcal{A}_i$ is called the *support* of $\mathbb{P}_i$. To avoid the triviality, $l_i \geq 1$ $(i = 0, \ldots, n)$ are always assumed in this paper.

Definition 11. A set of Laurent difference polynomials of the form (2) is called *Laurent transformally essential* if there exist k_i $(i = 0, \ldots, n)$ with $1 \leq k_i \leq l_i$ such that $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle \frac{M_{0k_0}}{M_{00}}, \frac{M_{1k_1}}{M_{10}}, \ldots, \frac{M_{nk_n}}{M_{n0}} \rangle / \mathbb{Q} = n$. In this case, we also say that $\mathcal{A}_0, \ldots, \mathcal{A}_n$ form a Laurent transformally essential system.

Although M_{i0} are used as denominators to define transformally essential systems, the following lemma shows that the definition does not depend on the choices of M_{i0}.

Lemma 12. *The following two conditions are equivalent.*

(1) *There exist k_i satisfying $1 \leq k_i \leq l_i$ for $i = 0, \ldots, n$ such that $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle \frac{M_{0k_0}}{M_{00}}, \ldots, \frac{M_{nk_n}}{M_{n0}} \rangle / \mathbb{Q} = n$.*

(2) *There exist pairs (k_i, j_i) $(i = 0, \dots, n)$ with $k_i \neq j_i \in \{0, \dots, l_i\}$ such that $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle \frac{M_{0k_0}}{M_{0j_0}}, \dots, \frac{M_{nk_n}}{M_{nj_n}} \rangle / \mathbb{Q} = n$.*

Proof. It is trivial that 1) implies 2). For the other direction, assume 2) holds. Without loss of generality, suppose $\frac{M_{1k_1}}{M_{1j_1}}, \dots, \frac{M_{nk_n}}{M_{nj_n}}$ are transformally independent over $\mathbb{Q}$. We need to show 1) holds. Suppose the contrary, then for any $m_i \in \{1, \dots, l_i\}$, $\frac{M_{1m_1}}{M_{10}}, \dots, \frac{M_{nm_n}}{M_{n0}}$ are transformally dependent over $\mathbb{Q}$. Now we claim that $(*)$ suppose for each $i \in \{1, 2\}$, a and b_i are transformally dependent over $\mathbb{Q}$, then a and b_1/b_2 are transformally dependent over $\mathbb{Q}$. Indeed, if a is transformally algebraic over $\mathbb{Q}$, then $(*)$ follows. If a is transformally transcendental over $\mathbb{Q}$, then each b_i is transformally algebraic over $\mathbb{Q}\langle a \rangle$. Thus, b_1/b_2 is transformally algebraic over $\mathbb{Q}\langle a \rangle$ (Levin, 2008, p. 245) and the claim is proved. Since $\frac{M_{ik_i}}{M_{ij_i}} = \frac{M_{ik_i}}{M_{i0}} / \frac{M_{ij_i}}{M_{i0}}$, by claim $(*)$, $\frac{M_{ik_i}}{M_{ij_i}}$ $(i = 1, \dots, n)$ are transformally dependent over $\mathbb{Q}$, which leads to a contradiction. □

Let $\mathbb{m}$ be the set of all difference monomials in $\mathbb{Y}$. Let

$$\mathcal{I}_{\mathbb{Y},\mathbf{u}} = \big([\mathrm{N}(\mathbb{P}_0), \dots, \mathrm{N}(\mathbb{P}_n)] : \mathbb{m}\big)_{\mathbb{Q}\{\mathbb{Y}, \mathbf{u}_0, \dots, \mathbf{u}_n\}}, \tag{4}$$

$$\mathcal{I}_{\mathbf{u}} = \mathcal{I}_{\mathbb{Y},\mathbf{u}} \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}. \tag{5}$$

The following result is a foundation for defining sparse difference resultants.

Theorem 13. *Let $\mathbb{P}_0, \dots, \mathbb{P}_n$ be the Laurent difference polynomials defined in (2). Then the following assertions hold.*

(1) *$\mathcal{I}_{\mathbb{Y},\mathbf{u}}$ is a reflexive prime difference ideal in $\mathbb{Q}\{\mathbb{Y}, \mathbf{u}_0, \dots, \mathbf{u}_n\}$.*
(2) *$\mathcal{I}_{\mathbf{u}}$ is of codimension one if and only if $\mathbb{P}_0, \dots, \mathbb{P}_n$ form a Laurent transformally essential system.*

Proof. Let $\eta = (\eta_1, \dots, \eta_n)$ be a sequence of transformally independent elements over $\mathbb{Q}\langle \mathbf{u} \rangle$, where $\mathbf{u}$ is defined in (3). Let

$$\zeta_i = -\sum_{k=1}^{l_i} u_{ik} \frac{M_{ik}(\eta)}{M_{i0}(\eta)} \quad (i = 0, 1, \dots, n). \tag{6}$$

We claim that $\theta = (\eta; \zeta_0, u_{01}, \dots, u_{0l_0}; \dots; \zeta_n, u_{n1}, \dots, u_{nl_n})$ is a generic zero of $\mathcal{I}_{\mathbb{Y},\mathbf{u}}$, which implies that $\mathcal{I}_{\mathbb{Y},\mathbf{u}}$ is a reflexive prime difference ideal.

Clearly, each $\mathrm{N}(\mathbb{P}_i)$ vanishes at θ. For any $f \in \mathcal{I}_{\mathbb{Y},\mathbf{u}}$, there exists an $M \in \mathbb{m}$ such that $Mf \in [\mathrm{N}(\mathbb{P}_0), \dots, \mathrm{N}(P_n)]$, so $f(\theta) = 0$ follows. Conversely, let f be any difference polynomial in $\mathbb{Q}\{\mathbb{Y}, \mathbf{u}_0, \dots, \mathbf{u}_n\}$ satisfying $f(\theta) = 0$. Clearly, $\mathrm{N}(\mathbb{P}_0), \mathrm{N}(\mathbb{P}_1), \dots, \mathrm{N}(\mathbb{P}_n)$ constitute an ascending chain with u_{i0} as leaders. Let f_1 be the difference remainder of f w.r.t. this ascending chain. Then f_1 is free from u_{i0} $(i = 0, \dots, n)$ and there exist $a, s \in \mathbb{N}$ such that $(\prod_{i=0}^n \prod_{l=0}^s (\sigma^l(\mathrm{I}_{\mathrm{N}(\mathbb{P}_i)})))^a \cdot f \equiv f_1, \mathrm{mod}[\mathrm{N}(\mathbb{P}_0), \dots, \mathrm{N}(P_n)]$. Clearly, $f_1(\theta) = 0$. Since $f_1 \in \mathbb{Q}\{\mathbb{Y}, \mathbf{u}\}$, $f_1 = 0$. Thus, $f \in \mathcal{I}_{\mathbb{Y},\mathbf{u}}$. So $\mathcal{I}_{\mathbb{Y},\mathbf{u}}$ is a reflexive prime difference ideal with a generic zero θ.

Consequently, $\mathcal{I}_{\mathbf{u}} = \mathcal{I}_{\mathbb{Y},\mathbf{u}} \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$ is a reflexive prime difference ideal with a generic zero $\zeta = (\zeta_0, u_{01}, \dots, u_{0l_0}; \dots; \zeta_n, u_{n1}, \dots, u_{nl_n})$. From (6), it is clear that $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle \zeta \rangle / \mathbb{Q} \le \sum_{i=0}^n l_i + n$. If there exist pairs (i_k, j_k) $(k = 1, \dots, n)$ with $1 \le j_k \le l_{i_k}$ and $i_{k_1} \neq i_{k_2}$ $(k_1 \neq k_2)$ such that $\frac{M_{i_1 j_1}}{M_{i_1 0}}, \dots, \frac{M_{i_n j_n}}{M_{i_n 0}}$ are transformally independent over $\mathbb{Q}$, then by Lemma 2, $\zeta_{i_1}, \dots, \zeta_{i_n}$ are transformally independent over $\mathbb{Q}\langle \mathbf{u} \rangle$. It follows that $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle \zeta \rangle / \mathbb{Q} = \sum_{i=0}^n l_i + n$. Thus, $\mathcal{I}_{\mathbf{u}}$ is of codimension 1.

Conversely, let us assume that $\mathcal{I}_{\mathbf{u}}$ is of codimension 1. That is, $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle \zeta \rangle / \mathbb{Q} = \sum_{i=0}^n l_i + n$. We want to show that there exist pairs (i_k, j_k) $(k = 1, \dots, n)$ with $1 \le j_k \le l_{i_k}$ and $i_{k_1} \neq i_{k_2}$ $(k_1 \neq k_2)$ such that $\frac{M_{i_1 j_1}}{M_{i_1 0}}, \dots, \frac{M_{i_n j_n}}{M_{i_n 0}}$ are transformally independent over $\mathbb{Q}$. Suppose the contrary, i.e., $\frac{M_{i_1 j_1}(\eta)}{M_{i_1 0}(\eta)}, \dots, \frac{M_{i_n j_n}(\eta)}{M_{i_n 0}(\eta)}$ are transformally dependent for any n different i_k and $j_k \in \{1, \dots, l_{i_k}\}$. Since each ζ_{i_k} is a linear combination of $\frac{M_{i_kj_k}(\eta)}{M_{i_k0}(\eta)}$ $(j_k = 1, \ldots, l_{i_k})$, it follows that $\zeta_{i_1}, \ldots, \zeta_{i_n}$ are transformally dependent over $\mathbb{Q}\langle\mathbf{u}\rangle$. Thus, we have $\sigma.\mathrm{tr}.\deg\mathbb{Q}\langle\zeta\rangle/\mathbb{Q} < \sum_{i=0}^{n} l_i + n$, a contradiction to the hypothesis. □

Let $[\mathbb{P}_0, \ldots, \mathbb{P}_n]$ be the difference ideal in $\mathbb{Q}\{\mathbb{Y}^{\pm}; \mathbf{u}_0, \ldots, \mathbf{u}_n\}$ generated by $\mathbb{P}_i$. Then we have

Corollary 14. $[\mathbb{P}_0, \ldots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\} = \mathcal{I}_{\mathbf{u}}$. *The reflexive prime difference ideal* $[\mathbb{P}_0, \ldots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$ *is of codimension one if and only if* $\{\mathbb{P}_i : i = 0, \ldots, n\}$ *is a Laurent transformally essential system.*

Proof. It is easy to show that $[\mathbb{P}_0, \ldots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\} = \mathcal{I}_{\mathbb{Y},\mathbf{u}} \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\} = \mathcal{I}_{\mathbf{u}}$. And the result is a direct consequence of Theorem 13. □

Now suppose $\{\mathbb{P}_0, \ldots, \mathbb{P}_n\}$ is a Laurent transformally essential system. Since $\mathcal{I}_{\mathbf{u}}$ defined in (5) is a reflexive prime difference ideal of codimension one, by Theorem 7, there exists a unique irreducible difference polynomial $\mathbf{R}(\mathbf{u}; u_{00}, \ldots, u_{n0}) = \mathbf{R}(\mathbf{u}_0, \ldots, \mathbf{u}_n) \in \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$ such that $\mathbf{R}$ can serve as the first polynomial in each characteristic set of $\mathcal{I}_{\mathbf{u}}$ w.r.t. any ranking endowed on $\mathbf{u}_0, \ldots, \mathbf{u}_n$. That is, if u_{ij} appears in $\mathbf{R}$, then among all the difference polynomials in $\mathcal{I}_{\mathbf{u}}$, $\mathbf{R}$ is of minimal order in u_{ij} and of minimal degree in the maximal transform of u_{ij}.

Now the definition of the sparse difference resultant is given as follows:

Definition 15. The above $\mathbf{R}(\mathbf{u}_0, \ldots, \mathbf{u}_n) \in \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$ is defined to be the *sparse difference resultant* of the Laurent transformally essential system $\mathbb{P}_0, \ldots, \mathbb{P}_n$, denoted by $\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n}$ or $\mathrm{Res}(\mathbb{P}_0, \ldots, \mathbb{P}_n)$.

The following lemma gives another description of the sparse difference resultant from the perspective of generic zeros.

Lemma 16. *Let* $\zeta_i = -\sum_{k=1}^{l_i} u_{ik} \frac{M_{ik}(\eta)}{M_{i0}(\eta)}$ $(i = 0, 1, \ldots, n)$ *be defined as in Eq.* (6), *where* $\eta = (\eta_1, \ldots, \eta_n)$ *is a generic zero of* $[0]_{\mathbb{Q}\langle\mathbf{u}\rangle\{\mathbb{Y}\}}$. *Then, among all the polynomials in* $\mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$ *vanishing at* $(\mathbf{u}; \zeta_0, \ldots, \zeta_n)$, $\mathbf{R}(\mathbf{u}_0, \ldots, \mathbf{u}_n) = \mathbf{R}(\mathbf{u}; u_{00}, \ldots, u_{n0})$ *is of minimal order in each* u_{i0} *and of minimal degree in the maximal transform of* u_{i0}.

Proof. It is a direct consequence of Theorem 13 and Definition 15. □

Remark 17. From its definition, the sparse difference resultant can be computed as follows. With the characteristic set method given in Gao et al. (2009), we can compute a proper irreducible ascending chain $\mathcal{A}$ which is a characteristic set for the difference polynomial system $\{\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_n\}$ under a ranking such that $u_{ij} < y_k$. Then the first difference polynomial in $\mathcal{A}$ is the sparse difference resultant. This algorithm does not have a complexity analysis. In Section 5, we will give a single exponential algorithm to compute the sparse difference resultant.

We give several examples which will be used throughout the paper.

Example 18. Let $n = 1$ and $\mathbb{P}_0 = u_{00} + u_{01}y_1^2$, $\mathbb{P}_1 = u_{10}y_1^{(1)} + u_{11}y_1$. Clearly, $\mathbb{P}_0, \mathbb{P}_1$ are Laurent transformally essential. The sparse difference resultant of $\mathbb{P}_0, \mathbb{P}_1$ is

$$\mathbf{R} = u_{10}^2 u_{01} u_{00}^{(1)} - u_{11}^2 u_{00} u_{01}^{(1)}.$$

Example 19. Let $n = 2$ and the $\mathbb{P}_i$ have the form

$$\mathbb{P}_i = u_{i0}y_1^{(2)} + u_{i1}y_1^{(3)} + u_{i2}y_2^{(3)} \quad (i = 0, 1, 2).$$

It is easy to show that $y_1^{(3)}/y_1^{(2)}$ and $y_2^{(3)}/y_1^{(2)}$ are transformally independent over $\mathbb{Q}$. Thus, $\mathbb{P}_0$, $\mathbb{P}_1$, $\mathbb{P}_2$ form a Laurent transformally essential system. The sparse difference resultant is

$$\mathbf{R} = \mathrm{Res}(\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2) = \begin{vmatrix} u_{00} & u_{01} & u_{02} \\ u_{10} & u_{11} & u_{12} \\ u_{20} & u_{21} & u_{22} \end{vmatrix}.$$

The following example shows that for a Laurent transformally essential system, its sparse difference resultant may not involve the coefficients of some $\mathbb{P}_i$.

Example 20. Let $n = 2$ and the $\mathbb{P}_i$ have the form

$$\mathbb{P}_0 = u_{00} + u_{01} y_1 y_2, \qquad \mathbb{P}_1 = u_{10} + u_{11} y_1^{(1)} y_2^{(1)}, \qquad \mathbb{P}_2 = u_{20} + u_{21} y_2.$$

Clearly, $\mathbb{P}_0$, $\mathbb{P}_1$, $\mathbb{P}_2$ form a Laurent transformally essential system. The sparse difference resultant of $\mathbb{P}_0$, $\mathbb{P}_1$, $\mathbb{P}_2$ is

$$\mathbf{R} = u_{00}^{(1)} u_{11} - u_{01}^{(1)} u_{10},$$

which is free from the coefficients of $\mathbb{P}_2$.

Example 20 can be used to illustrate the difference between the differential and difference cases. If $\mathbb{P}_0$, $\mathbb{P}_1$, $\mathbb{P}_2$ in Example 20 are differential polynomials, then the sparse differential resultant is $u_{01}^2 u_{10} u_{20}^2 u_{21}^2 - u_{01} u'_{00} u_{11} u_{20} u_{21}^2 u'_{20} + u_{00} u'_{01} u_{11} u_{20} u_{21}^2 u'_{20} + u_{01} u_{00} u_{11} u_{20}^2 \ (u'_{21})^2 + u_{00} u_{01} u_{11} u_{21}^2 (u'_{20})^2 - 2 u_{01} u_{00} u_{11} u_{20} u_{21} u'_{20} u'_{21} + u_{01} u'_{00} u_{11} u_{20}^2 u'_{21} u_{21} - u_{00} u'_{01} u_{11} \ u_{21} u'_{21} u_{20}^2$ which contains all the coefficients of $\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2$.

Remark 21. When all the $\mathcal{A}_i$ $(i = 0, \ldots, n)$ are sets of difference monomials, unless explicitly mentioned, we always consider $\mathbb{P}_i$ as Laurent difference polynomials. But when we regard $\mathbb{P}_i$ as difference polynomials, $\mathrm{Res}_{\mathcal{A}_0, \ldots, \mathcal{A}_n}$ is also called the sparse difference resultant of the difference polynomials $\mathbb{P}_i$ and we call $\mathbb{P}_i$ a *transformally essential system*. In this paper, sometimes we regard $\mathbb{P}_i$ as difference polynomials where it will be indicated.

We now define sparse difference resultants for specific Laurent difference polynomials over Laurent transformally essential systems. For any finite set $\mathcal{A} = \{M_0, \ldots, M_l\}$ of Laurent difference monomials in $\mathbb{Y}$ and a difference extension field $\mathcal{E}$ of $\mathbb{Q}$, we use

$$\mathcal{L}_{\mathcal{E}}(\mathcal{A}) = \left\{ \sum_{i=0}^{l} a_i M_i \right\} \tag{7}$$

to denote the set of all Laurent difference polynomials with support $\mathcal{A}$, where $a_i \in \mathcal{E}$.

Definition 22. Let $\mathcal{A}_i = \{M_{i0}, M_{i1}, \ldots, M_{il_i}\}$ $(i = 0, 1, \ldots, n)$ be a Laurent transformally essential system. Consider $n+1$ Laurent difference polynomials $(F_0, F_1, \ldots, F_n) \in \prod_{i=0}^{n} \mathcal{L}_{\mathcal{E}}(\mathcal{A}_i)$. The sparse difference resultant of $F_0, \ldots, F_n$, denoted as $\mathrm{Res}(F_0, \ldots, F_n)$, is obtained by replacing $\mathbf{u}_i$ with the corresponding coefficient vector of F_i in $\mathrm{Res}_{\mathcal{A}_0, \ldots, \mathcal{A}_n}$.

A major unsolved problem about difference resultant is whether $\mathbf{R}$ defined above contains all the information about the elimination ideal $\mathcal{I}_{\mathbf{u}}$ defined in (5). More precisely, we propose the following problem.

Problem 23. As shown by Example 3, the characteristic set for a reflexive prime difference ideal of codimension one could contain more than one elements. Let $\mathcal{I}_{\mathbf{u}}$ be the ideal defined in (5). Then $\mathcal{I}_{\mathbf{u}}$ is a reflexive prime difference ideal of codimension one and

$$\mathcal{I}_{\mathbf{u}} = \mathcal{I}_{\mathbb{Y},\mathbf{u}} \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\} = \mathrm{sat}(\mathbf{R}, R_1, \ldots, R_m), \tag{8}$$

where $\mathbf{R}$ is the sparse difference resultant of $\{\mathbb{P}_0, \ldots, \mathbb{P}_n\}$ and $\mathbf{R}, R_1, \ldots, R_m$ is a characteristic set of $\mathcal{I}_{\mathbf{u}}$. We conjecture that $m = 0$, or equivalently $\mathcal{I}_{\mathbf{u}} = \mathrm{sat}(\mathbf{R})$. If this is valid, then better properties can be shown for sparse difference resultants as we will explain later. It is easy to check that for Examples 18, 19, and 20, $\mathcal{I}_{\mathbf{u}} = \mathrm{sat}(\mathbf{R})$.

3.3. A criterion for Laurent transformally essential system in terms of supports

Let $\mathcal{A}_i$ $(i = 0, \ldots, n)$ be finite sets of Laurent difference monomials. According to Definition 11, in order to check whether they form a Laurent transformally essential system, we need to check whether there exist $M_{ik_i}, M_{ij_i} \in \mathcal{A}_i$ $(i = 0, \ldots, n)$ such that $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle M_{0k_0}/M_{0j_0}, \ldots, M_{nk_n}/M_{nj_n}\rangle/\mathbb{Q} = n$. This can be done with the difference characteristic set method given in Gao et al. (2009). In this section, a criterion will be given to check whether a Laurent difference system is transformally essential in terms of their supports, which is conceptually and computationally simpler than the naive approach based on the difference characteristic set method.

Let $B_i = \prod_{j=1}^n \prod_{k=0}^s (y_j^{(k)})^{t_{ijk}}$ $(i = 1, \ldots, m)$ be m Laurent difference monomials. We now introduce a new algebraic indeterminate x and let

$$d_{ij} = \sum_{k=1}^{s} t_{ijk} x^k \quad (i = 1, \ldots, m, j = 1, \ldots, n)$$

be univariate polynomials in $\mathbb{Z}[x]$. If $\mathrm{ord}(B_i, y_j) = -\infty$, then set $d_{ij} = 0$. The vector $(d_{i1}, d_{i2}, \ldots, d_{in})$ is called the *symbolic support vector* of B_i. The matrix $\mathrm{D} = (d_{ij})_{m\times n}$ is called the *symbolic support matrix* of $B_1, \ldots, B_m$.

Note that there is a one-to-one correspondence between Laurent difference monomials and their symbolic support vectors, so we will not distinguish these two concepts if there is no confusion. The same is true for a set of Laurent difference monomials and its symbolic support matrix.

Definition 24. A matrix $\mathrm{D} = (d_{ij})_{m\times n}$ over $\mathbb{Q}[x]$ is called *normal upper-triangular of rank r* if for each $i \le r$, $d_{ii} \ne 0$ and $d_{i,i-k} = 0$ $(1 \le k \le i-1)$, and the last $m - r$ rows are zero vectors.

Definition 25. A *generalized Laurent difference monomial* is a monomial of the form $\prod_{j=1}^n \prod_{k=0}^s (y_j^{(k)})^{t_{jk}}$ where $t_{jk} \in \mathbb{Q}$. A set of generalized Laurent difference monomials $B_1, B_2, \ldots, B_m$ is said to be in *r-upper-triangular* form if its symbolic support matrix $\mathrm{D} \in \mathbb{Q}[x]^{m\times n}$ is a normal upper triangular matrix of rank r.

The following lemma shows that it is easy to compute the difference transcendence degree of a set of Laurent difference monomials in upper-triangular form.

Lemma 26. *Let $B_1, \ldots, B_m$ be a set of generalized Laurent difference monomials in r-upper-triangular form. Then $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_1, \ldots, B_m\rangle/\mathbb{Q} = r$.*

Proof. From the structure of the symbolic support matrix, $B_i = \prod_{j=i}^n \prod_{k\ge 0} (y_j^{(k)})^{t_{ijk}}$ $(i = 1, \ldots, r)$ with $\mathrm{ord}(B_i, y_i) \ge 0$ and $B_{r+1} = \cdots = B_m = 1$. Let $B_i' = \prod_{j=i}^r \prod_{k\ge 0} (y_j^{(k)})^{t_{ijk}}$ and $\mathbb{Q}_1 = \mathbb{Q}\langle y_{r+1}, \ldots, y_n\rangle$. Then $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_1, \ldots, B_m\rangle/\mathbb{Q} = \sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_1, \ldots, B_r\rangle/\mathbb{Q} \ge \sigma.\mathrm{tr}.\deg \mathbb{Q}_1\langle B_1, \ldots, B_r\rangle/\mathbb{Q}_1 = \sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_1', \ldots, B_r'\rangle/\mathbb{Q}$. So it suffices to show that $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_1', \ldots, B_r'\rangle/\mathbb{Q} = r$.

If $r = 1$, $\mathrm{ord}(B_1', y_1) \ge 0$ implies that $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_1'\rangle/\mathbb{Q} = 1$. Suppose we have proved for the case $r - 1$. Let $B_i'' = \prod_{j=i}^{r-1} \prod_{k\ge 0} (y_j^{(k)})^{d_{ijk}}$, then by the hypothesis, $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_1'', \ldots, B_{r-1}''\rangle/\mathbb{Q} = r - 1$. Since $B_r' \in \mathbb{Q}\langle y_r\rangle$, $r \ge \sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_1', \ldots, B_r'\rangle/\mathbb{Q} = \sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_1', \ldots, B_r'\rangle/\mathbb{Q}\langle B_r'\rangle + \sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_r'\rangle/\mathbb{Q} \ge \sigma.\mathrm{tr}.\deg \mathbb{Q}\langle y_r\rangle\langle B_1', \ldots, B_{r-1}'\rangle/\mathbb{Q}\langle y_r\rangle + 1 = \sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_1'', \ldots, B_{r-1}''\rangle/\mathbb{Q} + 1 = r$. So $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_1, \ldots, B_m\rangle/\mathbb{Q} = r$. □

In the following, we will show that each set of generalized Laurent difference monomials can be transformed to an upper-triangular set with the same transformal transcendence degree. For a matrix D over $\mathbb{Q}[x]$, we use two types of elementary row operations and one type of elementary column operation on D, namely,

- interchanging two rows of D;
- adding an $f(x)$-multiple of the j-th row to the i-th row, where $f(x) \in \mathbb{Q}[x]$ and $i \neq j$;
- interchanging two columns of D.

