Sparse Difference Resultant*

Wei Li, Chun-Ming Yuan, Xiao-Shan Gao
KLMM, Institute of Systems Science, AMSS, Chinese Academy of Sciences, Beijing 100190, China
{liwei,cmyuan,xgao}@mmrc.iss.ac.cn

ABSTRACT

In this paper, the concept of sparse difference resultant for a Laurent transformally essential system of Laurent difference polynomials is introduced and its properties are proved. In particular, 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 system. Also, the precise order, degree, a determinant representation, and a Poisson-type product formula for the difference resultant are given.

Categories and Subject Descriptors

I.1.2 [**Computing Methodologies**]: Symbolic and Algebraic Manipulation - Algebraic algorithms

General Terms

Algorithms, Theory

Keywords

Sparse difference resultant, difference resultant, Laurent transformally essential system, Jacobi number, single exponential algorithm.

1. INTRODUCTION

The resultant, which gives conditions for an overdetermined system of polynomial equations to have common solutions, is a basic concept in algebraic geometry and a powerful tool in elimination theory [3, 6, 8, 16, 17, 26]. 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 is studied [15]. Kapranov, Sturmfels and Zelevinsky introduced the concept of $\mathcal{A}$-resultant [18]. Sturmfels further introduced the general mixed sparse resultant and gave a single exponential algorithm to compute the sparse resultant [26, 27]. 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 sparse resultants based on this matrix representation [10]. A determinant representation for the sparse resultant was finally given by D'Andrea [7]. Li [23] studied resultants and subresultants for linear differential and linear difference polynomials. Recently, in [13], a rigorous definition for the differential resultant of $n+1$ generic differential polynomials in n variables was presented [13] and also the theory of sparse differential resultants for Laurent differentially essential systems was developed [20, 21]. It is meaningful to generalize the theory of sparse resultant to difference polynomial systems.

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. In particular, we give order and degree bounds for the sparse difference resultant. Based on these bounds, we give an algorithm to compute the sparse difference resultant. The complexity of the algorithm in the worst case is single exponential of the form $O(m^{O(nlJ^2)}(nJ)^{O(lJ)})$, where n, m, J, and l are the number of variables, the degree, the Jacobi number, and the size of the Laurent transformally essential system respectively. Besides these, the difference resultant, which is non-sparse, is introduced and its basic properties are given, such as its precise order, degree, determinant representation, and Poisson-type product formula.

Although most properties for sparse difference resultants and difference resultants are similar to their differential counterparts given in [20, 21, 13], some of them are quite different in terms of descriptions and proofs. Firstly, the definition for difference resultant is more subtle than the differential case as illustrated in section 7. Secondly, the criterion for transformally essential systems given in Section 3.3 is quite different and much simpler than its differential counterpart given in [21]. Also, a determinant representation for the difference resultant is given in Section 6, but such a representation is still not known for differential resultants [28, 25]. Finally, some properties are more difficult in the difference case. For instance, we can only show that the vanishing of the difference resultant is a necessary condition for the corresponding difference polynomial system to have a common nonzero solution. However, the sufficient condition part is still open. Also, there does not exist a definition for homo-

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

ISSAC'13, June 26–29, 2013, Boston, Massachusetts, USA.

geneous difference polynomials, and the definition we give in this paper is different from its differential counterpart.

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. Then basic properties of sparse difference resultant are proved in Section 4. And in Section 5, we present an algorithm to compute the sparse difference resultant. Then we introduce the notion of difference resultant and prove its basic properties in section 6. In Section 7, we conclude the paper by proposing several problems for future research.

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 [5, 19].

Let $\mathcal{F}$ be an ordinary difference field with a transforming operator σ. For each $a \in \mathcal{F}$ and $n \in \mathbb{N}_0$, we denote $\sigma^n(a)$ by $a^{(n)}$, and by $a^{[n]}$ we mean the set $\{a, a^{(1)}, \ldots, a^{(n)}\}$. A typical example of difference field is $\mathbb{Q}(x)$ with $\sigma(f(x)) = f(x+1)$. Throughout this paper, we shall often use the prefix "σ-" to replace "difference" or "transformally".