Lemma 27. *Each matrix $\mathrm{D} \in \mathbb{Q}[x]^{m\times n}$ can be reduced to a normal upper-triangular matrix by performing a finite succession of the above three types of elementary operations.*

Proof. Since $\mathbb{Q}[x]$ is an Euclidean domain, it follows by Hoffman and Kunze (1971, p. 253). □

Theorem 28. *Let $B_1, \dots, B_m$ be a set of Laurent difference monomials with symbolic support matrix D. Then $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_1, \dots, B_m\rangle/\mathbb{Q} = \mathrm{rk}(\mathrm{D})$.*

Proof. First, we show that the above three types of elementary operations of D correspond to certain transformations of $B_1, \dots, B_m$. Indeed, interchanging the i-th and the j-th rows of D means interchanging B_i and B_j, and interchanging the i-th and the j-th columns of D means interchanging y_i and y_j in $B_1, \dots, B_m$ (or in the variable order). Multiplying the i-th row of D by a polynomial $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in \mathbb{Q}[x]$ and adding the result to the j-th row means changing B_j to $\prod_{k=0}^{d}(\sigma^k(B_i))^{a_k} B_j$.

So by Lemma 27, $B_1, \dots, B_m$ can be transformed to an upper-triangular set $C_1, \dots, C_m$ by just performing a finite succession of the above three types of elementary operations. If we can show that the above elementary matrix operations keep transformal transcendence degree, then by Lemma 26, the theorem follows. It is trivial for row or column interchanging operations. So it suffices to show that given $\sum_{k=0}^{d} a_i x^k \in \mathbb{Q}[x]^*$, $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_1, B_2\rangle/\mathbb{Q} = \sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_1, \prod_{k=0}^{d}(\sigma^k(B_1))^{a_k} B_2\rangle/\mathbb{Q}$. It can easily be proved, for we have $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle B_1\rangle/\mathbb{Q} = \sigma.\mathrm{tr}.\deg \mathbb{Q}\langle \prod_{k=0}^{d}(\sigma^k(B_1))^{a_k}\rangle/\mathbb{Q}$. □

Example 29. Let $B_1 = y_1 y_2$ and $B_2 = y_1^{(a)} y_2^{(b)}$. Then the symbolic support matrix of B_1 and B_2 is $\mathrm{D} = \left(\begin{smallmatrix} 1 & 1 \\ x^a & x^b \end{smallmatrix}\right)$. Then $\mathrm{rk}(\mathrm{D}) = \left\{\begin{smallmatrix} 1 \text{ if } a=b \\ 2 \text{ if } a\neq b \end{smallmatrix}\right.$. Thus, by Theorem 28, if $a \neq b$, B_1 and B_2 are transformally independent over $\mathbb{Q}$. Otherwise, they are transformally dependent over $\mathbb{Q}$.

We now extend Theorem 28 to generic difference polynomials in (2). Let $I \subseteq \{0, \dots, n\}$ and for any $i \in I$, let β_{ik} be the symbolic support vector of M_{ik}/M_{i0}. Then the vector

$$w_i = \sum_{k=0}^{l_i} u_{ik}\beta_{ik}$$

is called the *symbolic support vector* of $\mathbb{P}_i$ and the matrix D_I whose rows are w_i for $i \in I$ is called the *symbolic support matrix* of $\mathbb{P}_i$ $(i \in I)$. Then we have the following lemma.

Lemma 30. $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle \bigcup_{i\in I} \mathbf{u}_i\rangle\langle \mathbb{P}_i/M_{i0} : i \in I\rangle/\mathbb{Q}\langle \bigcup_{i\in I} \mathbf{u}_i\rangle = \mathrm{rk}(\mathrm{D}_I)$.

Proof. By Lemma 2, $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle \bigcup_{i\in I} \mathbf{u}_i\rangle\langle \mathbb{P}_i/M_{i0} : i \in I\rangle/\mathbb{Q}\langle \bigcup_{i\in I} \mathbf{u}_i\rangle$ is no less than the maximal transformal transcendence degree of M_{ik_i}/M_{i0} over $\mathbb{Q}$.

On the other hand, the transformal transcendence degree will not increase by linear combinations, for given arbitrary a_i and $\bar{a}_1$, $\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle\lambda\rangle\langle a_1 + \lambda\bar{a}_1, a_2, \dots, a_k\rangle/\mathbb{Q}\langle\lambda\rangle \le \max(\sigma.\mathrm{tr}.\deg \mathbb{Q}\langle a_1, a_2 \dots, a_k\rangle/\mathbb{Q}, \sigma.\mathrm{tr}.\deg \mathbb{Q}\langle \bar{a}_1, a_2, \dots, a_k\rangle/\mathbb{Q})$. So the transformal transcendence degree of $\mathbb{P}_i/M_{i0}$ $(i \in I)$ over $\mathbb{Q}\langle \bigcup_{i\in I} \mathbf{u}_i\rangle$ is no greater than the maximal transformal transcendence degree of M_{ik_i}/M_{i0} $(i \in I)$.

Thus, by Theorem 28, we have $\sigma.\mathrm{tr}.\deg\mathbb{Q}\langle\bigcup_{i\in I}\mathbf{u}_i\rangle\langle\mathbb{P}_i/M_{i0} : i \in I\rangle/\mathbb{Q}\langle\bigcup_{i\in I}\mathbf{u}_i\rangle = \max_{k_i}\sigma.\mathrm{tr}.\deg\mathbb{Q}\langle M_{ik_i}/M_{i0} : i \in I\rangle/\mathbb{Q} = \max_{k_i}\mathrm{rk}(\mathrm{D}_{k_i,i\in I})$, where $\mathrm{D}_{k_i,i\in I}$ is the symbolic support matrix of M_{ik_i}/M_{i0}. Denote the submatrix of D_I with rows corresponding to $\mathbb{P}_{i_1}/M_{i_10}, \dots, \mathbb{P}_{i_r}/M_{i_r0}$ and columns corresponding to $y_{j_1}, \dots, y_{j_r}$ by $\mathrm{D}_I\binom{i_1\dots i_r}{j_1\dots j_r}$. Then $\det\big(\mathrm{D}_I\binom{i_1\dots i_r}{j_1\dots j_r}\big) = \sum_{k_i}\prod_{j=1}^{r}u_{i_jk_j} \times \det\big(\mathrm{D}_{k_i,i\in I}\binom{i_1\dots i_r}{j_1\dots j_r}\big)$, which implies that $\mathrm{rk}(\mathrm{D}_I) = \max_{k_i}\mathrm{rk}(\mathrm{D}_{k_i,i\in I})$. Thus, the lemma follows. □

Now, we have the following criterion for Laurent transformally essential system.

Theorem 31. *Consider the set of generic Laurent difference polynomials defined in (2). The following three conditions are equivalent.*

(1) $\mathbb{P}_0, \dots, \mathbb{P}_n$ *form a Laurent transformally essential system.*
(2) *There exist* M_{ik_i} $(i = 0, \dots, n)$ *with* $1 \le k_i \le l_i$ *such that the symbolic support matrix of* $M_{0k_0}/M_{00}, \dots, M_{nk_n}/M_{n0}$ *is of rank* n.
(3) *The symbolic support matrix* $\mathrm{D}_{\mathbb{P}}$ *of* $\mathbb{P}_0, \dots, \mathbb{P}_n$ *is of full rank, that is,* $\mathrm{rk}(\mathrm{D}_{\mathbb{P}}) = n$.

Proof. The equivalence of 1) and 2) is a direct consequence of Theorem 28 and Definition 11. The equivalence of 1) and 3) follows from Lemma 30. □

Both Theorems 28 and 31 can be used to check whether a system is transformally essential.

Example 32. In Example 20, let $B_0 = M_{01}/M_{00} = y_1y_2$, $B_1 = M_{11}/M_{10} = y_1^{(1)}y_2^{(1)}$, and $B_2 = M_{21}/M_{20} = y_2$. Then the symbolic support matrix for $\{B_0, B_2\}$ is $D = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. We have $\mathrm{rk}(D) = 2$ and by Theorem 28, the system $\mathbb{P} = \{\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2\}$ is transformally essential. Also, the symbolic support matrix for $\mathbb{P}$ is $\mathrm{D}_{\mathbb{P}} = \begin{pmatrix} u_{01} & u_{01} \\ u_{11}x & u_{11}x \\ 0 & u_{21} \end{pmatrix}$. We have $\mathrm{rk}(\mathrm{D}_{\mathbb{P}}) = 2$ and by Theorem 31, $\mathbb{P}$ is transformally essential.

We end this section by introducing a new concept, namely super-essential systems, through which one can identify certain $\mathbb{P}_i$ whose coefficients will not occur in the sparse difference resultant. This will lead to the simplification in the computation of the resultant. Let $I \subset \{0, 1, \dots, n\}$. We denote by $\mathbb{P}_I$ the Laurent difference polynomial set consisting of $\mathbb{P}_i$ $(i \in I)$, and $\mathrm{D}_{\mathbb{P}_I}$ its symbolic support matrix. For a subset $I \subset \{0, 1, \dots, n\}$, if $|I| = \mathrm{rk}(\mathrm{D}_{\mathbb{P}_I})$, then $\mathbb{P}_I$, or $\{\mathcal{A}_i : i \in I\}$, is said to be *transformally independent.*

Definition 33. Let $I \subset \{0, 1, \dots, n\}$. We call I or $\mathbb{P}_I$ *super-essential* if $|I| - \mathrm{rk}(\mathrm{D}_{\mathbb{P}_I}) = 1$ and for each proper subset $J \subsetneq I$, $|J| = \mathrm{rk}(\mathrm{D}_{\mathbb{P}_J})$.

Note that super-essential systems are the difference analogue of essential systems introduced in Sturmfels (1994) and also that of rank essential systems introduced in Li et al. (2012). Using this definition, we have the following property, which is similar to Corollary 1.1 in Sturmfels (1994).

Theorem 34. *If* $\{\mathbb{P}_0, \dots, \mathbb{P}_n\}$ *is a Laurent transformally essential system, then for any* $I \subset \{0, 1, \dots, n\}$, $|I| - \mathrm{rk}(\mathrm{D}_{\mathbb{P}_I}) \le 1$ *and there exists a unique I which is super-essential. If I is super-essential, then the sparse difference resultant of* $\mathbb{P}_0, \dots, \mathbb{P}_n$ *involves only the coefficients of* $\mathbb{P}_i$ $(i \in I)$.

Proof. Since $n = \mathrm{rk}(\mathrm{D}_{\mathbb{P}}) \le \mathrm{rk}(\mathrm{D}_{\mathbb{P}_I}) + |\mathbb{P}| - |\mathbb{P}_I| = n + 1 + \mathrm{rk}(\mathrm{D}_{\mathbb{P}_I}) - |I|$, we have $|I| - \mathrm{rk}(\mathrm{D}_{\mathbb{P}_I}) \le 1$. Since $|I| - \mathrm{rk}(\mathrm{D}_{\mathbb{P}_I}) \ge 0$, for any I, either $|I| - \mathrm{rk}(\mathrm{D}_{\mathbb{P}_I}) = 0$ or $|I| - \mathrm{rk}(\mathrm{D}_{\mathbb{P}_I}) = 1$. Using the fact that $|\{0, 1, \dots, n\}| - \mathrm{rk}(\mathrm{D}_{\mathbb{P}}) = n$, it is easy to check the existence of a rank essential set I. For the uniqueness, we assume that there exist two subsets $I_1, I_2 \subset \{1, \dots, m\}$ which are super-essential. Then, we have $\mathrm{rk}(\mathrm{D}_{\mathbb{P}_{I_1\cup I_2}}) \le \mathrm{rk}(\mathrm{D}_{\mathbb{P}_{I_1}}) + \mathrm{rk}(\mathrm{D}_{\mathbb{P}_{I_2}}) - \mathrm{rk}(\mathrm{D}_{\mathbb{P}_{I_1\cap I_2}}) = |I_1 \cup I_2| - 2$, a contradiction.

Let I be a super-essential set. Similar to the proof of Theorem 13, it is easy to show that $[\mathbb{P}_i]_{i\in I} \cap \mathbb{Q}\{\mathbf{u}_i\}_{i\in I}$ is of codimension one, which means that the sparse difference resultant of $\mathbb{P}_0, \ldots, \mathbb{P}_n$ only involves the coefficients of $\mathbb{P}_i$ $(i \in I)$. □

4. Basic properties of sparse difference resultants

In this section, we will prove some basic properties for the sparse difference resultant.

4.1. Transformal homogeneity and the action of the transforming operator

We first introduce the concept of transformally homogeneous polynomials.

Definition 35. A difference polynomial $f \in \mathcal{F}\{y_0, \ldots, y_n\}$ is called *transformally homogeneous* if for a new difference indeterminate λ, there exists a difference monomial $M(\lambda)$ in λ such that $f(\lambda y_0, \ldots, \lambda y_n) = M(\lambda) f(y_0, \ldots, y_n)$.

The difference analogue of Euler's criterion for homogeneous polynomials is valid.

Lemma 36. *$f \in \mathcal{F}\{y_0, y_1, \ldots, y_n\}$ is transformally homogeneous if and only if for each $r \in \mathbb{N}_0$, there exists $m_r \in \mathbb{N}_0$ such that*

$$\sum_{i=0}^{n} y_i^{(r)} \frac{\partial f(y_0, \ldots, y_n)}{\partial y_i^{(r)}} = m_r f.$$

That is, f is transformally homogeneous if and only if f is homogeneous in $\{y_1^{(r)}, \ldots, y_n^{(r)}\}$ for each $r \in \mathbb{N}_0$.

Proof. "$\Longrightarrow$" Denote $\mathbb{Y} = (y_0, \ldots, y_n)$ temporarily. Suppose f is transformally homogeneous. That is, there exists a difference monomial $M(\lambda) = \prod_{r=0}^{r_0} (\lambda^{(r)})^{m_r}$ such that $f(\lambda\mathbb{Y}) = M(\lambda) f(\mathbb{Y})$. Then $\sum_{i=0}^{n} y_i^{(r)} \frac{\partial f}{\partial y_i^{(r)}}(\lambda\mathbb{Y}) = \sum_{i=0}^{n} \frac{\partial f}{\partial y_i^{(r)}}(\lambda\mathbb{Y}) \frac{\partial(\lambda y_i)^{(r)}}{\partial\lambda^{(r)}} = \frac{\partial f(\lambda\mathbb{Y})}{\partial\lambda^{(r)}} = \frac{\partial M(\lambda) f(\mathbb{Y})}{\partial\lambda^{(r)}} = \frac{m_r M(\lambda)}{\lambda^{(r)}} f(\mathbb{Y})$. Substitute $\lambda = 1$ into the above equality, $\sum_{i=0}^{n} y_i^{(r)} \frac{\partial f}{\partial y_j^{(r)}} = m_r f$ follows.

"$\Longleftarrow$" Suppose $\operatorname{ord}(f, \mathbb{Y}) = r_0$. Then for each $r \le r_0, \lambda^{(r)} \frac{\partial f(\lambda\mathbb{Y})}{\partial\lambda^{(r)}} = \lambda^{(r)} \sum_{i=0}^{n} y_i^{(r)} \frac{\partial f}{\partial y_i^{(r)}}(\lambda\mathbb{Y}) = \sum_{i=0}^{n} (\lambda y_i)^{(r)} \frac{\partial f}{\partial y_i^{(r)}}(\lambda\mathbb{Y}) = m_r f(\lambda\mathbb{Y})$. So $f(\lambda\mathbb{Y})$ is homogeneous of degree m_r in $\lambda^{(r)}$. Thus, $f(\lambda\mathbb{Y}) = f(\lambda y_0, \ldots, \lambda y_n; \lambda^{(1)} y_0^{(1)}, \ldots, \lambda^{(1)} y_n^{(1)}; \ldots; \lambda^{(r_0)} y_0^{(r_0)}, \ldots, \lambda^{(r_0)} y_n^{(r_0)}) = \prod_{r=0}^{r_0} (\lambda^{(r)})^{m_r} f(\mathbb{Y})$. Thus, f is transformally homogeneous. □

Theorem 37. *The sparse difference resultant is transformally homogeneous in each $\mathbf{u}_i$ which is the coefficient set of $\mathbb{P}_i$.*

Proof. Suppose $\operatorname{ord}(\mathbf{R}, \mathbf{u}_i) = h_i \ge 0$. Follow the notations used in Theorem 13. By Lemma 16, $\mathbf{R}(\mathbf{u}; \zeta_0, \ldots, \zeta_n) = 0$. Differentiating this identity w.r.t. $u_{ij}^{(k)}$ $(j = 1, \ldots, l_i)$ respectively, due to (6) we have

$$\overline{\frac{\partial\mathbf{R}}{\partial u_{ij}^{(k)}}} + \overline{\frac{\partial\mathbf{R}}{\partial u_{i0}^{(k)}}} \left(-\frac{M_{ij}(\eta)}{M_{i0}(\eta)}\right)^{(k)} = 0. \tag{9}$$

In the above equations, $\overline{\frac{\partial\mathbf{R}}{\partial u_{ij}^{(k)}}}$ $(k = 0, \ldots, h_i; j = 0, \ldots, l_i)$ are obtained by replacing u_{i0} by ζ_i $(i = 0, 1, \ldots, n)$ in each $\frac{\partial\mathbf{R}}{\partial u_{ij}^{(k)}}$ respectively.

Multiplying (9) by $u_{ij}^{(k)}$ and for j from 1 to l_i, adding them together, we get $\zeta_i^{(k)}\overline{\frac{\partial \mathbf{R}}{\partial u_{i0}^{(k)}}} + \sum_{j=1}^{l_i} u_{ij}^{(k)}\overline{\frac{\partial \mathbf{R}}{\partial u_{ij}^{(k)}}} = 0$. So the difference polynomial $f_k = \sum_{j=0}^{l_i} u_{ij}^{(k)}\frac{\partial \mathbf{R}}{\partial u_{ij}^{(k)}}$ vanishes at $(\zeta_0, \ldots, \zeta_n)$. Since $\mathrm{ord}(f_k, u_{i0}) \le \mathrm{ord}(\mathbf{R}, u_{i0})$ and $\deg(f_k) = \deg(\mathbf{R})$, by Lemma 16, there exists an $m_k \in \mathbb{Z}$ such that $f_k = m_k\mathbf{R}$. Thus, by Lemma 36, $\mathbf{R}$ is transformally homogeneous in $\mathbf{u}_i$. □

The following result shows that if we regard Res as a map from Laurent difference polynomial systems to their sparse difference resultants, it satisfies $\mathrm{Res} \circ \sigma = \sigma \circ \mathrm{Res}$.

Theorem 38. *Let $\mathbb{P}_0, \ldots, \mathbb{P}_n$ be a Laurent transformally essential system as defined in (2). Then* $\mathrm{Res}(\sigma(\mathbb{P}_0), \ldots, \sigma(\mathbb{P}_n)) = \sigma(\mathrm{Res}(\mathbb{P}_0, \ldots, \mathbb{P}_n))$.

Proof. Since $\mathbb{P}_i = \sum_{k=0}^{n} u_{ik}M_{ik}$, $\sigma(\mathbb{P}_i) = \sum_{k=0}^{n} \sigma(u_{ik})\sigma(M_{ik})$. Clearly, $\sigma(\mathbb{P}_i)$ is a generic sparse Laurent difference polynomial with coefficient vector $\sigma(\mathbf{u}_i) = (\sigma(u_{i0}), \ldots, \sigma(u_{il_i}))$. Denote $\mathbb{P}^\sigma = \{\sigma(\mathbb{P}_0), \ldots, \sigma(\mathbb{P}_n)\}$. It is easy to show that the symbolic support matrix of $\mathbb{P}^\sigma$ is $\mathrm{D}_{\mathbb{P}^\sigma} = \mathrm{diag}(x, \ldots, x) \cdot \mathrm{D}_{\mathbb{P}}$. So $\mathbb{P}^\sigma$ is also a Laurent transformally essential system and its sparse difference resultant exists. Thus, $\mathcal{I}_1 = [\mathbb{P}^\sigma] \cap \mathbb{Q}\{\sigma(\mathbf{u}_0), \ldots, \sigma(\mathbf{u}_n)\} = \mathrm{sat}(\mathrm{Res}(\sigma(\mathbb{P}_0), \ldots, \sigma(\mathbb{P}_n)), \ldots)$.

Let $\mathbb{H}_i = \sum_{k=0}^{n} \sigma(u_{ik})M_{ik}$. Since each $\mathbb{H}_i$ has the same support with $\mathbb{P}_i$ and its coefficient vector is $\sigma(\mathbf{u}_i)$, $\mathrm{Res}(\mathbb{H}_0, \ldots, \mathbb{H}_n) = \sigma(\mathrm{Res}(\mathbb{P}_0, \ldots, \mathbb{P}_n))$. Let $\mathcal{I}_2 = [\mathbb{H}_0, \ldots, \mathbb{H}_n] \cap \mathbb{Q}\{\sigma(\mathbf{u}_0), \ldots, \sigma(\mathbf{u}_n)\}$. We claim that $\mathcal{I}_1 = \mathcal{I}_2$, which implies that $\mathrm{Res}(\mathbb{H}_0, \ldots, \mathbb{H}_n) = \mathrm{Res}(\sigma(\mathbb{P}_0), \ldots, \sigma(\mathbb{P}_n))$ and the lemma follows.

Let $\xi_i = -\sum_{k=0}^{n} \sigma(u_{ik})\sigma(M_{ik}/M_{i0})$, $\theta_i = -\sum_{k=0}^{n} \sigma(u_{ik})M_{ik}/M_{i0}$ and denote $\hat{\mathbf{u}} = \bigcup_{i=0}^{n} \sigma(\mathbf{u}_i) \setminus \{\sigma(u_{i0})\}$. As in the proof of Theorem 13, we can show that $\xi = (\hat{\mathbf{u}}, \xi_0, \ldots, \xi_n)$ is a generic point of $\mathcal{I}_1$ and $\theta = (\hat{\mathbf{u}}, \theta_0, \ldots, \theta_n)$ is a generic point of $\mathcal{I}_2$. For any difference polynomial $G \in \mathcal{I}_1$, $G(\xi) = 0 = (\sum_\phi \phi(\sigma(\mathbb{Y}))F_\phi(\mathbf{u}))/M(\sigma(\mathbb{Y}))$ where ϕ and M are distinct difference monomials in $\sigma(\mathbb{Y})$. Then $F_\phi(\mathbf{u}) \equiv 0$ for each ϕ. Thus, $G(\theta) = (\sum_\phi \phi(\mathbb{Y})F_\phi(\mathbf{u}))/M(\mathbb{Y}) = 0$ and $G \in \mathcal{I}_2$ follows. So $\mathcal{I}_1 \subseteq \mathcal{I}_2$. Similarly, we can show that $\mathcal{I}_2 \subseteq \mathcal{I}_1$. Hence, $\mathcal{I}_1 = \mathcal{I}_2$. So $\mathrm{Res}(\sigma(\mathbb{P}_0), \ldots, \sigma(\mathbb{P}_n)) = \sigma(\mathrm{Res}(\mathbb{P}_0, \ldots, \mathbb{P}_n))$. □

4.2. Existence of nonzero solutions and incompleteness of difference projective space

In this section, we first give a condition for a system of Laurent difference polynomials to have nonzero solutions in terms of sparse difference resultants, and then show that the difference projective space is not transformally complete.

To be more precise, we first introduce some notations. Let $\mathcal{F}$ be a difference field and $\mathfrak{C}_\mathcal{F}$ the category of difference extension fields of $\mathcal{F}$, where the morphisms are the difference homomorphisms. By $\mathcal{E} \in \mathfrak{C}_\mathcal{F}$, we mean $\mathcal{E}$ is a difference extension field of $\mathcal{F}$.

Let $\mathcal{A} = \{M_0, M_1, \ldots, M_l\}$ be a Laurent monomial set. For any $\mathcal{E} \in \mathfrak{C}_\mathbb{Q}$, there is a one to one correspondence between $\mathcal{L}_\mathcal{E}(\mathcal{A})$ defined in (7) and $\mathcal{E}^{l+1}$. For $P = \sum_{i=0}^{l} c_iM_i \in \mathcal{L}_\mathcal{E}(\mathcal{A})$, denote the coefficient vector of P by $\mathbb{C}(P) = (c_0, \ldots, c_l) \in \mathcal{E}^{l+1}$. Conversely, for any $\mathbf{c} = (c_0, \ldots, c_l) \in \mathcal{E}^{l+1}$, denote the corresponding Laurent difference polynomial by $\mathbb{L}(\mathbf{c}) = \sum_{i=0}^{l} c_iM_i \in \mathcal{E}\{\mathbb{Y}^\pm\}$.