Let $\mathcal{G}$ be a σ-extension field of $\mathcal{F}$. A subset $\mathcal{S}$ of $\mathcal{G}$ is said to be *σ-independent* (resp. *σ-dependent*) over $\mathcal{F}$ or a set of difference indeterminates if the set $\{\sigma^k a \big| a \in \mathcal{S}, k \geq 0\}$ is algebraically independent (resp. dependent) over $\mathcal{F}$. We use $\triangle\mathrm{tr.deg}\,\mathcal{G}/\mathcal{F}$ and $\mathrm{tr.deg}\,\mathcal{G}/\mathcal{F}$ to denote the *σ-transcendence degree* and the algebraic transcendence degree of $\mathcal{G}$ over $\mathcal{F}$ respectively. The following property will be needed.

Lemma 2.1 *Let $P_i(\mathbb{U}, \mathbb{Y}) \in \mathcal{F}\langle\mathbb{Y}\rangle\{\mathbb{U}\}$ $(i = 1, \ldots, m)$ where $\mathbb{U} = (u_1, \ldots, u_r)$ and $\mathbb{Y}$ are sets of σ-indeterminates. If $P_i(\mathbb{U}, \mathbb{Y})$ are σ-dependent over $\mathcal{F}\langle\mathbb{U}\rangle$, then for any $\overline{\mathbb{U}} \in \mathcal{F}^r$, $P_i(\overline{\mathbb{U}}, \mathbb{Y})$ are σ-dependent over $\mathcal{F}$.*

Proof: It suffices to show the case $r = 1$. We denote $u = u_1$. Since $P_i(u, \mathbb{Y})$ are σ-dependent over $\mathcal{F}\langle u\rangle$, there exist s and l such that $\mathbb{P}_i^{(k)}(u, \mathbb{Y})\,(k \leq s)$ are algebraically dependent over $\mathcal{F}(u^{(k)} | k \leq s+l)$. By [16, p.168], $\mathbb{P}_i^{(k)}(\bar{u}, \mathbb{Y})\,(k \leq s)$ are algebraically dependent over $\mathcal{F}$ and the lemma follows. □

Let $\mathcal{F}\{\mathbb{Y}\} = \mathcal{F}\{y_1, \ldots, y_n\}$ be a σ-polynomial ring and $\mathscr{R}$ a ranking endowed on it. For a σ-polynomial $f \in \mathcal{F}\{\mathbb{Y}\}$, 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 correspondingly 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.

For each subset $S \subset \mathcal{F}\{\mathbb{Y}\}$, we use (S) and $[S]$ to denote the algebraic ideal and the σ-ideal in $\mathcal{F}\{\mathbb{Y}\}$ generated by S. A σ-ideal $\mathcal{I} \subset \mathcal{F}\{\mathbb{Y}\}$ is called *reflexive* if $a^{(1)} \in \mathcal{I} \Longrightarrow a \in \mathcal{I}$. An n-tuple over $\mathcal{F}$ is of the form $(a_1, \ldots, a_n)$ where the a_i are in some σ-overfield of $\mathcal{F}$. An n-tuple η is called a *generic zero* of a σ-ideal $\mathcal{I} \subset \mathcal{F}\{\mathbb{Y}\}$ if for each $P \in \mathcal{F}\{\mathbb{Y}\}$ we have $P(\eta) = 0 \Leftrightarrow P \in \mathcal{I}$. It is well known that

Lemma 2.2 *[5, p.77] A σ-ideal possesses a generic zero if and only if it is a reflexive prime σ-ideal other than* [1].

Let $\mathcal{I}$ be a reflexive prime σ-ideal and η a generic zero of $\mathcal{I}$. The *dimension* of $\mathcal{I}$ is defined to be $\triangle\mathrm{tr.deg}\mathcal{F}\langle\eta\rangle/\mathcal{F}$. There is another description of dimension in terms of characteristic set. Let $\mathcal{A}$ be a characteristic set of a reflexive prime σ-ideal $\mathcal{I}$ w.r.t. some ranking $\mathscr{R}$. We rewrite $\mathcal{A}$ in the following form [14]

$$\mathcal{A} = \left\{ \begin{array}{l} A_{11}, \ldots, A_{1k_1} \\ \cdots \\ A_{p1}, \ldots, A_{pk_p} \end{array} \right.$$

where $\mathrm{lvar}(A_{ij}) = y_{c_i}$ and $\mathrm{ord}(A_{ij}, y_{c_i}) < \mathrm{ord}(A_{i,j+l}, y_{c_i})$. Then 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, it may happen that $k_1 > 1$. Below, we will show a property of uniqueness still exists. Before this, we list several algebraic results about regular chains [2].