Let $\mathcal{A}_0, \ldots, \mathcal{A}_n$ be a Laurent transformally essential system of Laurent monomials and $\mathcal{E} \in \mathfrak{C}_\mathbb{Q}$. Clearly, each element $(P_0, \ldots, P_n) \in \mathcal{L}_\mathcal{E}(\mathcal{A}_0) \times \cdots \times \mathcal{L}_\mathcal{E}(\mathcal{A}_n)$ can be represented by one and only one element $(\mathbb{C}(P_0), \ldots, \mathbb{C}(P_n)) \in \hat{\mathcal{E}} = \mathcal{E}^{l_0+1} \times \cdots \times \mathcal{E}^{l_n+1}$. Let $\mathcal{Z}(\mathcal{A}_0, \ldots, \mathcal{A}_n)$ be the functor from $\mathfrak{C}_\mathbb{Q}$ to the category of sets such that for each $\mathcal{E} \in \mathfrak{C}_\mathbb{Q}$,

$$\mathcal{Z}_\mathcal{E}(\mathcal{A}_0, \ldots, \mathcal{A}_n) := \Big\{(\mathbf{v}_0, \ldots, \mathbf{v}_n) \in \hat{\mathcal{E}} \mid \mathbb{L}(\mathbf{v}_0) = \cdots = \mathbb{L}(\mathbf{v}_n) = 0 \\ \text{has common nonzero solutions for } \mathbb{Y}\Big\}.$$

Similarly, given $\mathcal{S} \subset \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$, we define the *difference variety* $\mathbb{V}(\mathcal{S})$ over $\mathbb{Q}$ as a functor from $\mathfrak{C}_\mathbb{Q}$ to the category of sets such that for each $\mathcal{E} \in \mathfrak{C}_\mathbb{Q}$,

$$\mathbb{V}_\mathcal{E}(\mathcal{S}) := \Big\{(\mathbf{v}_0, \ldots, \mathbf{v}_n) \in \hat{\mathcal{E}} \mid f(\mathbf{v}_0, \ldots, \mathbf{v}_n) = 0, \forall f \in \mathcal{S}\Big\}.$$

For two functors X and Y from $\mathfrak{C}_{\mathcal{F}}$ to the category of sets, we write $X \subseteq Y$ to indicate that X is a subfunctor of Y. Namely, $X_{\mathcal{E}} \subseteq Y_{\mathcal{E}}$ for every $\mathcal{E} \in \mathfrak{C}_{\mathcal{F}}$. The following result shows that the vanishing of the sparse difference resultant gives a necessary condition for the existence of nonzero solutions.

Lemma 39. *$\mathcal{Z}(\mathcal{A}_0, \ldots, \mathcal{A}_n) \subseteq \mathbb{V}(\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n})$, where $\mathbb{V}(\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n})$ is a difference variety over $\mathbb{Q}$.*

Proof. Let $\mathbb{P}_0, \ldots, \mathbb{P}_n$ be a generic Laurent transformally essential system corresponding to $\mathcal{A}_0, \ldots, \mathcal{A}_n$ with coefficient vectors $\mathbf{u}_0, \ldots, \mathbf{u}_n$. By Definition 15, $\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n} \in [\mathbb{P}_0, \ldots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$. For each $\mathcal{E} \in \mathfrak{C}_{\mathbb{Q}}$ and any point $(\mathbf{v}_0, \ldots, \mathbf{v}_n) \in \mathcal{Z}_{\mathcal{E}}(\mathcal{A}_0, \ldots, \mathcal{A}_n)$, let $(\overline{\mathbb{P}}_0, \ldots, \overline{\mathbb{P}}_n) \in \mathcal{L}_{\mathcal{E}}(\mathcal{A}_0) \times \cdots \times \mathcal{L}_{\mathcal{E}}(\mathcal{A}_n)$ be the system represented by $(\mathbf{v}_0, \ldots, \mathbf{v}_n)$. Since $\overline{\mathbb{P}}_0, \ldots, \overline{\mathbb{P}}_n$ have a common nonzero solution, $\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n}(\mathbf{v}_0, \ldots, \mathbf{v}_n) = 0$. So $\mathcal{Z}_{\mathcal{E}}(\mathcal{A}_0, \ldots, \mathcal{A}_n) \subseteq \mathbb{V}_{\mathcal{E}}(\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n})$. Thus, $\mathcal{Z}(\mathcal{A}_0, \ldots, \mathcal{A}_n) \subseteq \mathbb{V}(\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n})$ follows. □

Example 40. In Example 19, suppose $\mathcal{F} = \mathbb{Q}(x)$ and $\sigma f(x) = f(x+1)$. Then we have $\mathrm{Res}(\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2) \neq 0$. But $y_1 = 0$, $y_2 = 0$ constitute a zero solution of $\mathbb{P}_0 = \mathbb{P}_1 = \mathbb{P}_2 = 0$. This shows that Lemma 39 is not correct if we do not consider nonzero solutions.

The following theorem shows that a particular principal component of the sparse difference resultant gives a sufficient and necessary condition for a Laurent transformally essential system to have nonzero solutions in a certain sense.

Theorem 41. *Let $\mathcal{I}_{\mathbf{u}} = [\mathbb{P}_0, \ldots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\} = \mathrm{sat}(\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n}, R_1, \ldots, R_m)$ as defined in (8). Let $\overline{\mathcal{Z}(\mathcal{A}_0, \ldots, \mathcal{A}_n)}$ be the Cohn topological closure[1] of $\mathcal{Z}(\mathcal{A}_0, \ldots, \mathcal{A}_n)$ over $\mathbb{Q}$, that is, the minimal difference variety $\mathbb{V}$ over $\mathbb{Q}$ containing $\mathcal{Z}(\mathcal{A}_0, \ldots, \mathcal{A}_n)$. Then $\overline{\mathcal{Z}(\mathcal{A}_0, \ldots, \mathcal{A}_n)} = \mathbb{V}(\mathrm{sat}(\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n}, R_1, \ldots, R_m))$.*

Proof. Similarly to the proof of Lemma 39, we can show $\mathcal{I}_{\mathbf{u}}$ vanishes at $\mathcal{Z}_{\mathcal{E}}(\mathcal{A}_0, \ldots, \mathcal{A}_n)$ for each $\mathcal{E} \in \mathfrak{C}_{\mathbb{Q}}$. So $\overline{\mathcal{Z}(\mathcal{A}_0, \ldots, \mathcal{A}_n)} \subseteq \mathbb{V}(\mathrm{sat}(\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n}, R_1, \ldots, R_m))$.

For the other direction, follow notations in the proof of Theorem 13. By Theorem 13, $\mathcal{I}_{\mathbb{Y},\mathbf{u}}$ is a reflexive prime difference ideal with a generic point (η, ζ) where $\eta = (\eta_1, \ldots, \eta_n)$ is a generic point of $[0]_{\mathbb{Q}\langle\mathbf{u}\rangle\{\mathbb{Y}\}}$ and $\zeta = (\zeta_0, u_{01}, \ldots, u_{0l_0}; \ldots; \zeta_n, u_{n1}, \ldots, u_{nl_n})$. Let $(F_0, \ldots, F_n) \in \mathcal{L}_{\mathcal{E}}(\mathcal{A}_0) \times \cdots \times \mathcal{L}_{\mathcal{E}}(\mathcal{A}_n)$ be a set of Laurent difference polynomials represented by ζ where $\mathcal{E} = \mathbb{Q}\langle\zeta\rangle$. Clearly, η is a nonzero solution of $F_i = 0$. Thus, $\zeta \in \mathcal{Z}_{\mathcal{E}}(\mathcal{A}_0, \ldots, \mathcal{A}_n)$. Since ζ is a generic point of $\mathrm{sat}(\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n}, R_1, \ldots, R_m)$, we have $\mathbb{V}(\mathrm{sat}(\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n}, R_1, \ldots, R_m)) \subseteq \overline{\mathcal{Z}(\mathcal{A}_0, \ldots, \mathcal{A}_n)}$ and the theorem is proved. □

Remark 42. If Problem 23 can be solved positively, then the vanishing of $\mathrm{sat}(\mathbf{R})$ also gives a sufficient condition for $\mathbb{P}_0 = \cdots = \mathbb{P}_n = 0$ to have a nonzero solution in the sense of Cohn topological closure. That is, $\overline{\mathcal{Z}(\mathcal{A}_0, \ldots, \mathcal{A}_n)} = \mathbb{V}(\mathrm{sat}(\mathbf{R}))$.

The following example shows that the vanishing of the sparse difference resultant is not a sufficient condition for the given system to have common nonzero solutions.

Example 43. In Example 18, consider the specialized system $\overline{\mathbb{P}}_0 = y_1^2 - 1, \overline{\mathbb{P}}_1 = y_1^{(1)} + y_1$. From Example 18, it can be checked that $\mathrm{Res}(\overline{\mathbb{P}}_0, \overline{\mathbb{P}}_1) = 0$, but $\overline{\mathbb{P}}_0 = \overline{\mathbb{P}}_1 = 0$ has no solutions. Note that in this example, $\mathcal{I}_{\mathbf{u}} = \mathrm{sat}(\mathbf{R})$. Theorem 41 shows that $\mathcal{Z}(\mathcal{A}_0, \ldots, \mathcal{A}_n)$ is dense in $\mathbb{V}(\mathrm{sat}(\mathbf{R}))$. This example shows that for certain $\mathcal{A}_i$, $\mathcal{Z}(\mathcal{A}_0, \ldots, \mathcal{A}_n)$ is a proper subset of $\mathbb{V}(\mathrm{sat}(\mathbf{R}))$.

In the following, Example 43 is used to show that the difference projective space is not transformally complete. Before giving the main result, we introduce some basic notions.

[1] For rigorous definition, see Wibmer (2013).

Definition 44. The *difference projective (n-)space* over $\mathcal{F}$ is the functor $\mathbf{P}^n$ from $\mathfrak{C}_\mathcal{F}$ to the category of sets such that for each $\mathcal{E} \in \mathfrak{C}_\mathcal{F}$, $\mathbf{P}^n(\mathcal{E})$ is the projective $(n\text{-})$space over $\mathcal{E}$. Let $\mathcal{S}$ be a set of transformally homogenous difference polynomials in $\mathcal{F}\{z_0, \dots, z_n\}$. The subfunctor functor $\mathbb{V}(\mathcal{S})$ of $\mathbf{P}^n$ given by $\mathbb{V}_\mathcal{E}(\mathcal{S}) = \{\mathbf{a} \in \mathbf{P}^n(\mathcal{E}) \mid f(\mathbf{a}) = 0,\ \forall f \in \mathcal{S}\}$ is called a *projective difference variety over* $\mathcal{F}$.

More generally, given $n_1, \dots, n_p \in \mathbb{N}$, we define the p-difference projective space $\mathbf{P}^{n_1} \times \cdots \times \mathbf{P}^{n_p}$ over $\mathcal{F}$ as the functor mapping each $\mathcal{E} \in \mathfrak{C}_\mathcal{F}$ to $\mathbf{P}^{n_1}(\mathcal{E}) \times \cdots \times \mathbf{P}^{n_p}(\mathcal{E})$. Let $(z_{ij})_{1 \le i \le p, 0 \le j \le n_i}$ be a family of difference indeterminates over $\mathcal{F}$, set $\mathbf{z}_i = (z_{i0}, \dots, z_{in_i})$ and consider the difference polynomial ring $\mathcal{F}\{\mathbf{z}_1, \dots, \mathbf{z}_p\}$. Let $f \in \mathcal{F}\{\mathbf{z}_1, \dots, \mathbf{z}_p\}$. If for each index i, f is transformally homogenous in $\mathbf{z}_i$, f is said to be *transformally* p*-homogenous* in $\mathbf{z}_1, \dots, \mathbf{z}_p$. A *projective difference zero* of f is a point $(\mathbf{a}_1, \dots, \mathbf{a}_p) \in \mathbf{P}^{n_1}(\mathcal{E}) \times \cdots \times \mathbf{P}^{n_p}(\mathcal{E})$ such that $f(\mathbf{a}_1, \dots, \mathbf{a}_p) = 0$. A subfunctor $V \subset \mathbf{P}^{n_1} \times \cdots \times \mathbf{P}^{n_p}$ is called a *difference variety* over $\mathcal{F}$ if there exists a set of transformally p-homogenous polynomials $\mathcal{S} \subset \mathcal{F}\{\mathbf{z}_1, \dots, \mathbf{z}_p\}$ such that $V = \mathbb{V}(\mathcal{S})$. And by $V_\mathcal{E}$, we mean $\mathbb{V}_\mathcal{E}(\mathcal{S})$. If for each $\mathcal{E} \in \mathfrak{C}_\mathcal{F}$, $V_\mathcal{E} = \emptyset$, then we simply denote $V = \emptyset$.

Definition 45. A projective difference variety $V \subset \mathbf{P}^n$ over $\mathcal{F}$ is said to be transformally complete if the projection $\pi : \mathbf{P}^m \times V \to \mathbf{P}^m$ is transformally closed in the following sense: for each projective difference variety $W \subset \mathbf{P}^m \times V$ over $\mathcal{F}$, there exists a projective difference variety $\mathbb{V}(\mathcal{S}) \subset \mathbf{P}^m$ for $\mathcal{S} \subset \mathcal{F}\{z_0, z_1, \dots, z_m\}$ such that for each $\mathcal{E} \in \mathfrak{C}_\mathcal{F}$, $\mathbf{a} \in \mathbb{V}_\mathcal{E}(\mathcal{S})$ if and only if $\mathbf{a} \in \pi(W_{\mathcal{E}_1})$ for some difference extension field $\mathcal{E}_1$ of $\mathcal{E}$.

For convenience, $\mathbb{V}(\mathcal{S})$ that corresponds to W in Definition 45 is denoted by $\overline{\pi(W)}$. The following result shows that the projective space is not transformally complete.

Theorem 46. $\mathbf{P}^1$ *over* $\mathcal{F}$ *is not transformally complete.*[2]

Proof. Suppose $\mathbf{P}^1$ is transformally complete. Consider $\pi : \mathbf{P}^1 \times \mathbf{P}^1 \to \mathbf{P}^1$, where the coordinate ring of the first $\mathbf{P}^1$ is $\mathcal{F}\{y_0, y_1\}$ and the coordinate ring of the second $\mathbf{P}^1$ is $\mathcal{F}\{z_0, z_1\}$. Let $W = \mathbb{V}(y_0 y_1^{(1)} - y_1 y_0^{(1)}, z_1^2 y_0 - y_1 z_0^2, z_0 z_1^{(1)} + z_1 z_0^{(1)}) \subset \mathbf{P}^1 \times \mathbf{P}^1$. Let β be an algebraic transcendental element over $\mathcal{F}$. We adjoin $\sqrt{\beta}$ to $\mathcal{F}$ by defining $\sigma(\beta) = \beta$ and $\sigma(\sqrt{\beta}) = -\sqrt{\beta}$. Then $\mathcal{F}_1 = \mathcal{F}(\sqrt{\beta}) \in \mathfrak{C}_\mathcal{F}$. Clearly, $(1, \beta; 1, \sqrt{\beta}) \in W_{\mathcal{F}_1}$. So $W \neq \emptyset$.

For transformally homogenous difference polynomials $\mathbb{P}_i(z_0, z_1)$ $(i = 0, 1)$ in z_0 and z_1, define the sparse difference resultant of $\mathbb{P}_0, \mathbb{P}_1$ as $\mathrm{Res}(\mathbb{P}_0(1, z_1), \mathbb{P}_1(1, z_1))$. If we regard $z_1^2 y_0 - y_1 z_0^2, z_0 z_1^{(1)} + z_1 z_0^{(1)}$ as transformally homogenous difference polynomials in z_0, z_1 with y_0, y_1 as coefficients, then, by Example 18, $y_0 y_1^{(1)} - y_1 y_0^{(1)}$ is the sparse difference resultant of $z_1^2 y_0 - y_1 z_0^2, z_0 z_1^{(1)} + z_1 z_0^{(1)}$. Since $\mathbf{P}^1$ is assumed to be transformally complete, it is easy to show $\overline{\pi(W)} = \mathbb{V}(y_0 y_1^{(1)} - y_1 y_0^{(1)})$. This is equivalent to say that a specialized system of $z_1^2 y_0 - y_1 z_0^2, z_0 z_1^{(1)} + z_1 z_0^{(1)}$ has a common projective difference zero in z_0, z_1 if and only if the sparse difference resultant vanishes. But Example 43 shows this is impossible. Indeed, since $(1, 1) \in \mathbb{V}_\mathcal{F}(y_0 y_1^{(1)} - y_1 y_0^{(1)})$, $(1, 1) \in \pi_\mathcal{E}(W)$ for some $\mathcal{E} \in \mathfrak{C}_\mathcal{F}$. That is, there exists $(b_0, b_1) \in \mathbf{P}^1(\mathcal{E})$ such that $(1, 1; b_0, b_1) \in W_\mathcal{E}$. By Example 43, $b_1^2 - b_0^2 = 0, b_0 b_1^{(1)} + b_1 b_0^{(1)} = 0$ have no solution in $\mathbf{P}^1(\mathcal{E})$ for any $\mathcal{E} \in \mathfrak{C}_\mathcal{F}$, a contradiction. Thus, $\mathbf{P}^1$ is not transformally complete. □

4.3. Order and effective order bounds in terms of Jacobi numbers

In this section, we will give order and effective order bounds for the sparse difference resultant in terms of the Jacobi number of the given system.

[2] The theorem also holds in the case $\mathrm{char}(\mathcal{F}) = p \neq 0$. Since this paper only concerns the case of characteristic zero, we will not give the proof.

Consider a generic Laurent transformally essential system $\{\mathbb{P}_0, \dots, \mathbb{P}_n\}$ defined in (2) with $\mathbf{u}_i = (u_{i0}, u_{i1}, \dots, u_{il_i})$ being the coefficient vector of $\mathbb{P}_i$ $(i = 0, \dots, n)$. Suppose $\mathbf{R}$ is the sparse difference resultant of $\mathbb{P}_0, \dots, \mathbb{P}_n$. Denote $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i)$ to be the maximal order of $\mathbf{R}$ in u_{ik} $(k = 0, \dots, l_i)$, that is, $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) = \max_k \mathrm{ord}(\mathbf{R}, u_{ik})$. If $\mathbf{u}_i$ does not occur in $\mathbf{R}$, then set $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) = -\infty$. First, we have the following result.

Lemma 47. *If* $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) = h_i \geq 0$*, then* $\mathrm{ord}(\mathbf{R}, u_{ik}) = h_i$ *for each* $k = 0, \dots, l_i$.

Proof. First, for each $k \in \{1, \dots, l_i\}$, by differentiating $\mathbf{R}(\mathbf{u}; \zeta_0, \dots, \zeta_n) = 0$ w.r.t. $u_{ik}^{(h_i)}$, we have $\frac{\partial \mathbf{R}}{\partial u_{ik}^{(h_i)}}(\mathbf{u}, \zeta_0, \dots, \zeta_n) + \frac{\partial \mathbf{R}}{\partial u_{i0}^{(h_i)}}(\mathbf{u}, \zeta_0, \dots, \zeta_n)(-\frac{M_{ik}(\eta)}{M_{i0}(\eta)})^{(h_i)} = 0$. Suppose $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) = \mathrm{ord}(\mathbf{R}, u_{ik_0}) = h_i$. If $k_0 = 0$, then $\frac{\partial \mathbf{R}}{\partial u_{i0}^{(h_i)}}(\mathbf{u}, \zeta_0, \dots, \zeta_n) \neq 0$ by Lemma 16. So $\frac{\partial \mathbf{R}}{\partial u_{ik}^{(h_i)}} \neq 0$. Thus, $\mathrm{ord}(\mathbf{R}, u_{ik}) = h_i$ for each k. If $k_0 \neq 0$, then $\frac{\partial \mathbf{R}}{\partial u_{ik_0}^{(h_i)}}(\mathbf{u}, \zeta_0, \dots, \zeta_n) \neq 0$ and $\frac{\partial \mathbf{R}}{\partial u_{i0}^{(h_i)}} \neq 0$ follows. So by the case $k_0 = 0$, for each k, $\mathrm{ord}(\mathbf{R}, u_{ik}) = h_i$. □

Let $B = (b_{ij})$ be an $n \times n$ matrix where b_{ij} is an integer or $-\infty$. A *diagonal sum* of B is any sum $\sum_{i=1}^{n} b_{i\sigma(i)}$ with σ a permutation of $1, \dots, n$. Suppose A is an $m \times n$ matrix. Let $k = \min\{m, n\}$. A diagonal sum of A is a diagonal sum of any $k \times k$ submatrix of A. The *Jacobi number* of A is the maximal diagonal sum of A, denoted by $\mathrm{Jac}(A)$.

Let $s_{ij} = \mathrm{ord}(\mathrm{N}(\mathbb{P}_i), y_j)$ $(i = 0, \dots, n; j = 1, \dots, n)$ and $s_i = \mathrm{ord}(\mathrm{N}(\mathbb{P}_i))$. We call the $(n+1) \times n$ matrix $A = (s_{ij})$ the *order matrix* of $\mathbb{P}_0, \dots, \mathbb{P}_n$. By $A_{\hat{i}}$, we mean the submatrix of A obtained by deleting the $(i+1)$-th row from A. We use $\mathrm{N}(\mathbb{P})$ to denote the set $\{\mathrm{N}(\mathbb{P}_0), \dots, \mathrm{N}(\mathbb{P}_n)\}$ and by $\mathrm{N}(\mathbb{P})_{\hat{i}}$, we mean the set $\mathrm{N}(\mathbb{P}) \backslash \{\mathrm{N}(\mathbb{P}_i)\}$. We call $\mathrm{J}_i = \mathrm{Jac}(A_{\hat{i}})$ the *Jacobi number* of the system $\mathrm{N}(\mathbb{P})_{\hat{i}}$, also denoted by $\mathrm{Jac}(\mathrm{N}(\mathbb{P})_{\hat{i}})$. The following result shows that the order of a difference system is closely related with its Jacobi number.

Theorem 48. *(See Hrushovski, 2004.) Let* $S = \{f_1, \dots, f_n\} \subset \mathcal{F}\{\mathbb{Y}\}$ *be a system of difference polynomials over* $\mathcal{F}$ *and* $\mathcal{I} \subset \mathcal{F}\{\mathbb{Y}\}$ *a reflexive prime difference ideal minimal over the perfect difference ideal generated by* S*. If* $\mathcal{I}$ *is of dimension zero, then the order of* $\mathcal{I}$ *is bounded by* $\mathrm{Jac}(S)$.

Before giving an order bound for the sparse difference resultant in terms of Jacobi numbers, we first need several lemmas.

Lemma 49. *(See Cohn, 1983; Lando, 1970.) Let* A *be an* $m \times n$ *matrix whose entries are* 0*'s and* 1*'s. Let* $\mathrm{Jac}(A) = J < \min\{m, n\}$*. Then* A *contains an* $a \times b$ *zero sub-matrix with* $a + b = m + n - J$.

Lemma 50. *Let* $\mathbb{P}$ *be a Laurent transformally essential system with the following* $(n+1) \times n$ *order matrix*

$$\mathbf{A} = \begin{pmatrix} A_{11} & (-\infty)_{r \times t} \\ A_{21} & A_{22} \end{pmatrix},$$

where $r + t \geq n + 1$*. Then* $r + t = n + 1$ *and* $\mathrm{Jac}(A_{22}) \geq 0$*. Moreover, when regarded as difference polynomials in* $y_1, \dots, y_{r-1}$*,* $\{\mathbb{P}_0, \dots, \mathbb{P}_{r-1}\}$ *is Laurent transformally essential.*

Proof. The structure of A implies that the symbolic support matrix (for definition, see Section 3.3) of $\mathbb{P}$ has the following form:

$$\mathrm{D}_{\mathbb{P}} = \begin{pmatrix} B_{11} & 0_{r \times t} \\ B_{21} & B_{22} \end{pmatrix}.$$

Since $\mathbb{P}$ is Laurent transformally essential, by Theorem 31, $\mathrm{rk}(\mathrm{D}_{\mathbb{P}}) = n$. As $\mathrm{rk}(\mathrm{D}_{\mathbb{P}}) \leq \mathrm{rk}(B_{11}) + \mathrm{rk}((B_{21}\ \ B_{22})) \leq (n - t) + (n + 1 - r) = 2n + 1 - (r + t)$, $r + t \leq n + 1$. Thus, $r + t = n + 1$ follows. Since the above inequality becomes equality, B_{11} has full column rank. As a consequence,

$\mathrm{rk}(\mathrm{D}_{\mathbb{P}}) = \mathrm{rk}(B_{11}) + \mathrm{rk}(B_{22})$. Hence, B_{22} is a $t \times t$ nonsingular matrix. Regarding $\mathbb{P}_0, \ldots, \mathbb{P}_{r-1}$ as difference polynomials in $y_1, \ldots, y_{r-1}$, then B_{11} is the symbolic support matrix of $\{\mathbb{P}_0, \ldots, \mathbb{P}_{r-1}\}$ which is of full rank. Thus, $\{\mathbb{P}_0, \ldots, \mathbb{P}_{r-1}\}$ is a Laurent transformally essential system.