Let $\mathcal{B} = B_1, \ldots, B_m$ be an algebraic triangular set in $\mathcal{F}[\mathbb{Y}]$ with $\mathrm{lvar}(B_i) = y_i$ and $U = \mathbb{Y}\backslash\{y_1, \ldots, y_m\}$. A polynomial f is said to be invertible w.r.t. $\mathcal{B}$ if either $f \in \mathcal{F}[U]$ or $(f, B_1, \ldots, B_s) \cap \mathcal{F}[U] \neq \{0\}$ where $\mathrm{lvar}(f) = \mathrm{lvar}(B_s)$. We call $\mathcal{B}$ a *regular chain* if for each $i > 1$, the initial of B_i is invertible w.r.t. $B_1, \ldots, B_{i-1}$. By $\mathrm{asat}(\mathcal{B})$, we mean the algebraic saturation ideal $(\mathcal{B}) : \mathrm{I}_{\mathcal{B}}^{\infty}$. For a regular chain $\mathcal{B}$, a polynomial f is said to be invertible w.r.t. $\mathrm{asat}(\mathcal{B})$ if $(f, \mathrm{asat}(\mathcal{B})) \cap \mathcal{F}[U] \neq \{0\}$.

Lemma 2.3 *Let $\mathcal{B} \subset \mathcal{F}[\mathbb{Y}]$ be a regular chain. If $\sqrt{asat(\mathcal{B})} = \bigcap_{i=1}^{m} \mathcal{P}_i$ is a minimal prime decomposition, then $f \in \mathcal{F}[\mathbb{Y}]$ is invertible w.r.t. $asat(\mathcal{B})$ if and only if $f \notin \mathcal{P}_i$ for all i.*

Proof: By [12], the parametric set of $\mathcal{B}$ is that of $\mathcal{P}_i$ for each i. The lemma follows from the fact that for prime ideals $\mathcal{P}_i$, $f \notin \mathcal{P}_i$ if and only if $(f, \mathcal{P}_i) \cap \mathcal{F}[U] \neq \{0\}$. □

Lemma 2.4 *[2] Let $\mathcal{B}$ be a regular chain in $\mathcal{F}[U, \mathbb{Y}]$, $L \neq 0$ invertible w.r.t $\mathcal{B}$, and $Lf \in (\mathcal{B})$. Then $f \in asat(\mathcal{B})$.*

Lemma 2.5 *Let $A \in \mathcal{F}\{\mathbb{Y}\}$ be irreducible with $\deg(A, y_{i_0}) > 0$ for some i_0. If f is invertible w.r.t. $A^{[k]}$ when $A^{[k]}$ is treated as an algebraic triangular set, then $\sigma(f)$ is invertible w.r.t. $A^{[k+1]}$. In particular, $A^{[k]}$ is a regular triangular set for any $k \geq 0$.*

Proof: It is a direct consequence of [14, Theorem 4.2]. □

The following fact is needed to define sparse σ-resultant.

Lemma 2.6 *Let $\mathcal{I}$ be a reflexive prime σ-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: Let $\mathcal{A} = A_1, \ldots, A_m$ be a characteristic set of $\mathcal{I}$ w.r.t. some ranking $\mathscr{R}$ with A_1 irreducible. Suppose $\mathrm{lvar}(\mathcal{A}) = y_1$. Given another characteristic set $\mathcal{B} = B_1, \ldots, B_l$ of $\mathcal{I}$ w.r.t. some other ranking $\mathscr{R}'$ (B_1 is irreducible), we will show there exists $c \in \mathcal{F}$ s.t. $B_1 = c \cdot A_1$. It suffices to consider the case $\mathrm{lvar}(\mathcal{B}) \neq y_1$. Suppose $\mathrm{lvar}(B_1) = y_2$. Clearly, y_2 appears effectively in A_1 for $\mathcal{B}$ reduces A_1 to 0. And since $\mathcal{I}$ is reflexive, there exists some i_0 such that $\deg(A_1, y_{i_0}) > 0$.

Suppose $\mathrm{ord}(A_1, y_2) = o_2$. Take another ranking under which $y_2^{(o_2)}$ is the leader of A_1 and we use $\tilde{A}_1$ to distinguish it from A_1 under $\mathscr{R}$. By Lemma 2.5, for each k, $A_1^{[k]}$ and $\tilde{A}_1^{[k]}$ are regular triangular sets.