It remains to show that $\mathrm{Jac}(A_{22}) \geq 0$. Suppose the contrary, i.e. $\mathrm{Jac}(A_{22}) = -\infty$. Let $\bar{A}_{22}$ be a $t \times t$ matrix obtained from A_{22} by replacing $-\infty$ by 0 and replacing all the other elements in A_{22} by 1's. Then $\mathrm{Jac}(\bar{A}_{22}) < t$, and by Lemma 49, $\bar{A}_{12}$ contains an $a \times b$ zero submatrix with $a+b = 2t - \mathrm{Jac}(\bar{A}_{22}) \geq t+1$. By interchanging rows and columns when necessary, suppose such a zero submatrix is in the upper-right corner of $\bar{A}_{22}$. Then

$$A_{22} = \begin{pmatrix} C_{11} & (-\infty)_{a\times b} \\ C_{21} & C_{22} \end{pmatrix} \quad \text{and} \quad B_{22} = \begin{pmatrix} D_{11} & 0_{a\times b} \\ D_{21} & D_{22} \end{pmatrix},$$

where $a+b \geq t+1$. So $\mathrm{rk}(B_{22}) \leq (t-b)+(t-a) \leq t-1$ which implies that B_{22} is singular, a contradiction. So $\mathrm{Jac}(A_{22}) \geq 0$. □

The following theorem gives an order bound for the sparse difference resultant in terms of Jacobi numbers, which is the first main result in this section.

Theorem 51. *Let $\mathbb{P}$ be a Laurent transformally essential system and* $\mathbf{R}$ *the sparse difference resultant of $\mathbb{P}$. Then*[3] $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) \leq \mathrm{J}_i$.

Proof. Without loss of generality, we prove $\mathrm{ord}(\mathbf{R}, \mathbf{u}_0) \leq \mathrm{J}_0$. Two cases are considered:

Case 1) $\mathrm{J}_0 = -\infty$. We need to show that $\mathrm{ord}(\mathbf{R}, \mathbf{u}_0) = -\infty$. Since $\mathrm{J}_0 = -\infty$, by Lemma 49, the order matrix of $\mathrm{N}(\mathbb{P})_{\hat{0}}$ has an $r \times t$ submatrix $(-\infty)_{r\times t}$ with $r+t \geq n+1$. By Lemma 50, $\mathbb{P}$ contains a proper Laurent transformally essential subsystem $\{\mathbb{P}_{j_1}, \ldots, \mathbb{P}_{j_r}\} \subset \mathbb{P}\backslash\{\mathbb{P}_0\}$. So the unique super-essential subsystem of $\mathbb{P}$ is contained in $\mathbb{P}\backslash\{\mathbb{P}_0\}$. Thus, by Theorem 34, $\mathbf{R}$ does not involve the coefficients of $\mathbb{P}_0$. Thus, $\mathrm{ord}(\mathbf{R}, \mathbf{u}_0) = -\infty$ follows.

Case 2) $\mathrm{J}_0 \geq 0$. If $\mathrm{ord}(\mathbf{R}, \mathbf{u}_0) = -\infty$, it is trivial that $\mathrm{ord}(\mathbf{R}, \mathbf{u}_0) \leq \mathrm{J}_0$. Now suppose $\mathrm{ord}(\mathbf{R}, \mathbf{u}_0) \geq 0$. Denote $\tilde{\mathbf{u}} = \bigcup_{i=0}^{n} \mathbf{u}_i \backslash \{u_{i0}\}$ and $\hat{\mathbf{u}} = \tilde{\mathbf{u}} \cup \{u_{10}, \ldots, u_{n0}\}$. Let $\mathcal{J}_0 = ([\mathrm{N}(\mathbb{P}_1), \ldots, \mathrm{N}(\mathbb{P}_n)] : \mathbb{m})_{\mathbb{Q}\langle\tilde{\mathbf{u}}\rangle\{\mathbb{Y}, u_{10}, \ldots, u_{n0}\}}$. As in the proof of Theorem 13, it is easy to show that $\mathcal{J}_0$ is a reflexive prime difference ideal of dimension n. Since $\mathrm{ord}(\mathbf{R}, \mathbf{u}_0) \geq 0$, by Theorem 34, the unique super-essential subsystem of $\mathbb{P}$ contains $\mathbb{P}_0$. So the symbolic support matrix of $\mathrm{N}(\mathbb{P}_1), \ldots, \mathrm{N}(\mathbb{P}_n)$ is of full rank. For if not, there would be a super-essential system contained in $\{\mathbb{P}_1, \ldots, \mathbb{P}_n\}$, a contradiction. By Lemma 30, $\{u_{10}, \ldots, u_{n0}\}$ is a parametric set of $\mathcal{J}_0$. So $\mathcal{J} = [\mathcal{J}_0]_{\mathbb{Q}\langle\hat{\mathbf{u}}\rangle\{\mathbb{Y}\}}$ is a reflexive prime difference ideal of dimension 0. Since $\mathcal{J}$ is a component of the perfect difference ideal generated by $\mathrm{N}(\mathbb{P}_1), \ldots, \mathrm{N}(\mathbb{P}_n)$ in $\mathbb{Q}\langle\tilde{\mathbf{u}}\rangle\{\mathbb{Y}\}$, by Theorem 48, $\mathrm{ord}(\mathcal{J}) \leq \mathrm{J}_0$.

Suppose $\xi = (\xi_1, \ldots, \xi_n)$ is a generic point of $\mathcal{J}$. Let $\mathcal{I} = ([\mathcal{J}, \mathrm{N}(\mathbb{P}_0)] : \mathbb{m})_{\mathbb{Q}\langle\hat{\mathbf{u}}\rangle\{\mathbb{Y}, u_{00}\}}$ and $\zeta = -\sum_{k=1}^{l_0} u_{0k} M_{0k}(\xi)/M_{00}(\xi) \in \mathbb{Q}\langle\hat{\mathbf{u}}, \xi\rangle$. Then, (ξ, ζ) is a generic point of $\mathcal{I}$. Recall that $\mathcal{I}_{\mathbb{Y},\mathbf{u}} = ([\mathrm{N}(\mathbb{P}_0), \ldots, \mathrm{N}(\mathbb{P}_n)] : \mathbb{m})_{\mathbb{Q}\{\mathbb{Y}, \mathbf{u}_0, \ldots, \mathbf{u}_n\}}$ and $\mathcal{I}_{\mathbb{Y},\mathbf{u}} \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\} = \mathrm{sat}(\mathbf{R}, \ldots)$. Then $\mathcal{I} = [\mathcal{I}_{\mathbb{Y},\mathbf{u}}]_{\mathbb{Q}\langle\hat{\mathbf{u}}\rangle\{\mathbb{Y}, u_{00}\}}$. Since $\mathrm{ord}(\mathbf{R}, u_{00}) \geq 0$, $\mathcal{I}_{\mathbb{Y},\mathbf{u}} \cap \mathbb{Q}\{\hat{\mathbf{u}}\} = \{0\}$. So $\mathcal{I} \cap \mathbb{Q}\langle\hat{\mathbf{u}}\rangle\{u_{00}\} = \mathrm{sat}(\mathbf{R}, \ldots)$ which has a generic point ζ. Thus, by Cohn (1965, p. 79), $\mathrm{ord}(\mathbf{R}, u_{00}) = \mathrm{tr.deg}\, \mathbb{Q}\langle\hat{\mathbf{u}}, \zeta\rangle / \mathbb{Q}\langle\hat{\mathbf{u}}\rangle \leq \mathrm{tr.deg}\, \mathbb{Q}\langle\hat{\mathbf{u}}, \xi\rangle / \mathbb{Q}\langle\hat{\mathbf{u}}\rangle = \mathrm{ord}(\mathcal{J}) \leq \mathrm{J}_0$. □

Corollary 52. *Let $\mathbb{P}$ be a super-essential system. Then $\mathrm{J}_i \geq 0$ for $i = 0, \ldots, n$ and* $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) \leq \mathrm{J}_i$.

Proof. If $\mathrm{J}_i = -\infty$ for some i, as in the proof of Theorem 51, we can show that $\mathbb{P}$ contains a proper super-essential subsystem, a contradiction. Therefore, $\mathrm{J}_i \geq 0$ for $i = 0, \ldots, n$. By Theorem 51, for each i, $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) \leq \mathrm{J}_i$. □

Example 53. Let $n = 2$ and

[3] Here, if $\mathrm{J}_i = -\infty$, it means $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) = -\infty$.

$$\mathbb{P}_0 = u_{00} + u_{01} y_1 y_1^{(1)}, \qquad \mathbb{P}_1 = u_{10} + u_{11} y_1, \qquad \mathbb{P}_2 = u_{10} + u_{11} y_2^{(1)}.$$

The sparse resultant is $\mathbf{R} = u_{00}u_{11}u_{11}^{(1)} + u_{01}u_{10}u_{10}^{(1)}$. In this example, the order matrix of $\mathbb{P}$ is $A = \begin{pmatrix} 1 & -\infty \\ 0 & -\infty \\ -\infty & 1 \end{pmatrix}$. Thus $\mathrm{J}_0 = 1, \mathrm{J}_1 = 2, \mathrm{J}_2 = -\infty$. And $\mathrm{ord}(\mathbf{R}, \mathbf{u}_0) = 0 < \mathrm{J}_0, \mathrm{ord}(\mathbf{R}, \mathbf{u}_1) = 1 < \mathrm{J}_1, \mathrm{ord}(\mathbf{R}, \mathbf{u}_2) = -\infty$.

In the following, we give two improved order bounds based on the Jacobi bound given in Theorem 51.

For each $j \in \{1, \ldots, n\}$, let $\underline{o}_j = \min_i\{\mathrm{Lord}(\mathrm{N}(\mathbb{P}_i), y_j) \mid \mathrm{Lord}(\mathrm{N}(\mathbb{P}_i), y_j) \geq 0\}$. In other words, $\underline{o}_j$ is the smallest number such that $y_j^{(\underline{o}_j)}$ occurs in $\{\mathrm{N}(\mathbb{P}_0), \ldots, \mathrm{N}(\mathbb{P}_n)\}$. Denote $\underline{\gamma} = \sum_{j=1}^n \underline{o}_j$. Let $B = (s_{ij} - \underline{o}_j)$ be an $(n+1) \times n$ matrix. We call $\bar{\mathrm{J}}_i = \mathrm{Jac}(B_{\hat{i}}) = \mathrm{J}_i - \underline{\gamma}$ the *modified Jacobi number* of the system $\mathbb{P}_{\hat{i}}$. Then we have the following result.

Theorem 54. *Let $\mathbb{P}$ be a Laurent transformally essential system and $\mathbf{R}$ the sparse difference resultant of $\mathbb{P}$. Then for each i, $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) \leq \mathrm{J}_i - \underline{\gamma}$.*

Proof. It is trivial for the case $\underline{\gamma} = 0$. Now suppose $\underline{\gamma} > 0$. First, we perform the change of variables $\bar{y}_j = y_j^{(\underline{o}_j)}$ in $\mathbb{P}$ to reduce the problem to the case $\underline{\gamma} = 0$. Let $\hat{\mathbb{P}}_i$ be obtained from $\mathbb{P}_i$ by replacing $y_j^{(k)}$ by $y_j^{(k-\underline{o}_j)}$ $(j = 1, \ldots, n; k \geq \underline{o}_j)$ in $\mathbb{P}_i$ $(i = 0, \ldots, n)$ and denote $\hat{\mathbb{P}} = \{\hat{\mathbb{P}}_0, \ldots, \hat{\mathbb{P}}_n\}$. Since $\mathrm{D}_{\mathbb{P}} = \mathrm{D}_{\hat{\mathbb{P}}} \cdot \mathrm{diag}(x^{\underline{o}_1}, x^{\underline{o}_2}, \ldots, x^{\underline{o}_n})$, it implies that $\mathrm{rk}(\mathrm{D}_{\hat{\mathbb{P}}}) = \mathrm{rk}(\mathrm{D}_{\mathbb{P}}) = n$. Thus, $\mathcal{I} = [\hat{\mathbb{P}}] \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$ is a reflexive prime difference ideal of codimension 1. Recall that $\mathcal{I}_{\mathbf{u}} = [\mathbb{P}_0, \ldots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\} = \mathrm{sat}(\mathbf{R}, \ldots)$. We claim that $\mathcal{I} = \mathcal{I}_{\mathbf{u}}$, which implies that $\mathbf{R}$ is the sparse difference resultant of $\hat{\mathbb{P}}$.

Suppose $\mathbb{P}_i = u_{i0}M_{i0} + T_i$ and $\hat{\mathbb{P}}_i = u_{i0}\hat{M}_{i0} + \hat{T}_i$. Let $\zeta_i = -T_i/M_{i0}$ and $\theta_i = -\hat{T}_i/\hat{M}_{i0}$. Denote $\mathbf{u} = \bigcup_{i=0}^n \mathbf{u}_i \backslash \{u_{i0}\}$. As in the proof of Theorem 13, we can show that $\zeta = (\mathbf{u}, \zeta_0, \ldots, \zeta_n)$ is a generic point of $\mathcal{I}_{\mathbf{u}}$ and $\theta = (\mathbf{u}, \theta_0, \ldots, \theta_n)$ is a generic point of $\mathcal{I}$. For any difference polynomial $G \in \mathcal{I}_{\mathbf{u}}$, $G(\zeta) = 0 = (\sum \phi(\mathbb{Y})F_\phi(\mathbf{u}))/(\prod_{i=1}^n M_{i0}^{a_i})$ where $\phi(\mathbb{Y})$ are distinct difference monomials in $\mathbb{Y}$. Then $F_\phi(\mathbf{u}) \equiv 0$ for each ϕ. Thus, $G(\theta) = (\sum \hat{\phi}(\mathbb{Y})F_\phi(\mathbf{u}))/(\prod_{i=1}^n \hat{M}_{i0}^{a_i}) = 0$ and $G \in \mathcal{I}$ follows. So $\mathcal{I}_{\mathbf{u}} \subseteq \mathcal{I}$. In the similar way, we can show that $\mathcal{I} \subseteq \mathcal{I}_{\mathbf{u}}$. Hence, $\mathcal{I} = \mathcal{I}_{\mathbf{u}}$ and $\mathbf{R}$ is the sparse difference resultant of $\hat{\mathbb{P}}$. Since $\mathrm{Jac}(\hat{\mathbb{P}}_{\hat{i}}) = \mathrm{Jac}(\mathbb{P}_{\hat{i}}) - \underline{\gamma}$, by Theorem 51, the theorem is proved. □

Now, we assume that $\mathbb{P}$ is a Laurent transformally essential system which is not super-essential. By Theorem 34, $\mathbb{P}$ contains a unique super-essential sub-system $\mathbb{P}_I$. Without loss of generality, suppose $I = \{0, \ldots, r\}$ with $r < n$. Let A_I be the order matrix of $\mathbb{P}_I$ and for $i = 0, \ldots, r$, let $(A_I)_{\hat{i}}$ be the matrix obtained from A_I by deleting the $(i+1)$-th row. Note that $(A_I)_{\hat{i}}$ is an $r \times n$ matrix. Then we have the following result.

Theorem 55. *With the above notations, we have*

$$\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) = \begin{cases} h_i \leq \mathrm{Jac}((A_I)_{\hat{i}}) & i = 0, \ldots, r, \\ -\infty & i = r+1, \ldots, n. \end{cases}$$

Proof. It suffices to show that $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) \leq \mathrm{Jac}((A_I)_{\hat{i}})$ for $i = 0, \ldots, r$. Let $\mathbb{L}_i = u_{i0} + \sum_{j=1}^n u_{ij}y_j$ for $i = r+1, \ldots, n$. Since $\mathbb{P}_I$ is super essential, there exist $\frac{M_{ik_i}}{M_{i0}}$ $(i = 1, \ldots, r)$ such that their symbolic support matrix B is of full rank. Without loss of generality, we assume that the r-th principal submatrix of B is of full rank. Consider a new Laurent difference polynomial system $\widetilde{\mathbb{P}} = \mathbb{P}_I \cup \{\mathbb{L}_{r+1}, \ldots, \mathbb{L}_n\}$. This system is also Laurent transformally essential, since the symbolic support matrix of $\frac{M_{1k_1}}{M_{10}}, \ldots, \frac{M_{rk_r}}{M_{r0}}, y_{r+1}, \ldots, y_n$ is of full rank. Moreover, $\mathbb{P}_I$ is the unique rank-essential subsystem of $\widetilde{\mathbb{P}}$. So $\mathbf{R}$ is also the sparse difference resultant of $\widetilde{\mathbb{P}}$. Since the order vector of $\mathbb{L}_i$ is $(0, \ldots, 0)$

for $i = r+1, \ldots, n$, $\mathrm{Jac}(\widetilde{\mathbb{P}}_{\hat{i}}) = \mathrm{Jac}((A_I)_{\hat{i}})$ for $i = 0, \ldots, r$. By Theorem 51, $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) \le \mathrm{Jac}((A_I)_{\hat{i}})$ for $i = 0, \ldots, r$. □

Example 56. In Example 53, $I = \{0, 1\}$. Then $A_I = (1\ \ 0)^{\mathrm{T}}$. Thus $\mathrm{Jac}((A_I)_{\hat{0}}) = 0$, $\mathrm{Jac}((A_I)_{\hat{1}}) = 1$. For this example, the exact bounds are given: $\mathrm{ord}(\mathbf{R}, \mathbf{u}_0) = 0 = \mathrm{Jac}((A_I)_{\hat{0}})$, $\mathrm{ord}(\mathbf{R}, \mathbf{u}_1) = 1 = \mathrm{Jac}((A_I)_{\hat{1}})$, $\mathrm{ord}(\mathbf{R}, \mathbf{u}_2) = -\infty$.

We conclude this section by giving an improved Jacobi-type bound for the effective order of the sparse difference resultant.

Assume $\mathbb{P}$ is a Laurent transformally essential system whose sparse difference resultant is $\mathbf{R}$. By Lemma 47, $u_{i0}^{(s)}$ effectively appears in $\mathbf{R}$ if and only if $u_{ik}^{(s)}$ effectively appears in $\mathbf{R}$ for each $k \in \{0, \ldots, l_i\}$. Thus, we can define $\mathrm{Lord}(\mathbf{R}, \mathbf{u}_i) = \mathrm{Lord}(\mathbf{R}, u_{i0})$ and $\mathrm{Eord}(\mathbf{R}, \mathbf{u}_i) = \mathrm{ord}(\mathbf{R}, \mathbf{u}_i) - \mathrm{Lord}(\mathbf{R}, \mathbf{u}_i)$ whenever $\mathbf{u}_i$ effectively appears in $\mathbf{R}$.

For further discussion, suppose $\mathbb{P}_I$ is the super-essential subsystem of $\{\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_n\}$. Without loss of generality, assume $I = \{0, 1, \ldots, p\}$. For each $i \in \{0, \ldots, p\}$, let $\underline{s}_i = \min_{j=1}^{n}\{\mathrm{Lord}(\mathbb{P}_i, y_j) \mid \mathrm{Lord}(\mathbb{P}_i, y_j) \ne -\infty\}$ and $\underline{s} = \sum_{i=0}^{p} \underline{s}_i$. Let $\widetilde{\mathrm{J}}_i = \mathrm{J}_i - \underline{s} + \underline{s}_i$. Then,

Theorem 57. *The effective order of $\mathbf{R}$ in $\mathbf{u}_i$ is bounded by $\widetilde{\mathrm{J}}_i$ for each $0 \le i \le p$.*

Proof. Let $m = \max_{i=0}^{p} \underline{s}_i$. Consider the following difference system

$$\mathcal{P}_1 = \left\{\mathbb{P}_0^{(m-\underline{s}_0)}, \ldots, \mathbb{P}_p^{(m-\underline{s}_p)}\right\}$$

which is also super-essential. Suppose $\mathbf{R}_1$ is the sparse difference resultant of $\mathcal{P}_1$. Clearly, $\mathbf{R}_1 \in \mathcal{I}_{\mathbf{u}} = [\mathbb{P}_0, \ldots, \mathbb{P}_p] \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_p\}$, so $\mathrm{ord}(\mathbf{R}_1, \mathbf{u}_i) \ge \mathrm{ord}(\mathbf{R}, \mathbf{u}_i)$ for each $i \in \{0, \ldots, p\}$. Since $y_j^{[m-1]}$ $(j = 1, \ldots, n)$ do not occur in $\mathcal{P}_1$, by replacing $y_j^{(t)}$ $(j = 1, \ldots, n)$ by $z_j^{(t-m)}$ in $\mathcal{P}_1$, we obtain a new system $\mathcal{P}_2$. As in the proof of Theorem 54, we can show that $\mathbf{R}_1$ is also the sparse difference resultant of $\mathcal{P}_2$. Suppose B is the order matrix of $\mathcal{P}_2$. Clearly, $\mathrm{Jac}(B_{\hat{i}}) = \widetilde{\mathrm{J}}_i$. By Theorem 55, $\mathrm{ord}(\mathbf{R}_1, \mathbf{u}_i^{(m-\underline{s}_i)}) \le \widetilde{\mathrm{J}}_i$. So $\mathrm{Eord}(\mathbf{R}_1, \mathbf{u}_i) \le \widetilde{\mathrm{J}}_i$ and $\mathrm{ord}(\mathbf{R}_1, \mathbf{u}_i) \le \widetilde{\mathrm{J}}_i + m - \underline{s}_i$ for each $i \in \{0, \ldots, p\}$.

Let $h_i = \mathrm{ord}(\mathbf{R}, \mathbf{u}_i)$ and $o_i = \mathrm{Lord}(\mathbf{R}, \mathbf{u}_i)$. We need to show that $h_i - o_i \le \widetilde{\mathrm{J}}_i$ holds for each $i \in \{0, \ldots, p\}$. Suppose the contrary, i.e. there exists some $i_0 \in \{0, \ldots, p\}$ such that $\mathrm{Eord}(\mathbf{R}, \mathbf{u}_{i_0}) = h_{i_0} - o_{i_0} > \widetilde{\mathrm{J}}_{i_0}$.

Suppose $\bar{h}_{i_0} = \mathrm{ord}(\mathbf{R}_1, \mathbf{u}_{i_0})$ and $\bar{o}_{i_0} = \mathrm{Lord}(\mathbf{R}_1, \mathbf{u}_{i_0})$. Then, $\bar{h}_{i_0} \ge h_{i_0}$ and $\mathrm{Eord}(\mathbf{R}_1, \mathbf{u}_{i_0}) = \bar{h}_{i_0} - \bar{o}_{i_0} \le \widetilde{\mathrm{J}}_{i_0} < h_{i_0} - o_{i_0}$. Clearly, $\sigma^{\bar{h}_{i_0}} u_{i_0 0}$ appears effectively in both $\sigma^{\bar{h}_{i_0} - h_{i_0}}\mathbf{R}$ and $\mathbf{R}_1$. Let B_1 be the Sylvester resultant of $\sigma^{\bar{h}_{i_0} - h_{i_0}}\mathbf{R}$ and $\mathbf{R}_1$ w.r.t. $\sigma^{\bar{h}_{i_0}} u_{i_0 0}$. We claim that $B_1 \ne 0$. Suppose the contrary, then we have $\sigma^{\bar{h}_{i_0} - h_{i_0}}\mathbf{R} \mid \mathbf{R}_1$, for $\mathbf{R}$ is irreducible. This is impossible since $\sigma^{\bar{h}_{i_0} - h_{i_0} + o_{i_0}} u_{i_0 0}$ appears effectively in $\sigma^{\bar{h}_{i_0} - h_{i_0}}\mathbf{R}$ while not in $\mathbf{R}_1$ for $\bar{h}_{i_0} - h_{i_0} + o_{i_0} < \bar{o}_{i_0}$.

Let $\widetilde{h}_{i_0} = \mathrm{ord}(B_1, u_{i_0 0})$ and $\widetilde{o}_{i_0} = \mathrm{Lord}(B_1, u_{i_0 0})$. Since B_1 is the resultant of $\sigma^{\bar{h}_{i_0} - h_{i_0}}\mathbf{R}$ and $\mathbf{R}_1$, $\widetilde{h}_{i_0} < \bar{h}_{i_0}$ and $\widetilde{o}_{i_0} \ge \bar{h}_{i_0} - h_{i_0} + o_{i_0}$. Then $\widetilde{h}_{i_0} - \widetilde{o}_{i_0} < \bar{h}_{i_0} - (\bar{h}_{i_0} - h_{i_0} + o_{i_0}) = h_{i_0} - o_{i_0}$. Since $B_1 \in \mathcal{I}_{\mathbf{u}}$, by Lemma 16, $\mathrm{ord}(B_1, u_{i_0 0}) \ge \mathrm{ord}(\mathbf{R}, u_{i_0 0})$. Repeat the above procedure for B_1 and $\sigma^{\widetilde{h}_{i_0} - h_{i_0}}\mathbf{R}$, we obtain a nonzero difference polynomial $B_2 \in \mathcal{I}_{\mathbf{u}}$ and $\mathrm{ord}(B_2, u_{i_0 0}) < \mathrm{ord}(B_1, u_{i_0 0})$. Continuing procedures in this way, one can obtain a nonzero $B_l \in \mathcal{I}_{\mathbf{u}}$ such that $\mathrm{ord}(B_l, u_{i_0 0}) < \mathrm{ord}(\mathbf{R}, u_{i_0 0})$ which contradicts Lemma 16. □

By the proof of the above theorem, the order of $\mathbf{R}_1$ with respect to $\mathbf{u}_i$ is bounded by $\widetilde{J}_i + m - \underline{s}_i$. Thus, we have the following new order bound for $\mathbf{R}$.

Corollary 58. *Let $\mathbf{R}$ and $\widetilde{J}_i$ $(i = 0, \ldots, p)$ be defined as above. Then the order of $\mathbf{R}$ in $\mathbf{u}_i$ is bounded by $\underline{\mathrm{J}_i} = \widetilde{J}_i + \bar{s} - \underline{s}_i = \mathrm{J}_i - \underline{s} + \bar{s}$ for each $0 \le i \le p$ where $\bar{s} = \max_{i=0}^{p} \underline{s}_i$.*

Example 59. Let $\mathbb{P}_0 = u_{00} + u_{01}y_1 + u_{02}y_2$, $\mathbb{P}_1 = u_{10} + u_{11}y_1^{(1)} + u_{12}y_2^{(1)}$, $\mathbb{P}_2 = u_{20} + u_{21}y_1^{(1)} + u_{22}y_2^{(1)}$. Then $\mathrm{J}_0 = \bar{\mathrm{J}}_0 = 2$, $\mathrm{J}_1 = \bar{\mathrm{J}}_1 = 1$, $\mathrm{J}_2 = \bar{\mathrm{J}}_2 = 1$, $\widetilde{\mathrm{J}}_0 = \widetilde{\mathrm{J}}_1 = \widetilde{\mathrm{J}}_2 = 0$. By Corollary 58, $\underline{\mathrm{J}_0} = 1$, $\underline{\mathrm{J}_1} = 0$, $\underline{\mathrm{J}_2} = 0$. Notice that $\mathbf{R} = \begin{vmatrix} u_{00}^{(1)} & u_{01}^{(1)} & u_{02}^{(1)} \\ u_{10} & u_{11} & u_{12} \\ u_{20} & u_{21} & u_{22} \end{vmatrix}$ and $\widetilde{\mathrm{J}}_0 = \widetilde{\mathrm{J}}_1 = \widetilde{\mathrm{J}}_2 = 0$, $\underline{\mathrm{J}_0} = 1$, $\underline{\mathrm{J}_1} = \underline{\mathrm{J}_2} = 0$ give the exact effective order and order of $\mathbf{R}$ respectively.

5. Sparse difference resultants as algebraic sparse resultants

In this section, we will show that the sparse difference resultant is equal to the algebraic sparse resultant of certain generic sparse polynomial system, which leads to a determinant representation for the sparse difference resultant.

5.1. Preliminaries on algebraic sparse resultant

We first prove several properties on algebraic sparse resultants which are needed in this paper. For more details about sparse resultant, please refer to Gelfand et al. (1994) and Sturmfels (1993).

Let $\mathcal{B}_0, \ldots, \mathcal{B}_n$ be finite subsets of $\mathbb{Z}^n$. Assume $\mathbf{0} \in \mathcal{B}_i$ and $|\mathcal{B}_i| \geq 2$ for each i. For algebraic indeterminates $\mathbb{X} = \{x_1, \ldots, x_n\}$ and $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$, denote $\mathbb{X}^\alpha = \prod_{i=1}^n x_i^{\alpha_i}$. Let

$$\mathbb{F}_i(x_1, \ldots, x_n) = c_{i0} + \sum_{\alpha \in \mathcal{B}_i \setminus \{\mathbf{0}\}} c_{i\alpha}\mathbb{X}^\alpha \quad (i = 0, \ldots, n) \tag{10}$$

be generic sparse Laurent polynomials, where $c_{i\alpha}$ are algebraic indeterminates. We call $\mathcal{B}_i$ the support of $\mathbb{F}_i$ and $\omega_i = \sum_{\alpha \in \mathcal{B}_i} c_{i\alpha}\alpha$ is called the *symbolic support vector* of $\mathbb{F}_i$. The smallest convex subset of $\mathbb{R}^n$ containing $\mathcal{B}_i$ is called the *Newton polytope* of $\mathbb{F}_i$. For any subset $I \subset \{0, \ldots, n\}$, the matrix D_I whose row vectors are ω_i $(i \in I)$ is called the *symbolic support matrix* of $\{\mathbb{F}_i : i \in I\}$. Denote $\mathbf{c}_i = (c_{i\alpha})_{\alpha \in \mathcal{B}_i}$ and $\mathbf{c}_I = \bigcup_{i \in I} \mathbf{c}_i$.

The following result is a direct consequence of Lemma 30 in the algebraic case.

Lemma 60. *For any subset $I \subset \{0, \ldots, n\}$, $\mathrm{tr.deg}\,\mathbb{Q}(\mathbf{c}_I)(\mathbb{F}_i : i \in I)/\mathbb{Q}(\mathbf{c}_I) = \mathrm{rk}(\mathrm{D}_I)$.*

Definition 61. Follow the notations introduced above.

- A collection of $\{\mathbb{F}_i\}_{i \in I}$ is said to be *weak essential* if $\mathrm{rk}(\mathrm{D}_I) = |I| - 1$.
- A collection of $\{\mathbb{F}_i\}_{i \in I}$ is said to be *essential* if $\mathrm{rk}(\mathrm{D}_I) = |I| - 1$ and for each proper subset J of I, $\mathrm{rk}(\mathrm{D}_J) = |J|$.

Similar to Theorems 31 and 34, we have the following two lemmas.

Lemma 62. *The system $\{\mathbb{F}_i\}_{i \in I}$ is weak essential if and only if $(\mathbb{F}_i : i \in I) \cap \mathbb{Q}[\mathbf{c}_I]$ is of codimension one. In this case, there exists an irreducible polynomial $\mathbf{R} \in \mathbb{Q}[\mathbf{c}_I]$ such that $(\mathbb{F}_i : i \in I) \cap \mathbb{Q}[\mathbf{c}_I] = (\mathbf{R})$ and $\mathbf{R}$ is called the* sparse resultant *of $\{\mathbb{F}_i : i \in I\}$.*

Proof. Let $\zeta_i = -\sum_{\alpha \in \mathcal{B}_i \setminus \{\mathbf{0}\}} c_{i\alpha}\mathbb{X}^\alpha$ and $\zeta = (\zeta_i)_{i \in I}$. Then it is easy to show that $\theta = (x_1, \ldots, x_n, \zeta)$ is a generic point of $(\mathbb{F}_i : i \in I)_{\mathbb{Q}(\mathbf{c}_I \setminus \{c_{i0}\})[\mathbb{X}, c_{i0} : i \in I]}$. Thus, ζ is a generic point of $(\mathbb{F}_i : i \in I) \cap \mathbb{Q}[\mathbf{c}_I]$ and its codimension is equal to $|I| - \mathrm{tr.deg}\,\mathbb{Q}(\mathbf{c}_I \setminus \{c_{i0}\})(\zeta_i : i \in I)/\mathbb{Q}(\mathbf{c}_I \setminus \{c_{i0}\}) = |I| - \mathrm{tr.deg}\,\mathbb{Q}(\mathbf{c}_I)(\mathbb{F}_i : i \in I)/\mathbb{Q}(\mathbf{c}_I) = |I| - \mathrm{rk}(\mathrm{D}_I)$ by Lemma 60. By Definition 61, the first assertion follows. The last part of the lemma follows from a basic property of prime ideals of codimension one in algebraic geometry. □

Lemma 63. *$\{\mathbb{F}_i\}_{i \in \mathrm{I}}$ is essential if and only if $(\mathbb{F}_i : i \in I) \cap \mathbb{Q}[\mathbf{c}_I] = (\mathbf{R})$ and $\mathbf{c}_i$ appears effectively in $\mathbf{R}$ for each $i \in I$.*

Proof. The lemma follows from Lemma 62 and the fact that if $(\mathbb{F}_i : i \in I) \cap \mathbb{Q}[\mathbf{c}_I] = (\mathbf{R})$, then for each j, $(\mathbb{F}_i : i \neq j) \cap \mathbb{Q}[\mathbf{c}_i : i \neq j] = \{0\}$ is a necessary and sufficient condition for $\mathbf{c}_j$ appearing effectively in $\mathbf{R}$. □

Suppose an arbitrary total ordering of $\{\mathbb{F}_0, \ldots, \mathbb{F}_n\}$ is given, say $\mathbb{F}_n > \cdots > \mathbb{F}_1 > \mathbb{F}_0$. Now we define a total ordering among subsets of $\{\mathbb{F}_0, \ldots, \mathbb{F}_n\}$. For any two subsets $\mathcal{D} = \{D_0, \ldots, D_s\}$ and $\mathcal{C} = \{C_0, \ldots, C_t\}$ where $D_0 > \cdots > D_s$ and $C_0 > \cdots > C_t$, $\mathcal{D}$ is said to be of *higher ranking* than $\mathcal{C}$, denoted by $\mathcal{D} \succ \mathcal{C}$, if 1) there exists an $i \leq \min(s,t)$ such that $D_0 = C_0, \ldots, D_{i-1} = C_{i-1}$, $D_i > C_i$ or 2) $s > t$ and $D_i = C_i$ $(i = 0, \ldots, t)$. Note that if $\mathcal{D}$ is a proper subset of $\mathcal{C}$, then $\mathcal{C} \succ \mathcal{D}$.

Lemma 64. *Let $\mathbb{F} = \{\mathbb{F}_i : i = 0, \ldots, n\}$ be the system given in (10). Suppose $\mathrm{rk}(\mathrm{D}_{\mathbb{F}}) \leq n$. Then $\mathbb{F}$ has an essential subset with minimal ranking.*

Proof. It suffices to show that $\mathbb{F}$ contains an essential subset, for the existence of an essential subset with minimal ranking can be deduced since "$\succ$" is a total ordering.

Let $\mathcal{T}_i = \mathbb{F} \backslash \{\mathbb{F}_0, \ldots, \mathbb{F}_{i-1}\}$ $(i = 1, \ldots, n)$ and $\mathcal{T}_0 = \mathbb{F}$. We claim that at least one of $\mathcal{T}_i$ is weak essential. If $\mathrm{rk}(\mathrm{D}_{\mathcal{T}_0}) = n$, we are done. Otherwise, $\mathrm{rk}(\mathrm{D}_{\mathcal{T}_0}) < n$. It is clear that $\mathrm{rk}(\mathrm{D}_{\mathcal{T}_i}) = \mathrm{rk}(\mathrm{D}_{\mathcal{T}_{i-1}})$ or $\mathrm{rk}(\mathrm{D}_{\mathcal{T}_i}) = \mathrm{rk}(\mathrm{D}_{\mathcal{T}_{i-1}}) - 1$ for $i = 1, \ldots, n-1$, so when deleting one row from the matrix, the co-rank, i.e. $|\mathcal{T}_i| - \mathrm{rk}(\mathrm{D}_{\mathcal{T}_i})$, will be unchanged or decreased by 1. Since $\mathrm{rk}(\mathrm{D}_{\mathcal{T}_0}) < n$, the co-rank of $\mathrm{D}_{\mathcal{T}_0}$ is larger than 1. Since the co-rank of $\mathrm{D}_{\mathcal{T}_n}$ is 0, there exists a $k \in \{1, \ldots, n-1\}$ such that the co-rank of $\mathrm{D}_{\mathcal{T}_k}$ is 1. Then $\mathrm{D}_{\mathcal{T}_k}$ is weak essential. Now, let $\mathbf{R}$ be the sparse resultant of $\mathcal{T}_k$ and let $\mathcal{C}$ be the set of $\mathbb{F}_i \in \mathcal{T}_k$ such that the coefficients of $\mathbb{F}_i$ occur in $\mathbf{R}$ effectively. Then, $\mathcal{C}$ is an essential subset of $\mathbb{F}$ by Lemma 63. □

An essential system $\{\mathbb{F}_i\}_{i \in I}$ is called *variable-essential* if the number of x_k appearing effectively in $\mathbb{F}_i$ $(i \in I)$ is $|I| - 1$. The following lemma shows that a variable-essential system can be obtained from an essential one.

Lemma 65. *Suppose $\mathbb{F}_I = \{\mathbb{F}_i : i \in I\}$ is essential. Then there exist $n - |I| + 1$ of the x_i such that by setting these x_i to 1, the specialized system $\widetilde{\mathbb{F}}_I = \{\widetilde{\mathbb{F}}_i : i \in I\}$ satisfies*

(1) *$\widetilde{\mathbb{F}}_I$ is still essential.*
(2) $\mathrm{rk}(\mathrm{D}_{\widetilde{\mathbb{F}}_I}) = |I| - 1$ *is the number of variables in* $\widetilde{\mathbb{F}}_I$.
(3) $(\mathbb{F}_I) \cap \mathbb{Q}[\mathbf{c}_I] = (\widetilde{\mathbb{F}}_I) \cap \mathbb{Q}[\mathbf{c}_I]$.

Proof. Let $\mathrm{D}_I = (m_{ij})_{|I| \times n}$ be the symbolic support matrix of $\mathbb{F}_I$. Since $\mathbb{F}_I$ is essential, D_I contains a submatrix of rank $|I| - 1$. Without loss of generality, we assume the matrix $\mathrm{D}_0 = (m_{ij})_{i=1,\ldots,|I|-1; j=1,\ldots,|I|-1}$ is of full rank. Then consider the new system $\widetilde{\mathbb{F}}_I$ obtained by setting $x_i = 1$ $(i = |I|, \ldots, n)$ in $\mathbb{F}_I$. Since D_0 is a submatrix of $\mathrm{D}_{\widetilde{\mathbb{F}}_I}$, $\widetilde{\mathbb{F}}_I$ is weak essential. By Lemma 62, we have $(\mathbb{F}_I) \cap \mathbb{Q}[\mathbf{c}_I] = (\mathbf{R})$ and $(\widetilde{\mathbb{F}}_I) \cap \mathbb{Q}[\mathbf{c}_I] = (\widetilde{\mathbf{R}})$ where $\mathbf{R}, \widetilde{\mathbf{R}}$ are irreducible polynomials in $\mathbb{Q}[\mathbf{c}_I]$. Hence, there exists a monomial $\mathfrak{m} \in \mathbb{Q}[x_1, \ldots, x_n]$ such that $\mathfrak{m}\mathbf{R} = \sum Q_i \mathbb{F}_i$. Set $x_i = 1$ $(i = |I|, \ldots, n)$, then we have $\widetilde{\mathfrak{m}}\mathbf{R} = \sum \widetilde{Q}_i \widetilde{\mathbb{F}}_i$. Hence $\mathbf{R} \in (\widetilde{\mathbf{R}})$. Since both $\mathbf{R}$ and $\widetilde{\mathbf{R}}$ are irreducible, $(\widetilde{\mathbf{R}}) = (\mathbf{R})$ and (2) follows. Thus, $\mathbf{c}_i$ $(i \in I)$ appears effectively in $\widetilde{\mathbf{R}}$, for $\mathbb{F}_I$ is essential. By Lemma 63, $\widetilde{\mathbb{F}}_I$ is essential and (1) is proved. (2) is obvious and the lemma is proved. □

Lemma 66. *Let $\mathbb{F} = \{\mathbb{F}_0, \ldots, \mathbb{F}_n\}$ be a variable-essential system of the form (10). Then we can find an invertible variable transformation $x_1 = \prod_{j=1}^{n} z_j^{m_{1j}}, \ldots, x_n = \prod_{j=1}^{n} z_j^{m_{nj}}$ for $m_{ij} \in \mathbb{Q}$, such that the image $\mathbb{G}$ of $\mathbb{F}$ under the above transformation is a generic sparse Laurent polynomial system satisfying*

(1) *$\mathbb{G}$ is variable-essential.*
(2) $\mathrm{Span}_{\mathbb{Z}}(\mathcal{B}) = \mathbb{Z}^n$, *where $\mathcal{B}$ is the set of the supports of all monomials in $\mathbb{G}$.*
(3) $(\mathbb{F}) \cap \mathbb{Q}[\mathbf{c}] = (\mathbb{G}) \cap \mathbb{Q}[\mathbf{c}]$.

Proof. This is a direct consequence of the Smith normal form method (Cohen, 1993, p. 67). Also see Shen et al. (2011) for an alternative proof. □

We call a system $\mathbb{F} = \{\mathbb{F}_i : i = 0, \ldots, n\}$ *strong essential* if $\mathbb{F}$ satisfies conditions (1) and (2) in Lemma 66. Recall that condition (2) is a basic requirement for studying sparse resultants in historic literatures and a strong essential system here is just an essential system as defined in Sturmfels (1994) and D'Andrea (2002). If $\mathbb{F}$ is strong essential, a matrix representation for $\mathbf{R}$ can be derived, that is, $\mathbf{R}$ can be represented as the quotient of the determinants of two matrices as shown in D'Andrea (2002). Moreover, the exact degree of the sparse resultant $\mathbf{R}$ can be given in terms of mixed volumes (Sturmfels, 1994), famous as the BKK-type degree bound. That is,

Theorem 67. *(See Sturmfels, 1994.) Suppose $\mathbb{F} = \{\mathbb{F}_i : i = 0, \ldots, n\}$ is a strong essential system of the form (10). Then, for each $i \in \{0, 1, \ldots, n\}$, the degree of the sparse resultant in $\mathbf{u}_i$ is a positive integer, equal to the* mixed volume

$$\mathcal{M}(\mathcal{Q}_0, \ldots, \mathcal{Q}_{i-1}, \mathcal{Q}_{i+1}, \ldots, \mathcal{Q}_n) = \sum_{\mathrm{J} \subset \{0, \ldots, i-1, i+1, \ldots, n\}} (-1)^{n-|\mathrm{J}|} \operatorname{vol}\Big(\sum_{j \in \mathrm{J}} \mathcal{Q}_j\Big)$$

where $\mathcal{Q}_i$ is the Newton polytope of $\mathbb{F}_i$, $\operatorname{vol}(\mathcal{Q})$ means the n-dimensional volume of $\mathcal{Q} \subset \mathbb{R}^n$ and $\sum_{j \in \mathrm{J}} \mathcal{Q}_j$ is the Minkowski sum of $\mathcal{Q}_j$ $(j \in J)$.

5.2. Sparse difference resultant as algebraic sparse resultant

Let $\mathbb{P} = \{\mathbb{P}_0, \ldots, \mathbb{P}_n\}$ be a Laurent transformally essential system as defined in (2). Given a vector $\mathbf{k} = (k_0, k_1, \ldots, k_p) \in \mathbb{N}_0^{n+1}$, the Laurent polynomial system $\bigcup_{i=0}^{p} \mathbb{P}_i^{[k_i]}$ is called a *prolongation* of the system $\mathbb{P}$ with respect to $\mathbf{k}$, denoted by $\mathbb{P}^{[\mathbf{k}]}$. Since the coefficient vector of $\mathbb{P}_i^{(j)}$ is $(u_{i0}^{(j)}, \ldots, u_{il_i}^{(j)})$, the coefficients of distinct Laurent polynomials in $\mathbb{P}^{[\mathbf{k}]}$ are algebraically independent over $\mathbb{Q}$. Thus, regarded as purely algebraic Laurent polynomials, $\mathbb{P}^{[\mathbf{k}]}$ is a system of generic sparse Laurent polynomials. In this section, we will show that the sparse difference resultant of $\mathbb{P}$ is closely related to the algebraic sparse resultant of a certain system obtained from a prolongation of $\mathbb{P}$.

With the above preparation, we now give the main result of this section.

Theorem 68. *Let $\mathbf{R}$ be the sparse difference resultant of the Laurent transformally essential system (2). Then we can obtain a strong essential generic algebraic sparse polynomial system $\mathcal{S}$ from (2), such that the sparse resultant of $\mathcal{S}$ is equal to $\mathbf{R}$.*

Proof. By Theorem 34, the system (2) has a unique super-essential subsystem $\mathbb{P}_I$. Without loss of generality, assume $I = \{0, 1, \ldots, p\}$. For each $i \in \{0, \ldots, p\}$, let $k_i = \operatorname{Jac}((A_I)_{\hat{i}})$ as defined in Theorem 55 and let $\mathbf{k} = (k_0, k_1, \ldots, k_p) \in \mathbb{N}_0^{p+1}$. Let

$$\mathcal{P} = \bigcup_{i=0}^{p} \mathrm{N}(\mathbb{P}_i)^{[k_i]} \tag{11}$$

be the prolongation of $\mathrm{N}(\mathbb{P})_I$ with respect to $\mathbf{k}$. Then $\mathcal{P}$ is a generic sparse polynomial system in variables $y_i^{(j)}$ with coefficients $U = \bigcup_{i=0}^{n} \mathbf{u}_i^{[k_i]}$. In the rest of the proof, $\mathcal{P}$ is considered as a set of algebraic polynomials in variables $y_i^{(j)}$.

A total ordering for polynomials in $\mathcal{P}$ is assigned as follows: $\sigma^k \mathbb{P}_i < \sigma^l \mathbb{P}_j$ if and only if $i < j$ or $i = j$ and $k < l$. A total ordering $\succ$ among subsets of $\mathcal{P}$ is the same as the one given in Section 5.1. By Theorem 55, $\operatorname{rk}(\mathrm{D}_{\mathcal{P}}) \le \sum_{i=0}^{p} k_i + p = |\mathcal{P}| - 1$. By Lemma 64, we can construct an essential subsystem $\mathcal{P}_1$ of $\mathcal{P}$ with minimal ranking. Let $\mathbf{R}_1$ be the sparse resultant of $\mathcal{P}_1$, that is, $(\mathcal{P}_1) \cap \mathbb{Q}[U] = (\mathbf{R}_1)$.

We claim that $\mathbf{R}_1 = c \cdot \mathbf{R}$ for some $c \in \mathbb{Q}$. Since $\mathbb{P}_I$ is super essential, for each $i \in I$, $\operatorname{ord}(\mathbf{R}, \mathbf{u}_i) \ge 0$. By Theorem 55, $\mathbf{R} \in (\mathcal{P})$. Let $\mathcal{P}_2$ be the elements of $\mathcal{P}$ whose coefficients appear effectively in $\mathbf{R}$. By

Lemma 63, $\mathcal{P}_2$ is essential and $(\mathcal{P}_2) \cap \mathbb{Q}[U] = (\mathbf{R})$. Let k_1 and k_2 be the largest integers such that $\sigma^{k_1}\mathbb{P}_p \in \mathcal{P}_1$ and $\sigma^{k_2}\mathbb{P}_p \in \mathcal{P}_2$. Since $\mathcal{P}_1$ and $\mathcal{P}_2$ are essential, $\mathrm{ord}(\mathbf{R}_1, \mathbf{u}_p) = k_1$ and $\mathrm{ord}(\mathbf{R}, \mathbf{u}_p) = k_2$. Since $\mathcal{P}_2 \succ \mathcal{P}_1$, $k_1 \le k_2$. Since $\mathbf{R}_1 \in (\mathcal{P}_1) \cap \mathbb{Q}[U] \subset [\mathbb{P}_I] \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_p\} = \mathrm{sat}(\mathbf{R}, \ldots)$, by Lemma 16, $k_1 \ge k_2$. Hence, $k_1 = k_2$, i.e. $\mathrm{ord}(\mathbf{R}_1, \mathbf{u}_p) = \mathrm{ord}(\mathbf{R}, \mathbf{u}_p)$. Since $\mathbf{R}_1 \in \mathrm{sat}(\mathbf{R}, \ldots)$, $\mathbf{R}_1$ is algebraically reduced to zero by $\mathbf{R}$. Since both $\mathbf{R}$ and $\mathbf{R}_1$ are irreducible, $\mathbf{R} = c\mathbf{R}_1$ for some $c \in \mathbb{Q}$.

Apply Lemma 65 to $\mathcal{P}_1$, we obtain a variable-essential system $\mathcal{P}_3$ satisfying $(\mathcal{P}_3) \cap \mathbb{Q}[U] = (\mathbf{R})$. Then apply Lemma 66 to $\mathcal{P}_3$, we obtain a strong essential generic system $\mathcal{S}$ satisfying $(\mathcal{S}) \cap \mathbb{Q}[U] = (\mathbf{R})$ and the existence of $\mathcal{S}$ is proved.

We will show that $\mathcal{S}$ can be given algorithmically. Through the above procedures, only Lemma 64 is not constructive. Since $\mathcal{P}$ contains an essential subsystem, we can simply check each subsystems $\mathcal{S}$ of $\mathcal{P}$ to see whether $\mathcal{S}$ is essential and find the one with minimal ranking. Note that $\mathcal{S}$ is essential if and only if $\mathrm{rk}(\mathrm{D}_{\mathcal{S}}) = |\mathcal{S}| - 1$ and any proper subset $\mathcal{C}$ of $\mathcal{S}$ satisfies $\mathrm{rk}(\mathrm{D}_{\mathcal{C}}) = |\mathcal{C}|$. □

Example 69. Let $n = 3$. Denote $y_{ij} = y_i^{(j)}$ and let $\mathbb{P} = \{\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2, \mathbb{P}_3\}$ where $\mathbb{P}_0 = u_{00} + u_{01}y_{11}^2 y_{21}^2 y_3 + u_{02}y_1^2 y_2 y_3$, $\mathbb{P}_1 = u_{10} + u_{11}y_{12}^4 y_{22}^4 y_{31}^2 + u_{12}y_{11}^2 y_{21} y_{31}$, $\mathbb{P}_2 = u_{20} + u_{21}y_{11}^2 y_{21}^2 y_3 + u_{22}y_1^2 y_2 y_3$ and $\mathbb{P}_3 = u_{30} + u_{31}y_{11}y_3$.