Now we claim that $\mathrm{asat}(A_1^{[k]}) = \mathrm{asat}(\tilde{A}_1^{[k]})$. Suppose $f \in \mathrm{asat}(A_1^{[k]})$, then $(\prod_{i=0}^{k}\sigma^i(\mathrm{I}_{A_1}))^a f \in (A_1^{[k]})$. Since I_{A_1} is invertible w.r.t. $\tilde{A}_1$, by Lemma 2.5, $(\prod_{i=0}^{k}\sigma^i(\mathrm{I}_{A_1}))^a$ is invertible w.r.t. $\tilde{A}_1^{[k]}$. So by Lemma 2.4, $f \in \mathrm{asat}(\tilde{A}_1^{[k]})$ and $\mathrm{asat}(A_1^{[k]}) \subseteq \mathrm{asat}(\tilde{A}_1^{[k]})$ follows. Similarly, $\mathrm{asat}(\tilde{A}_1^{[k]}) \subseteq \mathrm{asat}(A_1^{[k]})$. Thus, $\mathrm{asat}(A_1^{[k]}) = \mathrm{asat}(\tilde{A}_1^{[k]})$.

Suppose $\mathrm{ord}(B_1, y_2) = o_2'$. Clearly, $o_2 \geq o_2'$. Assume $o_2 > o_2'$. Then B_1 is invertible w.r.t. $\mathrm{asat}(\tilde{A}_1^{[k]})$. Since $\mathrm{asat}(A_1^{[k]}) = \mathrm{asat}(\tilde{A}_1^{[k]})$, by Lemma 2.3, B_1 is invertible w.r.t. $\mathrm{asat}(A_1^{[k]})$. Thus, there exists a nonzero polynomial H with $\mathrm{ord}(H, y_1) < \mathrm{ord}(A_1, y_1)$ s.t. $H \in (B_1, \mathrm{asat}(A_1^{[k]})) \subset \mathcal{I}$, which is a contradiction. Thus, $o_2 = o_2'$. Since $\mathcal{B}$ reduces A_1 to zero and A_1 is irreducible, there exists $c \in \mathcal{F}$ such that $B_1 = c \cdot A_1$. □

3. SPARSE DIFFERENCE RESULTANT

In this section, the concepts of Laurent σ-polynomials and Laurent σ-essential systems are first introduced, and then the sparse σ-resultant for Laurent σ-essential systems is defined. And we also give a criterion for Laurent σ-essential systems in terms of the support of the given system.

3.1 Laurent difference polynomial

Similar to [21], before defining sparse σ- resultant, we first introduce the concept of Laurent σ-polynomials.

Definition 3.1 *A Laurent σ-monomial of order s is of the form $\prod_{i=1}^{n}\prod_{k=0}^{s}(y_i^{(k)})^{d_{ik}}$ where d_{ik} are integers which can be negative. A* Laurent σ-polynomial *over $\mathcal{F}$ is a finite linear combination of Laurent σ-monomials with coefficients in $\mathcal{F}$.*

Clearly, the collections of all Laurent σ-polynomials form a commutative σ-ring. We denote the σ-ring of Laurent σ-polynomials with coefficients in $\mathcal{F}$ by $\mathcal{F}\{\mathbb{Y}, \mathbb{Y}^{-1}\}$.

Definition 3.2 *For each $F \in \mathcal{F}\{\mathbb{Y}, \mathbb{Y}^{-1}\}$, the* normal form *of F, denoted by $\mathrm{N}(F)$, is defined to be the σ-polynomial in $\mathcal{F}\{\mathbb{Y}\}$ obtained by clearing denominators from F. The order and degree of F is defined to be the* order *and* degree *of $\mathrm{N}(F)$, denoted by $\mathrm{ord}(F)$ and $\deg(F)$.*

Definition 3.3 *Let $F \in \mathcal{F}\{\mathbb{Y}, \mathbb{Y}^{-1}\}$. An n-tuple $(a_1, \ldots, a_n)$ over $\mathcal{F}$ with each $a_i \neq 0$ is called a* nonzero σ-zero *of F if $F(a_1, \ldots, a_n) = 0$.*

3.2 Def nition of sparse difference resultant

In this section, the definition of the sparse σ-resultant will be given. We first define sparse σ-resultants for Laurent σ-polynomials whose coefficients are σ-indeterminates.