It is easy to show that $\mathbb{P}$ is a Laurent transformally essential system and $I = \{0, 1, 2\}$. Clearly, $\mathrm{Jac}((A_I)_{\hat{0}}) = 3, \mathrm{Jac}((A_I)_{\hat{1}}) = 2$ and $\mathrm{Jac}((A_I)_{\hat{2}}) = 3$. Using the notations in Theorem 68, we have $\mathcal{P} = \{\mathbb{P}_0^{[3]}, \mathbb{P}_1^{[2]}, \mathbb{P}_2^{[3]}\}$, and we can compute an essential subset $\mathcal{P}_1$ with minimal ranking. Here, we have $\mathcal{P}_1 = \{\sigma\mathbb{P}_0, \mathbb{P}_1, \sigma\mathbb{P}_2\}$. Using the variable order $y_{11} < y_{12} < y_{21} < y_{22} < y_{31}$ to obtain the symbolic support matrix of $\mathcal{P}_1$, the first 2×2 sub-matrix of $\mathrm{D}_{\mathcal{P}_1}$ is of rank 2. By the proof of Lemma 65, we set y_{21}, y_{22}, y_{31} to 1 to obtain a variable essential system $\mathcal{P}_2 = \{\widetilde{\sigma\mathbb{P}_0}, \widetilde{\mathbb{P}_1}, \widetilde{\sigma\mathbb{P}_2}\}$ where $\widetilde{\sigma\mathbb{P}_0} = u_{00}^{(1)} + u_{01}^{(1)}y_{12}^2 + u_{02}^{(1)}y_{11}^2$, $\widetilde{\mathbb{P}_1} = u_{10} + u_{11}y_{12}^4 + u_{12}y_{11}^2$, $\widetilde{\sigma\mathbb{P}_2} = u_{20}^{(1)} + u_{21}^{(1)}y_{12}^2 + u_{22}^{(1)}y_{11}^2$. Apply Lemma 66 to $\mathcal{P}_2$, set $z_1 = y_{11}^2, z_2 = y_{12}^2$, we obtain a strong essential generic system $\mathcal{P}_3 = \{\mathrm{Q}_0, \mathrm{Q}_1, \mathrm{Q}_2\}$ where $\mathrm{Q}_0 = u_{00}^{(1)} + u_{01}^{(1)}z_2 + u_{02}^{(1)}z_1$, $\mathrm{Q}_1 = u_{10} + u_{11}z_2^2 + u_{12}z_1$ and $\mathrm{Q}_2 = u_{20}^{(1)} + u_{21}^{(1)}z_2 + u_{22}^{(1)}z_1$. The sparse resultant of $\mathcal{P}_3$ is $R = u_{10}(u_{02}^{(1)}u_{21}^{(1)} - u_{01}^{(1)}u_{22}^{(1)})^2 + u_{11}(u_{00}^{(1)}u_{22}^{(1)} - u_{02}^{(1)}u_{20}^{(1)})^2 + u_{12}(u_{00}^{(1)}u_{21}^{(1)} - u_{01}^{(1)}u_{20}^{(1)})(u_{02}^{(1)}u_{21}^{(1)} - u_{01}^{(1)}u_{22}^{(1)})$, which is the sparse difference resultant of $\mathbb{P}$.

The following corollary is a direct consequence of the proof of Theorem 68 and D'Andrea (2002).

Corollary 70. *The sparse difference resultant* $\mathbf{R}$ *of a Laurent transformally essential system* (2) *can be represented as the quotient of two determinants whose elements are* $u_{ij}^{(k)}$ *or their sums for certain* $i \in \{0, \ldots, n\}$, $j \in \{0, \ldots, l_i\}$ *and* $k \in \{0, \ldots, \mathrm{J}_i\}$, *where* J_i *is the Jacobi number of the system* (2) *as defined in Section* 4.3.

Remark 71. It is desirable to derive a degree bound for $\mathbf{R}$ from Theorem 68. Let $\mathcal{S}$ be the strong essential set mentioned in the theorem. Then, the degree of $\mathbf{R}$ is equal to the mixed volume of $\mathcal{S}$ by Theorem 67. The problem is how to express the mixed volume of $\mathcal{S}$ in terms of certain quantities of $\mathbb{P}_I$ without computing $\mathcal{S}$.

6. A single exponential algorithm to compute the sparse difference resultant

In this section, we give an algorithm to compute the sparse difference resultant for a Laurent transformally essential system with single exponential complexity. The idea is to estimate the degree bounds for the resultant and then to use linear algebra to find the coefficients of the resultant.

6.1. Degree bounds for sparse difference resultants

In this section, we give an upper bound for the degree of the sparse difference resultant, which will be crucial to our algorithm to compute the sparse resultant. Before proposing the main theorem, we first give some algebraic results which will be needed in the proof.

Lemma 72. *(See Heintz, 1983; Vogel, 1984.) Let $V_1, \ldots, V_r$ $(r \geq 2)$ be pure dimensional projective varieties in $\mathbf{P}^n$. Then*

$$\prod_{i=1}^{r} \deg(V_i) \geq \sum_{C} \deg(C)$$

where C runs through all irreducible components of $V_1 \cap \cdots \cap V_r$.

Lemma 73. *(See Heintz, 1983; Li et al., 2011.) Let $\mathcal{I}$ be a prime ideal in $\mathcal{K}[\mathbb{X}]$ and $\mathcal{I}_r = \mathcal{I} \cap \mathcal{K}[x_1, \ldots, x_r]$ for any $1 \leq r \leq n$. Then $\deg(\mathcal{I}_r) \leq \deg(\mathcal{I})$.*

Now we are ready to give the main theorem of this section.

Theorem 74. *Let $\mathbb{P}_0, \ldots, \mathbb{P}_n$ be a Laurent transformally essential system of the form (2) with $\mathrm{ord}(\mathrm{N}(\mathbb{P}_i, y_j)) = s_{ij}$ and $\deg(\mathrm{N}(\mathbb{P}_i), \mathbb{Y}) = m_i$. Suppose $\mathrm{N}(\mathbb{P}_i) = \sum_{k=0}^{t_i} u_{ik} N_{ik}$ and J_i is the Jacobi number of $\{\mathrm{N}(\mathbb{P}_0), \ldots, \mathrm{N}(\mathbb{P}_n)\} \setminus \{\mathrm{N}(\mathbb{P}_i)\}$. Let $\mathbf{R}$ be the sparse difference resultant of $\mathbb{P}_i$. Suppose $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) = h_i$ for each i. Then the following assertions hold:*

1) $\deg(\mathbf{R}) \leq \prod_{i=0}^{n} (m_i + 1)^{h_i+1} \leq (m+1)^{\sum_{i=0}^{n}(\mathrm{J}_i+1)}$, *where* $m = \max_i\{m_i\}$.
2) $\mathbf{R}$ *has a representation*

$$\prod_{i=0}^{n} \prod_{k=0}^{h_i} \left(N_{i0}^{(k)}\right)^{\deg(\mathbf{R})} \cdot \mathbf{R} = \sum_{i=0}^{n} \sum_{k=0}^{h_i} G_{ik} \mathrm{N}(\mathbb{P}_i)^{(k)} \tag{12}$$

where $G_{ij} \in \mathbb{Q}[\mathbf{u}_0^{[h_0]}, \ldots, \mathbf{u}_n^{[h_n]}, y_1^{[t_1]}, \ldots, y_n^{[t_n]}]$ with $t_j = \max_{i=0}^{n}\{h_i + s_{ij}\}$ such that $\deg(G_{ij}(\mathbb{P}_i^{\mathrm{N}})^{(j)}) \leq [m + 1 + \sum_{i=0}^{n}(h_i + 1)\deg(N_{i0})]\deg(\mathbf{R})$.

Proof. In $\mathbf{R}$, let u_{i0} be replaced by $(\mathrm{N}(\mathbb{P}_i) - \sum_{k=1}^{t_i} u_{ik} N_{ik})/N_{i0}$ for each $i = 0, \ldots, n$ and let $\mathbf{R}$ be expanded as a difference polynomial in $\mathrm{N}(\mathbb{P}_i)$ and their transforms with coefficients in $\mathbb{Q}\{\mathbb{Y}^{\pm}; \mathbf{u}_0, \ldots, \mathbf{u}_n\}$. Then there exist $a_{ik} \in \mathbb{N}$ and polynomials G_{ik} such that $\prod_{i=0}^{n} \prod_{k=0}^{h_i} (N_{i0}^{(k)})^{a_{ik}} \mathbf{R} = \sum_{i=0}^{n} \sum_{k=0}^{h_i} G_{ik} \mathrm{N}(\mathbb{P}_i)^{(k)} + T$ with $T \in \mathbb{Q}\{\mathbf{u}, \mathbb{Y}\}$ free from u_{i0}. Since $T \in \mathcal{I}_{\mathbb{Y},\mathbf{u}} \cap \mathbb{Q}\{\mathbf{u}, \mathbb{Y}\} = \{0\}$ by Theorem 13, $T = 0$. Thus,

$$\prod_{i=0}^{n} \prod_{k=0}^{h_i} \left(N_{i0}^{(k)}\right)^{a_{ik}} \mathbf{R} = \sum_{i=0}^{n} \sum_{k=0}^{h_i} G_{ik} \mathrm{N}(\mathbb{P}_i)^{(k)}.$$

1) Let $t_j = \max_{i=0}^{n}\{h_i + s_{ij}\}$ and $\mathbb{Y}^{[\mathbf{t}]} = \{y_1^{[t_1]}, \ldots, y_n^{[t_n]}\}$. Denote $\mathbb{m}^{[\mathbf{t}]}$ to be the set of all monomials in $\mathbb{Y}^{[\mathbf{t}]}$. Let $\mathcal{J} = (\mathrm{N}(\mathbb{P}_0)^{[h_0]}, \ldots, \mathrm{N}(\mathbb{P}_n)^{[h_n]}) : \mathbb{m}^{[\mathbf{t}]}$ be an algebraic ideal in $\mathcal{R} = \mathbb{Q}[\mathbb{Y}^{[\mathbf{t}]}, \mathbf{u}_0^{[h_0]}, \ldots, \mathbf{u}_n^{[h_n]}]$. Then $\mathbf{R} \in \mathcal{J}$ by the above equality. Let $\eta = (\eta_1, \ldots, \eta_n)$ be a generic zero of $[0]$ over $\mathbb{Q}\langle\mathbf{u}\rangle$ and denote $\zeta_i = -\sum_{k=1}^{t_i} u_{ik} \frac{N_{ik}(\eta)}{N_{i0}(\eta)}$ $(i = 0, \ldots, n)$. It is easy to show that $\mathcal{J}$ is a prime ideal in $\mathcal{R}$ with a generic zero $(\eta^{[\mathbf{t}]}; \widetilde{\mathbf{u}}, \zeta_0^{[h_0]}, \ldots, \zeta_n^{[h_n]})$ and $\mathcal{J} \cap \mathbb{Q}[\mathbf{u}_0^{[h_0]}, \ldots, \mathbf{u}_n^{[h_n]}] = (\mathbf{R})$, where $\widetilde{\mathbf{u}} = \bigcup_i \mathbf{u}_i^{[h_i]} \setminus \{u_{i0}^{[h_i]}\}$. Let H_{ik} be the homogeneous polynomial corresponding to $\mathrm{N}(\mathbb{P}_i)^{(k)}$ with x_0 the variable of homogeneity. Then $\mathcal{J}^0 = ((H_{ik})_{1 \leq i \leq n; 0 \leq k \leq h_i}) : \widetilde{\mathbb{m}}$ is a prime ideal in $\mathbb{Q}[x_0, \mathbb{Y}^{[\mathbf{t}]}, \mathbf{u}_0^{[h_0]}, \ldots, \mathbf{u}_n^{[h_n]}]$ where $\widetilde{\mathbb{m}}$ is the whole set of monomials in $\mathbb{Y}^{[\mathbf{t}]}$ and x_0. And $\deg(\mathcal{J}^0) = \deg(\mathcal{J})$.

Since $\mathbb{V}((H_{ik})_{1 \leq i \leq n; 0 \leq k \leq h_i}) = \mathbb{V}(\mathcal{J}^0) \cup \mathbb{V}(H_{ik}, x_0) \bigcup_{j,l} \mathbb{V}(H_{ik}, y_j^{(l)})$, $\mathbb{V}(\mathcal{J}^0)$ is an irreducible component of $\mathbb{V}((H_{ik})_{1 \leq i \leq n; 0 \leq k \leq h_i})$. By Lemma 72, $\deg(\mathcal{J}^0) \leq \prod_{i=0}^{n} \prod_{k=0}^{h_i} (m_i + 1) = \prod_{i=0}^{n} (m_i + 1)^{h_i+1}$. Thus, $\deg(\mathcal{J}) \leq \prod_{i=0}^{n} (m_i + 1)^{h_i+1}$. Since $\mathcal{J} \cap \mathbb{Q}[\mathbf{u}_0^{[h_0]}, \ldots, \mathbf{u}_n^{[h_n]}] = (\mathbf{R})$, by Lemma 73, $\deg(\mathbf{R}) \leq \deg(\mathcal{J}) \leq \prod_{i=0}^{n} (m_i + 1)^{h_i+1} \leq (m+1)^{\sum_{i=0}^{n}(\mathrm{J}_i+1)}$ follows. The last inequality holds because $h_i \leq \mathrm{J}_i$ by Theorem 54.

2) To obtain the degree bounds for the above representation of $\mathbf{R}$, that is, to estimate $\deg(G_{ik} \mathrm{N}(\mathbb{P}_i)^{(k)})$ and a_{ik}, we take each monomial M in $\mathbf{R}$ and substitute u_{i0} by $(\mathrm{N}(\mathbb{P}_i) - \sum_{k=1}^{l_i} u_{ik} N_{ik})/$

N_{i0} into M and then expand it. To be more precise, we take one monomial $M(\mathbf{u}; u_{00}, \ldots, u_{n0}) = \mathbf{u}^{\gamma} \prod_{i=0}^{n} \prod_{k=0}^{h_i} (u_{i0}^{(k)})^{d_{ik}}$ with $|\gamma| + \sum_{i=0}^{n} \sum_{k=0}^{h_i} d_{ik} = \deg(\mathbf{R})$ for an example, where $\mathbf{u}^{\gamma}$ represents a difference monomial in $\mathbf{u}$ and their transforms with exponent vector γ. Then

$$M(\mathbf{u}; u_{00}, \ldots, u_{n0}) = \mathbf{u}^{\gamma} \prod_{i=0}^{n} \prod_{k=0}^{h_i} \left(\left(\mathrm{N}(\mathbb{P}_i) - \sum_{k=1}^{l_i} u_{ik} N_{ik} \right)^{(k)} \right)^{d_{ik}} \Bigg/ \prod_{i=0}^{n} \prod_{k=0}^{h_i} (N_{i0}^{(k)})^{d_{ik}}.$$

When expanded, every term of $\prod_{i=0}^{n} \prod_{k=0}^{h_i} (N_{i0}^{(k)})^{d_{ik}} M$ is of degree bounded by $|\gamma| + \sum_{i=0}^{n} \sum_{k=0}^{h_i} (m_i + 1) d_{ik} \le (m+1)\deg(\mathbf{R})$ in $\mathbf{u}_0^{[h_0]}, \ldots, \mathbf{u}_n^{[h_n]}$ and $\mathbb{Y}^{[\mathbf{t}]}$. Suppose $\mathbf{R} = \sum_M a_M M$ where $a_M \in \mathbb{Q}$ and given $a_{ik} \ge \max_M \{d_{ik}\}$. Then $\prod_{i=0}^{n} \prod_{k=0}^{h_i} (N_{i0}^{(k)})^{a_{ik}} \mathbf{R} = \sum_{i=0}^{n} \sum_{k=0}^{h_i} G_{ik} \mathrm{N}(\mathbb{P}_i)^{(k)}$ and $\deg(G_{ik} \mathrm{N}(\mathbb{P}_i)^{(k)}) \le (m+1) \times \deg(\mathbf{R}) + \sum_{i=0}^{n} \sum_{k=0}^{h_i} \deg(N_{i0}) a_{ik}$. Take $a_{ik} = \deg(\mathbf{R})$, then (12) follows. □

For a transformally essential difference polynomial system with degree zero terms, the second part of Theorem 74 can be improved as follows.

Corollary 75. *Let* $\mathbb{P}_i = u_{i0} + \sum_{k=1}^{l_i} u_{ik} N_{ik}$ $(i = 0, \ldots, n)$ *be a transformally essential difference polynomial system and* $\mathbf{R}$ *be the sparse difference resultant of* $\mathbb{P}_i$. *Suppose* $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) = h_i$ *for each* i *and* $m = \max_i \{\deg(\mathbb{P}_i, \mathbb{Y})\}$. *Then* $\mathbf{R}$ *has a representation*

$$\mathbf{R}(\mathbf{u}_0, \ldots, \mathbf{u}_n) = \sum_{i=0}^{n} \sum_{j=0}^{h_i} G_{ij} \mathbb{P}_i^{(j)}$$

where $G_{ij} \in \mathbb{Q}[\mathbf{u}_0^{[h_0]}, \ldots, \mathbf{u}_n^{[h_n]}, y_1^{[t_1]}, \ldots, y_n^{[t_n]}]$ *with* $t_j = \max_{i=0}^{n} \{h_i + s_{ij}\}$ *such that* $\deg(G_{ij} \mathbb{P}_i^{(j)}) \le (m+1)\deg(\mathbf{R}) \le (m+1)^{\sum_{i=0}^{n}(h_i+1)+1}$.

Proof. It is direct consequence of Theorem 74 by setting $N_{i0} = 1$. □

6.2. A single exponential algorithm to compute the sparse difference resultant

If a polynomial R is a linear combination of some known polynomials $F_i (i = 1, \ldots, s)$, that is $R = \sum_{i=1}^{s} H_i F_i$, and we know the upper bounds of the degrees of R and $H_i F_i$, then a general idea to estimate the computational complexity of R is to use linear algebra to find coefficients of R. For the sparse difference resultant, we already have given its degree bound and the degrees of terms in the linear combination as in Theorem 74.

Now, we give the algorithm **SDResultant** to compute sparse difference resultants based on linear algebra techniques which is almost identical to the differential case (Li et al., 2012). The algorithm works adaptively by searching for $\mathbf{R}$ with an order vector $(h_0, \ldots, h_n) \in \mathbb{N}_0^{n+1}$ with $h_i \le \mathrm{J}_i$ by Theorem 74. Denote $o = \sum_{i=0}^{n} h_i$. We start with $o = 0$. And for this o, choose one vector $(h_0, \ldots, h_n)$ at a time. For this $(h_0, \ldots, h_n)$, we search for $\mathbf{R}$ from degree $d = 1$. If we cannot find an $\mathbf{R}$ with such a degree, then we repeat the procedure with degree $d+1$ until $d > \prod_{i=0}^{n} (m_i + 1)^{h_i+1}$. In that case, we choose another $(h_0, \ldots, h_n)$ with $\sum_{i=0}^{n} h_i = o$. But if for all $(h_0, \ldots, h_n)$ with $h_i \le \mathrm{J}_i$ and $\sum_{i=0}^{n} h_i = o$, $\mathbf{R}$ cannot be found, then we repeat the procedure with $o + 1$. In this way, we will find an $\mathbf{R}$ with the smallest order satisfying Eq. (12), which is the sparse difference resultant.

Theorem 76. *Let* $\mathbb{P} = \{\mathbb{P}_0, \ldots, \mathbb{P}_n\}$ *be a Laurent transformally essential system of the form* (2). *Let* $\mathrm{J}_i = \mathrm{Jac}(\mathrm{N}(\mathbb{P})_{\hat{i}})$, $\mathrm{J} = \sum_{i=0}^{n} \mathrm{J}_i$ *and* $m = \max_i \deg(\mathrm{N}(\mathbb{P}_i), \mathbb{Y})$. *Algorithm* ***SDResultant*** *computes the sparse difference resultant* $\mathbf{R}$ *with the following complexities:*

1) *In terms of a degree bound* D *of* $\mathbf{R}$, *it needs at most* $O(\frac{[(m(\mathrm{J}+n+2)+1)D]^{O(l\mathrm{J}+l)}}{n^n})$ $\mathbb{Q}$*-arithmetic operations, where* $l = \sum_{i=0}^{n}(l_i + 1)$ *is the size of all* $\mathbb{P}_i$.

Algorithm 1 SDResultant($\mathbb{P}_0, \ldots, \mathbb{P}_n$).

Input: A generic Laurent transformally essential system $\mathbb{P}_0, \ldots, \mathbb{P}_n$.
Output: The sparse difference resultant $\mathbf{R}(\mathbf{u}_0, \ldots, \mathbf{u}_n)$ of $\mathbb{P}_0, \ldots, \mathbb{P}_n$.

```
1. For $i = 0, \ldots, n$, set $\mathrm{N}(\mathbb{P}_i) = \sum_{k=0}^{l_i} u_{ik} N_{ik}$ with $\deg(N_{i0}) \leq \deg(N_{ik})$.
   Set $m_i = \deg(\mathrm{N}(\mathbb{P}_i))$, $m_{i0} = \deg(N_{i0})$, $\mathbf{u}_i = \mathrm{coeff}(\mathbb{P}_i)$, $|\mathbf{u}_i| = l_i + 1$.
   Set $s_{ij} = \mathrm{ord}(\mathrm{N}(\mathbb{P}_i), y_j)$, $A = (s_{ij})$ and compute $\mathrm{J}_i = \mathrm{Jac}(A_{\hat{i}})$.
2. Set $\mathbf{R} = 0$, $o = 0$, $m = \max_i\{m_i\}$.
3. While $\mathbf{R} = 0$ do
   3.1. For each $(h_0, \ldots, h_n) \in \mathbb{N}_0^{n+1}$ with $\sum_{i=0}^n h_i = o$ and $h_i \leq \mathrm{J}_i$ do
        3.1.1. $U = \bigcup_{i=0}^n \mathbf{u}_i^{[h_i]}$, $t_j = \max_{i=0}^n\{h_i + e_{ij}\}$, $\mathbb{Y}^{[\mathbf{t}]} = \{y_1^{[t_1]}, \ldots, y_n^{[t_n]}\}$. $d = 1$.
        3.1.2. While $\mathbf{R} = 0$ and $d \leq \prod_{i=0}^n (m_i + 1)^{h_i+1}$ do
               3.1.2.1. Set $\mathbf{R}_0$ to be a homogeneous GPol of degree $d$ in $U$.
               3.1.2.2. Set $\mathbf{c}_0 = \mathrm{coeff}(\mathbf{R}_0, U)$.
               3.1.2.3. Set $G_{ij} (i = 0, \ldots, n;\ j = 0, \ldots, h_i)$ to be GPols in variables $\mathbb{Y}^{[\mathbf{t}]}$ and $U$
                        of total degree $[m + 1 + \sum_{i=0}^n (h_i + 1) m_{i0}]d - m_i - 1$.
               3.1.2.4. Set $\mathbf{c}_{ij} = \mathrm{coeff}(G_{ij}, \mathbb{Y}^{[\mathbf{t}]} \cup U)$.
               3.1.2.5. Set $\mathcal{P}$ to be the set of coefficients of $\prod_{i=0}^n \prod_{k=0}^{h_i} (N_{i0}^{(k)})^d \mathbf{R}_0 -$
                        $\sum_{i=0}^n \sum_{j=0}^{h_i} G_{ij} (\mathrm{N}(\mathbb{P}_i))^{(j)}$ as a polynomial in $\mathbb{Y}^{[\mathbf{t}]}$ and $U$.
               3.1.2.6. Note that $\mathcal{P}$ is a set of linear polynomials in $\mathbb{Z}[\mathbf{c}_0, \mathbf{c}_{ij}]$.
                            Solve the linear equation $\mathcal{P} = 0$ in $\mathbf{c}_0$ and $\mathbf{c}_{ij}$.
               3.1.2.7. If $\mathbf{c}_0$ has a nonzero solution, then substitute it into $\mathbf{R}_0$ to
                        get $\mathbf{R}$ and go to Step 4, else $\mathbf{R} = 0$.
               3.1.2.8. $d := d + 1$.
   3.2. $o := o + 1$.
4. Return $\mathbf{R}$.
```

/ * / GPol stands for generic algebraic polynomial.

/ * / coeff(P, V) returns the set of coefficients of P as a polynomial in variables V.

2) *The algorithm needs at most* $O((\mathrm{J} + n + 2)^{O(l\mathrm{J}+l)} (m + 1)^{O((l\mathrm{J}+l)(\mathrm{J}+n+2))} / n^n)$ $\mathbb{Q}$*-arithmetic operations.*

Proof. The algorithm finds a difference polynomial $P \in \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$ satisfying Eq. (12), which has the smallest order and the smallest degree among those with the same order. Existence for such a difference polynomial is guaranteed by Theorem 74. Such a P must be in $\mathcal{I}_{\mathbf{u}} = \mathrm{sat}(\mathbf{R}, \ldots)$. Since each difference polynomial in $\mathrm{sat}(\mathbf{R}, \ldots)$ not equal to $\mathbf{R}$ either has greater order than $\mathbf{R}$ or has the same order but greater degree than $\mathbf{R}$, P must be $\mathbf{R}$ (up to a factor in $\mathbb{Q}$).

We will estimate the complexity of the algorithm below. Denote D to be the degree bound of $\mathbf{R}$. By Theorem 74, $D \leq (m + 1)^{\sum_{i=0}^n (\mathrm{J}_i+1)} = (m + 1)^{\mathrm{J}+n+1}$, where $\mathrm{J} = \sum_{i=0}^n \mathrm{J}_i$. In each loop of Step 3, the complexity of the algorithm is clearly dominated by Step 3.1.2, where we need to solve a system of linear equations $\mathcal{P} = 0$ over $\mathbb{Q}$ in $\mathbf{c}_0$ and $\mathbf{c}_{ij}$. Clearly, $|\mathbf{c}_0| = \binom{d+L_1-1}{L_1-1}$ and $|\mathbf{c}_{ij}| = \binom{d_1-m_i-1+L_1+L_2}{L_1+L_2}$, where $L_1 = |U| = \sum_{i=0}^n (h_i + 1)(l_i + 1)$, $L_2 = |\mathbb{Y}^{[\mathbf{t}]}| = \sum_{j=1}^n (\max_i\{h_i + e_{ij}\} + 1)$ and $d_1 = [m + 1 + \sum_{i=0}^n (h_i + 1) m_{i0}]d$. Then $\mathcal{P} = 0$ is a linear equation system with $W_1 = \binom{d+L_1-1}{L_1-1} + \sum_{i=0}^n (h_i + 1)\binom{d_1-m_i-1+L_1+L_2}{L_1+L_2}$ variables and $W_2 = \binom{d_1+L_1+L_2}{L_1+L_2}$ equations. To solve it, we need at most $(\max\{W_1, W_2\})^\omega$ arithmetic operations over $\mathbb{Q}$, where ω is the matrix multiplication exponent and the currently best known ω is 2.376.

The iteration in Step 3.1.2 may go through 1 to $\prod_{i=0}^n (m_i + 1)^{h_i+1} \leq (m + 1)^{\sum_{i=0}^n (\mathrm{J}_i+1)}$, and the iteration in Step 3.1 at most will repeat $\prod_{i=0}^n (\mathrm{J}_i + 1)$ times. By Theorem 74, Step 3 may loop from $o = 0$ to J. In the whole algorithm, $L_1 \leq \sum_{i=0}^n (\mathrm{J}_i + 1)(l_i + 1) \leq l\mathrm{J} + l$, $L_2 = |\mathbb{Y}^{[\mathbf{t}]}| \leq \sum_{j=1}^n (\max_i\{\mathrm{J}_i + e_{ij}\} + 1) = \mathrm{J} + n$ by Li et al. (2012, Lemma 5.6), and $d_1 \leq [m + 1 + \sum_{i=0}^n (\mathrm{J}_i + 1) m_{i0}]D = (m(\mathrm{J} + n + 2) + 1)D$. Thus, $W_1 \leq \binom{D+l\mathrm{J}+l-1}{l\mathrm{J}+l-1} + \sum_{i=0}^n (\mathrm{J}_i + 1)\binom{(m(\mathrm{J}+n+2)+1)D-m_i-1+l\mathrm{J}+l+\mathrm{J}+n}{l\mathrm{J}+l+\mathrm{J}+n}$ and $\max\{W_1, W_2\} \leq (\mathrm{J} + n + 2)\binom{[m(\mathrm{J}+n+2)+1]D+l\mathrm{J}+l+\mathrm{J}+n}{l\mathrm{J}+l+\mathrm{J}+n}$.

Hence, the whole algorithm needs at most

$$\begin{aligned}
&\sum_{o=0}^{J}\ \sum_{\substack{h_i\le J_i\\ h_0+\cdots+h_n=o}}\ \sum_{d=1}^{\prod_{i=0}^{n}(m_i+1)^{h_i+1}} \big(\max\{W_1,W_2\}\big)^{2.376}\\
&\le \left(\prod_{i=0}^{n}(J_i+1)\right)\cdot D\cdot\left[(J+n+2)\binom{[m(J+n+2)+1]D+lJ+l+J+n}{lJ+l+J+n}\right]^{2.376}\\
&\le (J+n+2)^{3.376}\frac{(J+n+1)^{n+1}}{n^n}\cdot D\cdot\big[\big[m(J+n+2)+1\big]D\big]^{2.376(lJ+l+J+n)}
\end{aligned}$$

$\mathbb{Q}$-arithmetic operations. In the above inequalities, we assume $[m(J+n+2)+1]D \ge lJ+l+J+n$.

Since $l \ge 2(n+1)$, the complexity bound is $O([(m(J+n+2)+1)D]^{O(lJ+l)}/n^n)$. Our complexity assumes an $O(1)$-complexity cost for all field operations over $\mathbb{Q}$. Thus, the complexity follows. Now 1) is proved. To prove 2), we just need to replace D by the degree bound for $\mathbf{R}$ in Theorem 74 in the complexity bound in 1). □

Remark 77. As we indicated at the end of Section 3.3, if we first compute the super-essential set I, then the algorithm can be improved by only considering the Laurent difference polynomials $\mathbb{P}_i$ $(i \in I)$ in the linear combination of the sparse resultant.

7. Difference resultant

In this section, we introduce the notion of difference resultant and prove its basic properties.

Definition 78. Let $\mathbb{m}_{s,r}$ be the set of all difference monomials in $\mathbb{Y}$ of order $\le s$ and degree $\le r$. Let $\mathbf{u} = \{u_M\}_{M\in\mathbb{m}_{s,r}}$ be a set of difference indeterminates over $\mathbb{Q}$. Then, $\mathbb{P} = \sum_{M\in\mathbb{m}_{s,r}} u_M M$ is called a *generic difference polynomial* of order s and degree r.

Throughout this section, a generic difference polynomial is assumed to be of degree greater than zero. For any vector $\alpha = (a_1,\ldots,a_m) \in \mathbb{Z}^m$ and $\mathbb{X} = (x_1,\ldots,x_m)$, denote $x_1^{a_1}x_2^{a_2}\cdots x_m^{a_m}$ by $\mathbb{X}^\alpha$. Let

$$\mathbb{P}_i = u_{i0} + \sum_{\substack{\alpha\in\mathbb{Z}_{\ge 0}^{n(s_i+1)}\\ 1\le|\alpha|\le m_i}} u_{i\alpha}\big(\mathbb{Y}^{[s_i]}\big)^{\alpha} \quad (i=0,1,\ldots,n) \tag{13}$$

be $n+1$ generic difference polynomials in $\mathbb{Y}$ of order s_i, degree m_i and coefficients $\mathbf{u}_i$. Since $\{1, y_1, \ldots, y_n\}$ is contained in the support of each $\mathbb{P}_i$, $\{\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_n\}$ is a super-essential system and the sparse difference resultant exists. We define $\mathrm{Res}(\mathbb{P}_0,\ldots,\mathbb{P}_n)$ to be the *difference resultant* of $\mathbb{P}_0,\ldots,\mathbb{P}_n$.

Because each generic difference polynomial $\mathbb{P}_i$ contains all difference monomials of order bounded by s_i and total degree at most m_i, the difference resultant is sometimes called the *dense* difference resultant, in contrary to the sparse difference resultant.

The difference resultant satisfies all the properties we have proved for sparse difference resultants in previous sections. Apart from these, the difference resultant possess other better properties to be given in the rest of this section.

7.1. Exact order and degree

In this section, we will give the precise order and degree for the difference resultant, which is of BKK-style (Bernshtein, 1975; Cox et al., 1998).

Theorem 79. *Let $\mathbb{P}_i$ $(i = 0,\ldots,n)$ be generic difference polynomials of the form (13) with order s_i, degree m_i, and coefficients $\mathbf{u}_i$. Let $\mathbf{R}(\mathbf{u}_0,\ldots,\mathbf{u}_n)$ be the difference resultant of $\mathbb{P}_0,\ldots,\mathbb{P}_n$. Denote $s = \sum_{i=0}^{n} s_i$. Then*

$\mathbf{R}(\mathbf{u}_0, \ldots, \mathbf{u}_n)$ is also the algebraic sparse resultant of $\mathbb{P}_0^{[s-s_0]}, \ldots, \mathbb{P}_n^{[s-s_n]}$ treated as polynomials in $\mathbb{Y}^{[s]}$. And for each $i \in \{0, 1, \ldots, n\}$ and $k = 0, \ldots, s - s_i$,

$$\operatorname{ord}(\mathbf{R}, \mathbf{u}_i) = s - s_i \tag{14}$$

$$\deg\big(\mathbf{R}, \mathbf{u}_i^{(k)}\big) = \mathcal{M}\big((\mathcal{Q}_{jl})_{j \neq i, 0 \leq l \leq s - s_j}, \mathcal{Q}_{i0}, \ldots, \mathcal{Q}_{i,k-1}, \mathcal{Q}_{i,k+1}, \ldots, \mathcal{Q}_{i,s-s_i}\big) \tag{15}$$

where $\mathcal{Q}_{jl}$ is the Newton polytope of $\mathbb{P}_j^{(l)}$ as a polynomial in $\mathbb{Y}^{[s]}$ and $\mathbf{u}_i^{(k)} = (u_{i\alpha}^{(k)})_{u_{i\alpha} \in \mathbf{u}_i}$.

Proof. Regard $\mathbb{P}_i^{(k)}$ $(i = 0, \ldots, n; k = 0, \ldots, s - s_i)$ as polynomials in the $n(s+1)$ variables $\mathbb{Y}^{[s]} = \{y_1, \ldots, y_n, y_1^{(1)}, \ldots, y_n^{(1)}, \ldots, y_1^{(s)}, \ldots, y_n^{(s)}\}$, and we denote its support by $\mathcal{B}_{ik}$. Since the coefficients $\mathbf{u}_i^{(k)}$ of $\mathbb{P}_i^{(k)}$ can be treated as algebraic indeterminates, $\mathbb{P}_i^{(k)}$ are generic sparse polynomials with supports $\mathcal{B}_{ik}$, respectively. Now we claim that $\overline{\mathcal{B}}$ is strong essential, that is

C1) $\overline{\mathcal{B}} = \{\mathcal{B}_{ik} : 0 \leq i \leq n; 0 \leq k \leq s - s_i\}$ is an essential set.
C2) $\overline{\mathcal{B}} = \{\mathcal{B}_{ik} : 0 \leq i \leq n; 0 \leq k \leq s - s_i\}$ jointly spans the affine lattice $\mathbb{Z}^{n(s+1)}$.

Note that $|\overline{\mathcal{B}}| = n(s+1) + 1$. To prove C1), it suffices to show that any $n(s+1)$ distinct $\mathbb{P}_i^{(k)}$ are algebraically independent. Without loss of generality, we prove that for a fixed $l \in \{0, \ldots, s - s_0\}$,

$$S_l = \big\{(\mathbb{P}_i^{(k)})_{1 \leq i \leq n; 0 \leq k \leq s - s_i}, \mathbb{P}_0, \ldots, \mathbb{P}_0^{(l-1)}, \mathbb{P}_0^{(l+1)}, \ldots, \mathbb{P}_0^{(s-s_0)}\big\}$$

is an algebraically independent set. Clearly, $\{y_j^{(k)}, \ldots, y_j^{(s_i+k)} \mid j = 1, \ldots, n\}$ is a subset of the support of $\mathbb{P}_i^{(k)}$. Choose a monomial from each $\mathbb{P}_i^{(k)}$ and denote it by $m(\mathbb{P}_i^{(k)})$. Let

$$m\big(\mathbb{P}_0^{(k)}\big) = \begin{cases} y_1^{(k)} & 0 \leq k \leq l - 1 \\ y_1^{(s_0+k)} & l + 1 \leq k \leq s - s_0 \end{cases} \quad \text{and} \quad m\big(\mathbb{P}_1^{(k)}\big) = \begin{cases} y_1^{(l+k)} & 0 \leq k \leq s_0 \\ y_2^{(s_1+k)} & s_0 + 1 \leq k \leq s - s_1. \end{cases}$$

For each $i \in \{2, \ldots, n\}$, let

$$m\big(\mathbb{P}_i^{(k)}\big) = \begin{cases} y_i^{(k)} & 0 \leq k \leq \sum_{j=0}^{i-1} s_j \\ y_{i+1}^{(s_i+k)} & \sum_{j=0}^{i-1} s_j + 1 \leq k \leq s - s_i. \end{cases}$$

So $m(S_l)$ is equal to $\{y_j^{[s]} : 1 \leq j \leq n\}$, which are algebraically independent over $\mathbb{Q}$. Thus, the $n(s+1)$ members of S_l are algebraically independent over $\mathbb{Q}$. For if not, all the $\mathbb{P}_i^{(k)} - u_{i0}^{(k)}$ $(\mathbb{P}_i^{(k)} \in S_l)$ are algebraically dependent over $\mathbb{Q}(\mathbf{v})$ where $\mathbf{v} = \bigcup_{i=0}^n \mathbf{u}_i^{[s-s_i]} \backslash \{u_{i0}^{[s-s_i]}\}$. Now specialize the coefficient of $m(\mathbb{P}_i^{(k)})$ in $\mathbb{P}_i^{(k)}$ to 1, and all the other coefficients of $\mathbb{P}_i^{(k)} - u_{i0}^{(k)}$ to 0, by the algebraic version of Lemma 2, $\{m(\mathbb{P}_i^{(k)}) : \mathbb{P}_i^{(k)} \in S_l\}$ are algebraically dependent over $\mathbb{Q}$, which is a contradiction. Thus, claim C1) is proved. Claim C2) follows from the fact that 1 and $\mathbb{Y}^{[s]}$ are contained in the support of $\mathbb{P}_0^{[s-s_0]}$.

By C1) and C2), the sparse resultant of $(\mathbb{P}_i^{(k)})_{0 \leq i \leq n; 0 \leq k \leq s - s_i}$ exists and we denote it by G. Then $(G) = ((\mathbb{P}_i^{(k)})_{0 \leq i \leq n; 0 \leq k \leq s - s_i}) \cap \mathbb{Q}[\mathbf{u}_0^{[s-s_0]}, \ldots, \mathbf{u}_n^{[s-s_n]}]$, and by Theorem 67, $\deg(G, \mathbf{u}_i^{(k)}) = \mathcal{M}((\mathcal{Q}_{jl})_{j \neq i, 0 \leq l \leq s - s_j}, \mathcal{Q}_{i0}, \ldots, \mathcal{Q}_{i,k-1}, \mathcal{Q}_{i,k+1}, \ldots, \mathcal{Q}_{i,s-s_i})$, where $\mathbf{u}_i^{(k)} = (u_{i0}^{(k)}, \ldots, u_{i\alpha}^{(k)}, \ldots)$. The theorem is proved if we can show that $G = c \cdot \mathbf{R}$ for some $c \in \mathbb{Q}$.

Since $G \in [\mathbb{P}_0, \ldots, \mathbb{P}_n]$ and $\operatorname{ord}(G, \mathbf{u}_i) = s - s_i$, by Lemma 16, $\operatorname{ord}(\mathbf{R}, \mathbf{u}_i) \leq s - s_i$ for each $i = 0, \ldots, n$. If for some i, $\operatorname{ord}(\mathbf{R}, \mathbf{u}_i) = h_i < s - s_i$, then $\mathbf{R} \in ((\mathbb{P}_j^{(k)})_{j \neq i; 0 \leq k \leq s - s_j}, \mathbb{P}_i, \ldots, \mathbb{P}_i^{(h_i)})$, a contradiction to C1). Thus, $\operatorname{ord}(\mathbf{R}, \mathbf{u}_i) = s - s_i$ and $\mathbf{R} \in (G)$. Since $\mathbf{R}$ is irreducible, there exists some $c \in \mathbb{Q}$ such that $G = c \cdot \mathbf{R}$. So $\mathbf{R}$ is equal to the algebraic sparse resultant of $\mathbb{P}_0^{[s-s_0]}, \ldots, \mathbb{P}_n^{[s-s_n]}$. □

As a direct consequence of the above theorem and the determinant representation for algebraic sparse resultants given in D'Andrea (2002), we have the following result.

Corollary 80. *The difference resultant for generic difference polynomials $\mathbb{P}_i$ $(i = 0, \ldots, n)$ can be written as the form* $\det(D_1)/\det(D_0)$ *where D_1 and D_0 are matrices whose elements are coefficients of $\mathbb{P}_i$ and their transforms up to the order $s - s_i$ and D_0 is a minor of D_1.*

Based on the matrix representation given in the above corollary, the efficient algorithms given by Emiris and Canny (1995) and Emiris and Pan (2005) can be used to compute the difference resultant.

Corollary 81. *The degree of* **R** *in each coefficient set* $\mathbf{u}_i$ *is*

$$\deg(\mathbf{R}, \mathbf{u}_i) = \sum_{k=0}^{s-s_i} \mathcal{M}\big((\mathcal{Q}_{jl})_{j\neq i, 0\leq l\leq s-s_j}, \mathcal{Q}_{i0}, \ldots, \mathcal{Q}_{i,k-1}, \mathcal{Q}_{i,k+1}, \ldots, \mathcal{Q}_{i,s-s_i}\big),$$

and the total degree of **R** *is*

$$\deg(\mathbf{R}) = \sum_{i=0}^{n} \sum_{k=0}^{s-s_i} \mathcal{M}\big((\mathcal{Q}_{jl})_{j\neq i, 0\leq l\leq s-s_j}, \mathcal{Q}_{i0}, \ldots, \mathcal{Q}_{i,k-1}, \mathcal{Q}_{i,k+1}, \ldots, \mathcal{Q}_{i,s-s_i}\big).$$

Example 82. Consider two generic difference polynomials of order one and degree two in one indeterminate y: $\mathbb{P}_i = u_{i0} + u_{01}y + u_{i2}y^{(1)} + u_{i3}y^2 + u_{i4}yy^{(1)} + u_{i5}(y^{(1)})^2, i = 0, 1$. Then the degree bound given by Theorem 74 is $\deg(\mathbf{R}) \leq (2+1)^4 = 81$. By Theorem 79, $\deg(\mathbf{R}, \mathbf{u}_0) = \mathcal{M}(\mathcal{Q}_{10}, \mathcal{Q}_{11}, \mathcal{Q}_{00}) + \mathcal{M}(\mathcal{Q}_{10}, \mathcal{Q}_{11}, \mathcal{Q}_{01}) = 8 + 8 = 16$ and consequently $\deg(\mathbf{R}) = 32$, where $\mathcal{Q}_{00} = \mathcal{Q}_{10} = \mathrm{conv}\{(0,0,0), (2,0,0), (0,2,0)\}$, $\mathcal{Q}_{01} = \mathcal{Q}_{11} = \mathrm{conv}\{(0,0,0), (0,2,0), (0,0,2)\}$, and $\mathrm{conv}(\cdot)$ means taking the convex hull in $\mathbb{R}^3$. By the proof of Theorem 79, **R** is the sparse resultant of $\mathbb{P}_0, \sigma(\mathbb{P}_0), \mathbb{P}_1, \sigma(\mathbb{P}_1)$.

7.2. Poisson-type product formulas

In this section, we will give a Poisson-type product formula for difference resultant.

Let $\widetilde{\mathbf{u}} = \bigcup_{i=0}^{n} \mathbf{u}_i \setminus \{u_{00}\}$ and $\mathbb{Q}\langle\widetilde{\mathbf{u}}\rangle$ be the transformally transcendental extension of $\mathbb{Q}$ in the usual sense. Let $\mathbb{Q}_0 = \mathbb{Q}\langle\widetilde{\mathbf{u}}\rangle(u_{00}, \ldots, u_{00}^{(s-s_0-1)})$. Here, $\mathbb{Q}_0$ is not necessarily a difference extension field of $\mathbb{Q}$, for the transforms of u_{00} are not defined. In the following, we will follow Cohn (1948) to obtain algebraic extensions $\mathcal{G}_i$ of $\mathbb{Q}_0$ and define transforming operators to make $\mathcal{G}_i$ difference fields. Consider **R** as an irreducible algebraic polynomial $r(u_{00}^{(s-s_0)})$ in $\mathbb{Q}_0[u_{00}^{(s-s_0)}]$. In a suitable algebraic extension field of $\mathbb{Q}_0$, $r(u_{00}^{(s-s_0)}) = 0$ has $t_0 = \deg(r, u_{00}^{(s-s_0)}) = \deg(\mathbf{R}, u_{00}^{(s-s_0)})$ roots $\gamma_1, \ldots, \gamma_{t_0}$. Thus

$$\mathbf{R}(\mathbf{u}_0, \ldots, \mathbf{u}_n) = A \prod_{\tau=1}^{t_0} \big(u_{00}^{(s-s_0)} - \gamma_\tau\big) \tag{16}$$

where $A \in \mathbb{Q}_0$. Let $\mathcal{I}_{\mathbf{u}} = [\mathbb{P}_0, \ldots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$. By the definition of the difference resultant, $\mathcal{I}_{\mathbf{u}}$ is an essential reflexive prime difference ideal in the decomposition of $\{\mathbf{R}\}$ which is not held by any difference polynomial of order less than $s - s_0$ in u_{00}. Suppose $\mathbf{R}, \mathbf{R}_1, \mathbf{R}_2, \ldots$ is a basic sequence[4] of **R** corresponding to $\mathcal{I}_{\mathbf{u}}$. That is, $\mathcal{I}_{\mathbf{u}} = \bigcup_{k\geq 0} \mathrm{asat}(\mathbf{R}, \mathbf{R}_1, \ldots, \mathbf{R}_k)$. Regard all the $\mathbf{R}_i$ as algebraic polynomials over the coefficient field $\mathbb{Q}\langle\widetilde{\mathbf{u}}\rangle$. Denote $\gamma_{\tau 0} = \gamma_\tau$. Clearly, $u_{00}^{(s-s_0)} = \gamma_{\tau 0}$ is a generic zero of $\mathrm{asat}(\mathbf{R})$. Suppose $\gamma_{\tau i}$ $(i \leq k)$ are found in some algebraic extension field of $\mathbb{Q}_0$ such that $u_{00}^{(s-s_0+i)} = \gamma_{\tau i}$ $(0 \leq i \leq k)$ is a generic zero of $\mathrm{asat}(\mathbf{R}, \mathbf{R}_1, \ldots, \mathbf{R}_k)$. Then let $\gamma_{\tau,k+1}$ be an element such that $u_{00}^{(s-s_0+i)} = \gamma_{\tau i}$ $(0 \leq i \leq k+1)$ is a generic zero of $\mathrm{asat}(\mathbf{R}, \mathbf{R}_1, \ldots, \mathbf{R}_k, \mathbf{R}_{k+1})$. Clearly, $\gamma_{\tau,k+1}$ is also algebraic over $\mathbb{Q}_0$. Let $\mathcal{G}_\tau = \mathbb{Q}\langle\widetilde{\mathbf{u}}\rangle(u_{00}, \ldots, u_{00}^{(s-s_0-1)}, \gamma_\tau, \gamma_{\tau 1}, \ldots)$. Clearly, $\mathcal{G}_\tau$ is an algebraic extension

[4] For the rigorous definition of *basic sequence*, please refer to Cohn (1948). Here, we list its basic properties: i) For each $k \geq 0$, $\mathrm{ord}(\mathbf{R}_k, u_{00}) = s - s_0 + k$ and $\mathbf{R}, \mathbf{R}_1, \ldots, \mathbf{R}_k$ is an irreducible algebraic ascending chain, and ii) $\bigcup_{k\geq 0} \mathrm{asat}(\mathbf{R}, \mathbf{R}_1, \ldots, \mathbf{R}_k)$ is a reflexive prime difference ideal.

of $\mathbb{Q}_0$ and $\mathcal{G}_\tau$ is algebraically isomorphic to the quotient field of $\mathbb{Q}\{\mathbf{u}_0,\dots,\mathbf{u}_n\}/\mathcal{I}_\mathbf{u}$. Since the quotient field of $\mathbb{Q}\{\mathbf{u}_0,\dots,\mathbf{u}_n\}/\mathcal{I}_\mathbf{u}$ is also a difference field, we can introduce a transforming operator σ_τ into $\mathcal{G}_\tau$ to make it a difference field such that the above isomorphism becomes a difference one. That is, $\sigma_\tau|_{\mathbb{Q}_0} = \sigma|_{\mathbb{Q}_0}$ and

$$\sigma_\tau^k(u_{00}) = \begin{cases} u_{00}^{(k)} & 0 \le k \le s-s_0-1 \\ \gamma_{\tau,k-s-s_0} & k \ge s-s_0 \end{cases}$$

In this way, $(\mathcal{G}_\tau, \sigma_\tau)$ is a difference field.