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

$$\mathbb{P}_i = \sum_{k=0}^{l_i} u_{ik} M_{ik} \ (i = 0, \ldots, n), \tag{1}$$

where all the u_{ik} are σ-independent over $\mathbb{Q}$. Denote

$$\mathbf{u}_i = (u_{i0}, u_{i1}, \ldots, u_{in}) \text{ and } \mathbf{u} = \bigcup_{i=0}^{n} \mathbf{u}_i \backslash \{u_{i0}\}. \tag{2}$$

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

Definition 3.4 *A set of Laurent σ-polynomials of the form (1) is called* Laurent σ-essential *if there exist k_i $(i = 0, \ldots, n)$ with $1 \leq k_i \leq l_i$ s.t. $\triangle\mathrm{tr.deg}\,\mathbb{Q}\langle\frac{M_{0k_0}}{M_{00}}, \ldots, \frac{M_{nk_n}}{M_{n0}}\rangle/\mathbb{Q} = n$. In this case, $\mathcal{A}_0, \ldots, \mathcal{A}_n$ are also called Laurent σ-essential.*

Although M_{i0} are used as denominators in the above definition, the σ-essential condition does not depend on the choices of M_{i0}. Let $\mathcal{I}_{\mathbb{Y},\mathbf{u}} = ([\mathrm{N}(\mathbb{P}_0), \ldots, \mathrm{N}(\mathbb{P}_n)] : \mathbf{m}) \subset \mathbb{Q}\{\mathbb{Y}, \mathbf{u}_0, \ldots, \mathbf{u}_n\}$ where $\mathbf{m}$ is the set of all σ-monomials in $\mathbb{Y}$. The following result is a foundation for defining sparse σ-resultants.

Theorem 3.5 *Let $\mathbb{P}_0, \ldots, \mathbb{P}_n$ be the Laurent σ-polynomials defined in (1). Then the following assertions hold.*

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

Proof: Let $\eta = (\eta_1, \ldots, \eta_n)$ be a sequence of σ-independent elements over $\mathbb{Q}\langle\mathbf{u}\rangle$, where $\mathbf{u}$ is defined in (2). Let

$$\zeta_i = -\sum_{k=1}^{l_i} u_{ik}\frac{M_{ik}(\eta)}{M_{i0}(\eta)} \ (i = 0, 1, \ldots, n), \tag{3}$$

and $\zeta = (\zeta_0, u_{01}, \ldots, u_{0l_0}; \ldots; \zeta_n, u_{n1}, \ldots, u_{nl_n})$. It is easy to show that $(\eta; \zeta)$ is a generic zero of $\mathcal{I}_{\mathbb{Y},\mathbf{u}}$, and by Lemma 2.2, $\mathcal{I}_{\mathbb{Y},\mathbf{u}}$ is a reflexive prime σ-ideal.

Consequently, $\mathcal{I}_{\mathbf{u}} = \mathcal{I}_{\mathbb{Y},\mathbf{u}} \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$ is a reflexive prime σ-ideal with a generic zero ζ. So $\mathcal{I}_{\mathbf{u}}$ is of codimension one $\Leftrightarrow \triangle\mathrm{tr.deg}\,\mathbb{Q}\langle\zeta\rangle/\mathbb{Q} = \sum_{i=0}^{n} l_i + n \Leftrightarrow$ there exist distinct $i_1, \ldots, i_n$ s.t. $\zeta_{i_1}, \ldots, \zeta_{i_n}$ are σ-independent over $\mathbb{Q}\langle\mathbf{u}\rangle \Leftrightarrow$ $\mathbb{P}_0, \ldots, \mathbb{P}_n$ form a Laurent σ-essential system. And the last "$\Leftrightarrow$" follows from Lemma 2.1. □

Let $[\mathbb{P}_0, \ldots, \mathbb{P}_n]$ be the σ-ideal in $\mathbb{Q}\{\mathbb{Y}, \mathbb{Y}^{-1}; \mathbf{u}_0, \ldots, \mathbf{u}_n\}$ generated by $\mathbb{P}_i$. Then we have

Corollary 3.6 *$\mathcal{I}_{\mathbf{u}} = [\mathbb{P}_0, \ldots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$ is a reflexive prime σ-ideal of codimension one if and only if $\{\mathbb{P}_i : i = 0, \ldots, n\}$ is a Laurent σ-essential system.*

Proof: It is a direct consequence of Theorem 3.5 and the fact that $[\mathbb{P}_0, \ldots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\} = \mathcal{I}_{\mathbb{Y},\mathbf{u}} \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$. □

Now suppose $\{\mathbb{P}_0, \ldots, \mathbb{P}_n\}$ is a Laurent σ-essential system. Since $\mathcal{I}_{\mathbf{u}}$ is a reflexive prime σ-ideal of codimension one, by Lemma 2.6, there exists a unique irreducible σ-polynomial $\mathbf{R}(\mathbf{u}_0, \ldots, \mathbf{u}_n) \in \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$ 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,