Let F be a difference polynomial in $\mathbb{Q}\{\mathbf{u}_0,\mathbf{u}_1,\dots,\mathbf{u}_n\} = \mathbb{Q}\{\widetilde{\mathbf{u}}, u_{00}\}$. For convenience, by the symbol $F|_{u_{00}^{(s-s_0)}=\gamma_\tau}$, we mean substituting $u_{00}^{(s-s_0+k)}$ by $\sigma_\tau^k\gamma_\tau = \gamma_{\tau k}$ $(k \ge 0)$ into F. Similarly, by saying F vanishes at $u_{00}^{(s-s_0)} = \gamma_\tau$, we mean $F|_{u_{00}^{(s-s_0)}=\gamma_\tau} = 0$. The following lemma is a direct consequence of the above discussion.

Lemma 83. *$F \in \mathcal{I}_\mathbf{u}$ if and only if F vanishes at $u_{00}^{(s-s_0)} = \gamma_\tau$.*

Proof. Since $\mathcal{I}_\mathbf{u} = \bigcup_{k\ge 0} \mathrm{asat}(\mathbf{R}, \mathbf{R}_1, \dots, \mathbf{R}_k)$ and $u_{00}^{(s-s_0+i)} = \gamma_{\tau i}$ $(0 \le i \le k)$ is a generic zero of $\mathrm{asat}(\mathbf{R}, \mathbf{R}_1, \dots, \mathbf{R}_k)$, the lemma follows. □

Remark 84. In order to make $\mathcal{G}_\tau$ a difference field, we need to introduce a transforming operator σ_τ which is closely related to γ_τ. Since even for a fixed τ, generic zeros of $\mathrm{asat}(\mathbf{R}, \mathbf{R}_1, \dots, \mathbf{R}_k)$ beginning from $u_{00}^{(s-s_0)} = \gamma_\tau$ may not be unique, the definition of σ_τ also may not be unique, which is different from the differential case. In fact, it is a common phenomenon in difference algebra. Here, we just choose one, for they do not influence the following discussions.

Now we give the following Poisson type formula for the difference resultant.

Theorem 85. *Let $\mathbf{R}$ be the difference resultant of $\mathbb{P}_0,\dots,\mathbb{P}_n$. Let $\deg(\mathbf{R}, u_{00}^{(s-s_0)}) = t_0$. Then there exist $\xi_{\tau k}$ $(\tau = 1,\dots,t_0; k = 1,\dots,n)$ in extension fields $(\mathcal{G}_\tau, \sigma_\tau)$ of $(\mathbb{Q}\langle\widetilde{\mathbf{u}}\rangle, \sigma)$ such that*

$$\mathbf{R} = A \prod_{\tau=1}^{t_0} \mathbb{P}_0(\xi_{\tau 1},\dots,\xi_{\tau n})^{(s-s_0)}, \tag{17}$$

with $A \in \mathbb{Q}\langle\widetilde{\mathbf{u}}\rangle[u_{00}^{[s-s_0-1]}]$. Note that (17) is formal and it should be understood as $\mathbb{P}_0(\xi_\tau)^{(s-s_0)} \triangleq \sigma^{s-s_0}u_{00} + \sigma_\tau^{s-s_0}(\sum_{\alpha\in\mathcal{B}_0\setminus\{0\}} u_{0\alpha}(\xi_\tau^{[s-s_0]})^\alpha)$ where $\xi_\tau = (\xi_{\tau 1},\dots,\xi_{\tau n})$.

Proof. By Theorem 37, there exists $m \in \mathbb{N}$ such that

$$u_{00}\frac{\partial \mathbf{R}}{\partial u_{00}} + \sum_\alpha u_{0\alpha}\frac{\partial \mathbf{R}}{\partial u_{0\alpha}} = m\mathbf{R}.$$

Setting $u_{00}^{(s-s_0)} = \gamma_\tau$ in both sides of the above equation, we have

$$u_{00}\frac{\partial \mathbf{R}}{\partial u_{00}}\bigg|_{u_{00}^{(s-s_0)}=\gamma_\tau} + \sum_\alpha u_{0\alpha}\frac{\partial \mathbf{R}}{\partial u_{0\alpha}}\bigg|_{u_{00}^{(s-s_0)}=\gamma_\tau} = 0.$$

Let $\xi_{\tau\alpha} = (\frac{\partial \mathbf{R}}{\partial u_{0\alpha}} / \frac{\partial \mathbf{R}}{\partial u_{00}})|_{u_{00}^{(s-s_0)}=\gamma_\tau}$. Then $u_{00} = -\sum_\alpha u_{0\alpha}\xi_{\tau\alpha}$ with $u_{00}^{(s-s_0)} = \gamma_\tau$. That is, $\gamma_\tau = -\sigma_\tau^{s-s_0}(\sum_\alpha u_{0\alpha}\xi_{\tau\alpha}) = -(\sum_\alpha u_{0\alpha}\xi_{\tau\alpha})^{(s-s_0)}$. Thus,

$$\mathbf{R} = A \prod_{\tau=1}^{t_0} \left(u_{00} + \sum_\alpha u_{0\alpha}\xi_{\tau\alpha}\right)^{(s-s_0)}.$$

Suppose $\mathbb{P}_0 = u_{00} + \sum_{j=1}^{n} u_{0j0} y_j + T_0$. Let $\xi_{\tau j} = (\frac{\partial \mathbf{R}}{\partial u_{0j0}} / \frac{\partial \mathbf{R}}{\partial u_{00}})|_{u_{00}^{(s-s_0)}=\gamma_\tau}$ $(j = 1, \ldots, n)$ and $\xi_\tau = (\xi_{\tau 1}, \ldots, \xi_{\tau n})$. It remains to show that $\xi_{\tau\alpha} = (\xi_\tau^{[s_0]})^\alpha$.

Let $\zeta_i = -\sum_\alpha u_{i\alpha} (\mathbb{Y}^{[s_i]})^\alpha$ $(i = 0, \ldots, n)$. Clearly, $\zeta = (\mathbf{u}, \zeta_0, \ldots, \zeta_n)$ is a generic zero of $\mathcal{I}_\mathbf{u} = [\mathbb{P}_0, \ldots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$, where $\mathbf{u} = \bigcup_{i=1}^{n} \mathbf{u}_i \backslash \{u_{i0}\}$. For each $(\mathbb{Y}^{[s_0]})^\alpha = \prod_{j=1}^{n} (y_j^{(k)})^{m_{jk}}$, by Eq. (9), $(\mathbb{Y}^{[s_0]})^\alpha = \overline{\frac{\partial \mathbf{R}}{\partial u_{0\alpha}}} / \overline{\frac{\partial \mathbf{R}}{\partial u_{00}}} = \prod_{j=1}^{n} \prod_{k=0}^{s_0} ((\overline{\frac{\partial \mathbf{R}}{\partial u_{0j0}}} / \overline{\frac{\partial \mathbf{R}}{\partial u_{00}}})^{(k)})^{m_{jk}}$, where $\overline{\frac{\partial \mathbf{R}}{\partial u_{0\alpha}}} = \frac{\partial \mathbf{R}}{\partial u_{0\alpha}}|_{u_{i0}=\zeta_i}$. So $\frac{\partial \mathbf{R}}{\partial u_{0\alpha}} \prod_{j=1}^{n} \prod_{k=0}^{s_0} ((\frac{\partial \mathbf{R}}{\partial u_{00}})^{(k)})^{m_{jk}} - \frac{\partial \mathbf{R}}{\partial u_{00}} \prod_{j=1}^{n} \prod_{k=0}^{s_0} ((\frac{\partial \mathbf{R}}{\partial u_{0j0}})^{(k)})^{m_{jk}} \in \mathcal{I}_\mathbf{u}$. By Lemma 83, $\xi_{\tau\alpha} = \prod_{j=1}^{n} \prod_{k=0}^{s_0} (\xi_{\tau j}^{(k)})^{m_{jk}} = (\xi_\tau^{[s_0]})^\alpha$. Thus, (17) follows. □

Theorem 86. *The points $\xi_\tau = (\xi_{\tau 1}, \ldots, \xi_{\tau n})$ $(\tau = 1, \ldots, t_0)$ in (17) are generic zeros of the difference ideal $[\mathbb{P}_1, \ldots, \mathbb{P}_n]_{\mathbb{Q}\langle \mathbf{u}_1, \ldots, \mathbf{u}_n \rangle \{\mathbb{Y}\}}$.*

Proof. Clearly, ξ_τ are n-tuples over $\mathbb{Q}\langle \mathbf{u}_1, \ldots, \mathbf{u}_n \rangle$. For each $i = 1, \ldots, n$, rewrite $\mathbb{P}_i = u_{i0} + \sum_\alpha u_{i\alpha} \prod_{j=1}^{n} \prod_{k=1}^{s_i} (y_j^{(k)})^{\alpha_{jk}}$. Since $\zeta_i = -\sum_\alpha u_{i\alpha} \prod_{j=1}^{n} \prod_{k=1}^{s_i} (y_j^{(k)})^{\alpha_{jk}}$ and $y_j = \overline{\frac{\partial \mathbf{R}}{\partial u_{0j0}}} / \overline{\frac{\partial \mathbf{R}}{\partial u_{00}}}$, $\zeta_i + \sum_\alpha u_{i\alpha} \prod_{j=1}^{n} \prod_{k=1}^{s_i} ((\overline{\frac{\partial \mathbf{R}}{\partial u_{0j0}}} / \overline{\frac{\partial \mathbf{R}}{\partial u_{00}}})^{(k)})^{\alpha_{jk}} = 0$. Let $a_{jk} = \max_\alpha \alpha_{jk}$, then $u_{i0} \prod_{j=1}^{n} \prod_{k=1}^{s_i} ((\frac{\partial \mathbf{R}}{\partial u_{00}})^{(k)})^{a_{jk}} + \sum_\alpha u_{i\alpha} \prod_{j=1}^{n} \prod_{k=1}^{s_i} ((\frac{\partial \mathbf{R}}{\partial u_{0j0}})^{(k)})^{\alpha_{jk}} ((\frac{\partial \mathbf{R}}{\partial u_{00}})^{(k)})^{a_{jk}-\alpha_{jk}} \in \mathcal{I}_\mathbf{u}$. Thus, by Lemma 83, $\mathbb{P}_i(\xi_\tau) = u_{i0} + \sum_\alpha u_{i\alpha} \prod_{j=1}^{n} \prod_{k=1}^{s_i} (\xi_{\tau j}^{(k)})^{\alpha_{jk}} = 0$ $(i = 1, \ldots, n)$.

On the other hand, suppose $F \in \mathbb{Q}\langle \mathbf{u}_1, \ldots, \mathbf{u}_n \rangle \{\mathbb{Y}\}$ vanishes at ξ_τ. Without loss of generality, suppose $F \in \mathbb{Q}\{\mathbf{u}_1, \ldots, \mathbf{u}_n, \mathbb{Y}\}$. Clearly, $\mathbb{P}_1, \ldots, \mathbb{P}_n$ constitute an ascending chain in $\mathbb{Q}\{\mathbf{u}_1, \ldots, \mathbf{u}_n, \mathbb{Y}\}$ with u_{i0} as leaders. Let G be the difference remainder of F with respect to this ascending chain. Then G is free from u_{i0} and $F \equiv G \operatorname{mod} [\mathbb{P}_1, \ldots, \mathbb{P}_n]$. Then $G(\xi_\tau) = G(\widetilde{\mathbf{u}}; \xi_{\tau 1}, \ldots, \xi_{\tau n}) = 0$, where $\widetilde{\mathbf{u}} = \bigcup_{i=1}^{n} \mathbf{u}_i \backslash \{u_{i0}\}$. So there exist $a_k \in \mathbb{N}$ such that $G_1 = \prod_k ((\frac{\partial \mathbf{R}}{\partial u_{00}})^{(k)})^{a_k} G(\widetilde{\mathbf{u}}; \mathbb{Y}) \in \mathcal{I}_\mathbf{u}$. Thus, G_1 vanishes at $u_{i0} = \zeta_i$ $(i = 1, \ldots, n)$ while $\frac{\partial \mathbf{R}}{\partial u_{00}}$ does not. It follows that $G(\widetilde{\mathbf{u}}; \mathbb{Y}) \equiv 0$ and $F \in [\mathbb{P}_1, \ldots, \mathbb{P}_n]$. So ξ_τ are generic zeros of $[\mathbb{P}_1, \ldots, \mathbb{P}_n]_{\mathbb{Q}\langle \mathbf{u}_1, \ldots, \mathbf{u}_n \rangle \{\mathbb{Y}\}}$. □

By Theorems 85 and 86, we can see that difference resultants have Poisson-type product formula, which is similar to their algebraic and differential analogues.

We conclude this section by proving the following theorem, which explores the relationship between the difference resultant and the solvability of the given systems.

Theorem 87. *Let $\mathbf{R}$ be the difference resultant of $\mathbb{P}_0, \ldots, \mathbb{P}_n$. Suppose when each $\mathbf{u}_i$ is specialized to $\mathbf{v}_i$, $\mathbb{P}_i$ is specialized to $\overline{\mathbb{P}}_i$. If $\overline{\mathbb{P}}_0 = \cdots = \overline{\mathbb{P}}_n = 0$ has a common difference solution, then $\mathbf{R}(\mathbf{v}_0, \ldots, \mathbf{v}_n) = 0$. Moreover, if $\mathbf{R}(\mathbf{v}_0, \ldots, \mathbf{v}_n) = 0$ and $\frac{\partial \mathbf{R}}{\partial u_{00}}(\mathbf{v}_0, \ldots, \mathbf{v}_n) \neq 0$, then $\overline{\mathbb{P}}_0 = \cdots = \overline{\mathbb{P}}_n = 0$ has at most one solution $(\bar{y}_1, \ldots, \bar{y}_n)$ with each $\bar{y}_k = (\frac{\partial \mathbf{R}}{\partial u_{0k}} / \frac{\partial \mathbf{R}}{\partial u_{00}})(\mathbf{v}_0, \ldots, \mathbf{v}_n)$, where u_{0k} is the coefficient of y_k in $\mathbb{P}_0$.*

Proof. Suppose $\mathbb{P}_i = u_{i0} + T_i$ $(i = 1, \ldots, n)$ and $\mathbf{u} = \bigcup_{i=0}^{n} \mathbf{u}_i \backslash \{u_{i0}\}$. Clearly, $(\mathbb{Y}; \mathbf{u}, -T_0(\mathbb{Y}), \ldots, -T_n(\mathbb{Y}))$ is a generic zero of $[\mathbb{P}_0, \ldots, \mathbb{P}_n]_{\mathbb{Q}\{\mathbb{Y}; \mathbf{u}_0, \ldots, \mathbf{u}_n\}}$. Taking the partial derivative of $\mathbf{R}(\mathbf{u}; -T_0(\mathbb{Y}), \ldots, -T_n(\mathbb{Y})) = 0$ w.r.t. u_{0k}, we can show that $\frac{\partial \mathbf{R}}{\partial u_{00}} y_k - \frac{\partial \mathbf{R}}{\partial u_{0k}} \in [\mathbb{P}_0, \ldots, \mathbb{P}_n]$ $(k = 1, \ldots, n)$. If $\overline{\mathbb{P}}_0 = \cdots = \overline{\mathbb{P}}_n = 0$ has a common solution ξ, then $(\xi; \mathbf{v}_0, \ldots, \mathbf{v}_n)$ is a common solution of $[\mathbb{P}_0, \ldots, \mathbb{P}_n]$. Since $\mathbf{R} \in [\mathbb{P}_0, \ldots, \mathbb{P}_n]$, $\mathbf{R}$ must vanish at $(\mathbf{v}_0, \ldots, \mathbf{v}_n)$. Now suppose $\mathbf{R}(\mathbf{v}_0, \ldots, \mathbf{v}_n) = 0$ and $\frac{\partial \mathbf{R}}{\partial u_{00}}(\mathbf{v}_0, \ldots, \mathbf{v}_n) \neq 0$. If $(\bar{y}_1, \ldots, \bar{y}_n)$ is a common solution of $\overline{\mathbb{P}}_i = 0$, then each $\frac{\partial \mathbf{R}}{\partial u_{00}} y_k - \frac{\partial \mathbf{R}}{\partial u_{0k}}$ vanishes at $(\bar{y}_1, \ldots, \bar{y}_n; \mathbf{v}_0, \ldots, \mathbf{v}_n)$. Thus, $\bar{y}_k = (\frac{\partial \mathbf{R}}{\partial u_{0k}} / \frac{\partial \mathbf{R}}{\partial u_{00}})(\mathbf{v}_0, \ldots, \mathbf{v}_n)$, since $\frac{\partial \mathbf{R}}{\partial u_{00}}(\mathbf{v}_0, \ldots, \mathbf{v}_n) \neq 0$. Hence, the second assertion holds. □

Remark 88. If Problem 23 can be solved positively, then Theorem 87 can be strengthened as follows: If $\mathbf{R}(\mathbf{v}_0, \ldots, \mathbf{v}_n) = 0$ and $\frac{\partial \mathbf{R}}{\partial u_{00}}(\mathbf{v}_0, \ldots, \mathbf{v}_n) \neq 0$, then $\overline{\mathbb{P}}_0 = \cdots = \overline{\mathbb{P}}_n = 0$ has a unique solution $(\bar{y}_1, \ldots, \bar{y}_n)$ with each $\bar{y}_k = (\frac{\partial \mathbf{R}}{\partial u_{0k}} / \frac{\partial \mathbf{R}}{\partial u_{00}})(\mathbf{v}_0, \ldots, \mathbf{v}_n)$.

8. Conclusion and problem

In this paper, we first introduce the concepts of Laurent difference polynomial and Laurent transformally essential system and give a criterion for a difference polynomial system to be Laurent transformally essential in terms of its supports. Then the sparse difference resultant for a Laurent transformally essential system is defined and its basic properties are proved. Furthermore, order and degree bounds for the sparse difference resultant are given. Based on these bounds, an algorithm to compute the sparse difference resultant is proposed, which is single exponential in terms of the Jacobi number, the number of variables, and the size of the system. Besides these, the difference resultant is introduced and its basic properties are given, such as its precise order and BKK style degree, determinant representation, and a Poisson-type product formula.

We now propose several questions for further study apart from Problem 23.

The degree of the algebraic sparse resultant is equal to the mixed volume of certain polytopes generated by the supports of the polynomials as shown in Pedersen and Sturmfels (1993) or Gelfand et al. (1994, p. 255). And Theorem 79 shows that the degree of difference resultants is exactly of such BKK-style. It is desirable to obtain such a bound for sparse difference resultant. For more details, see Remark 71.

There exist very efficient algorithms to compute algebraic sparse resultants (Emiris, 1996; Emiris and Canny, 1995; Emiris and Pan, 2005; D'Andrea, 2002), which are based on matrix representations for the resultant. How to apply the principles behind these algorithms to compute sparse difference resultants is an important problem.

In the algebraic case, it is well known that the resultant vanishes if and only if the corresponding system of homogenous polynomials has common solutions in the projective space (Hodge and Pedoe, 1968). So it is interesting to see whether this result can be extended to the difference case. However, the corresponding result in the difference case might not be valid due to the reason that the projective difference space is not complete as shown in Theorem 46. In algebraic geometry, the fact that the projective space is complete plays a crucial role. Moreover, comparing with their algebraic and differential counterparts, difference fields have many surprising phenomena (Cohn, 1952).

Algebraic resultants and sparse resultants have many interesting applications (Canny, 1990; Cox et al., 1998; Emiris and Mourrain, 1999; Gelfand et al., 1994). It is desirable to develop the corresponding theory for difference polynomial systems based on difference resultants.

Acknowledgement

The authors would like to thank the anonymous referees for valuable suggestions. In particular, Theorem 38 is added due to a question of a referee.

References

Bernshtein, D.N., 1975. The number of roots of a system of equations. Funct. Anal. Appl. 9 (3), 183–185.
Bouziane, D., Kandri-Rody, A., Maârouf, H., 2001. Unmixed-dimensional decomposition of a finitely generated perfect differential ideal. J. Symb. Comput. 31 (6), 631–649.
Canny, J.F., 1990. Generalized characteristic polynomials. J. Symb. Comput. 9, 241–250.
Cohen, H., 1993. A Course in Computational Algebraic Number Theory. Springer-Verlag, New York.
Cohn, R.M., 1948. Manifolds of difference polynomials. Trans. Am. Math. Soc. 64 (1).
Cohn, R.M., 1952. Extensions of difference fields. Am. J. Math. 74 (2), 507–530.
Cohn, R.M., 1965. Difference Algebra. Interscience Publishers, New York.
Cohn, R.M., 1983. Order and dimension. Proc. Am. Math. Soc. 87 (1), 1–6.
Cox, D., Little, J., O'Shea, D., 1998. Using Algebraic Geometry. Springer.
D'Andrea, C., 2002. Macaulay style formulas for sparse resultants. Trans. Am. Math. Soc. 354 (7), 2595–2629.
Eisenbud, D., 1995. Commutative Algebra: With a View Toward Algebraic Geometry. Springer, New York.
Eisenbud, D., Schreyer, F.O., Weyman, J., 2004. Resultants and chow forms via exterior syzygies. J. Am. Math. Soc. 16 (3), 537–579.
Emiris, I.Z., 1996. On the complexity of sparse elimination. J. Complex. 12, 134–166.
Emiris, I.Z., Canny, J.F., 1995. Efficient incremental algorithms for the sparse resultant and the mixed volume. J. Symb. Comput. 20 (2), 117–149.
Emiris, I.Z., Mourrain, B., 1999. Matrices in elimination theory. J. Symb. Comput. 28 (1,2), 3–43.
Emiris, I.Z., Pan, V.Y., 2005. Improved algorithms for computing determinants and resultants. J. Complex. 21, 43–71.

Gao, X.S., Chou, S.C., 1993. On the dimension for arbitrary ascending chains. Chin. Sci. Bull. 38, 396–399.

Gao, X.S., Li, W., Yuan, C.M., 2013. Intersection theory in differential algebraic geometry: generic intersections and the differential Chow form. Trans. Am. Math. Soc. 365 (9), 4575–4632.

Gao, X.S., Luo, Y., Yuan, C.M., 2009. A characteristic set method for ordinary difference polynomial systems. J. Symb. Comput. 44 (3), 242–260.

Gelfand, I.M., Kapranov, M., Zelevinsky, A., 1994. Discriminants, Resultants and Multidimensional Determinants. Birkhäuser, Boston.

Heintz, J., 1983. Definability and fast quantifier elimination in algebraically closed fields. Theor. Comput. Sci. 24, 239–277.

Hodge, W.V.D., Pedoe, D., 1968. Methods of Algebraic Geometry, vol. I. Cambridge Univ. Press.

Hoffman, K., Kunze, R., 1971. Linear Algebra. Prentice-Hall.

Hrushovski, E., 2004. The elementary theory of the Frobenius automorphisms. Available from http://www.ma.huji.ac.il/~ehud/.

Jouanolou, J.P., 1991. Le formalisme du rèsultant. Adv. Math. 90 (2), 117–263.

Kapranov, M., Sturmfels, B., Zelevinsky, A., 1992. Chow polytopes and general resultants. Duke Math. J. 67, 189–218.

Kolchin, E.R., 1974. Differential equations in a projective space and linear dependence over a projective variety. In: Contributions to Analysis: A Collection of Papers Dedicated to Lipman Bers. Academic Press, pp. 195–214.

Lando, B.A., 1970. Jacobi's bound for the order of systems of first order differential equations. Trans. Am. Math. Soc. 152, 119–135.

Levin, A., 2008. Difference Algebra. Springer, New York.

Li, W., Gao, X.S., Yuan, C.M., 2011. Sparse differential resultant. In: Proc. ISSAC 2011. ACM Press, New York, pp. 225–232.

Li, W., Gao, X.S., 2012. Differential Chow form for projective differential variety. J. Algebra 370, 344–360.

Li, W., Yuan, C.M., Gao, X.S., 2012. Sparse differential resultant for Laurent differential polynomials. arXiv:1111.1084v3. 70 pages.

Li, W., Yuan, C.M., Gao, X.S., 2013. Sparse difference resultant. In: Proc. ISSAC 2013. ACM Press, Boston.

Pedersen, P., Sturmfels, B., 1993. Product formulas for resultants and Chow forms. Math. Z. 214 (1), 377–396.

Rueda, S.L., 2013. Linear sparse differential resultant formulas. Linear Algebra Appl. 438 (11), 4296–4321.

Rueda, S.L., Sendra, J.R., 2010. Linear complete differential resultants and the implicitization of linear DPPEs. J. Symb. Comput. 45 (3), 324–341.

Shen, L., Chionh, E., Gao, X.S., Li, J., 2011. Proper reparametrization for inherently improper unirational varieties. J. Syst. Sci. Complex. 24 (2), 367–380.

Sturmfels, B., 1993. Sparse elimination theory. In: Eisenbud, D., Robbiano, L. (Eds.), Computational Algebraic Geometry and Commutative Algebra. Cambridge University Press, pp. 264–298.

Sturmfels, B., 1994. On the Newton polytope of the resultant. J. Algebr. Comb. 3, 207–236.

Vogel, W., 1984. Lectures on Results on Bézout's Theorem. Springer-Verlag, Berlin.

Wibmer, M., 2013. Lecture Notes on Algebraic Difference Equations. Preprint.

Wu, W.T., 2003. Mathematics Machenization. Science Press/Kluwer, Beijing.

Zhang, Z.Y., Yuan, C.M., Gao, X.S., 2012. Matrix formula of differential resultant for first order generic ordinary differential polynomials. arXiv:1204.3773.