Lemma 3.7 *Among all the polynomials in $\mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$ vanishing at $(\mathbf{u}; \zeta_0, \ldots, \zeta_n)$, $\mathbf{R}$ is of minimal order and degree in each u_{i0} $(i = 0, \ldots, n)$.*

Now the definition of sparse σ-resultant is given as follows:

Definition 3.8 *The above $\mathbf{R} \in \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$ is defined to be the* sparse difference resultant *of the Laurent σ-essential system $\mathbb{P}_0, \ldots, \mathbb{P}_n$, denoted by $\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n}$ or $\mathrm{Res}_{\mathbb{P}_0,\ldots,\mathbb{P}_n}$.*

We give an example to show that for a Laurent σ-essential system, $\mathbf{R}$ may not involve the coefficients of some $\mathbb{P}_i$.

Example 3.9 *Let $n = 2$ and $\mathbb{P}_i$ has the form $\mathbb{P}_0 = u_{00} + u_{01}y_1y_2$, $\mathbb{P}_1 = u_{10} + u_{11}y_1^{(1)}y_2^{(1)}$, $\mathbb{P}_2 = u_{20} + u_{21}y_1^{(1)}y_2$. Clearly, $\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2$ form a Laurent σ-essential system. The sparse σ-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 3.9 can be used to illustrate the difference between the differential and difference cases. If $\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2$ are differential polynomials, then the sparse differential resultant is $u_{01}u_{11}u_{20}u_{21}u'_{00} - u_{11}u_{20}u_{00}u_{21}u'_{01} - u_{11}u_{20}^2u_{01}^2 - u_{01}u_{00}u_{21}^2u_{10}$, which contains all the coefficients of $\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2$.

We now define the sparse σ-resultant for specific Laurent σ-polynomials. For any finite set $\mathcal{A}$ of Laurent σ-monomials in $\mathbb{Y}$, let $\mathcal{L}(\mathcal{A}) = \{\sum_{M\in\mathcal{A}} a_M M\}$ where the a_M are in some σ-extension field of $\mathbb{Q}$. Then $\mathcal{L}(\mathcal{A})$ can be considered as the set of all l-tuples over $\mathbb{Q}$ where $l = |\mathcal{A}|$.

Definition 3.10 *Let $\mathcal{A}_i = \{M_{i0}, \ldots, M_{il_i}\}$ $(i = 0, \ldots, n)$ be a Laurent σ-essential system. Consider $n+1$ Laurent σ-polynomials $(F_0, \ldots, F_n) \in \prod_{i=0}^n \mathcal{L}(\mathcal{A}_i)$. The sparse σ-resultant of $F_0, \ldots, F_n$ is obtained by replacing $\mathbf{u}_i$ by the corresponding coefficient vector of F_i in $\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n}(\mathbf{u}_0, \ldots, \mathbf{u}_n)$.*

The following lemma shows that the sparse σ-resultant gives a necessary condition for a system to have common nonzero solutions.

Lemma 3.11 *Suppose $(F_0, \ldots, F_n) \in \prod_{i=0}^n \mathcal{L}(\mathcal{A}_i)$ have common nonzero solutions. Then $\mathrm{Res}_{F_0,\ldots,F_n} = 0$.*

Proof: By Definition 3.8, $\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n} \in [\mathbb{P}_0, \ldots, \mathbb{P}_n]$. If the F_i have a common nonzero solution, clearly, $\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n}$ vanishes at the coefficients of F_i. □

3.3 Criterion for Laurent transformally essential systems in terms of the supports

Let $\mathcal{A}_i$ $(i = 0, \ldots, n)$ be finite sets of Laurent σ-monomials. According to Definition 3.4, in order to check whether they are Laurent σ-essential, we need to check whether there exist $M_{ik_i} \in \mathcal{A}_i$ s.t. $\triangle\mathrm{tr.deg}\,\mathbb{Q}\langle M_{0k_0}/M_{00}, \ldots, M_{nk_n}/M_{n0}\rangle/\mathbb{Q} = n$. This can be done with the characteristic set method [14]. In this section, we will give a conceptually and computationally simpler criterion which is based on linear algebra.

Let $B_i = \prod_{j=1}^n \prod_{k\geq 0}^s (y_j^{(k)})^{d_{ijk}}$ $(i = 1, \ldots, m)$ be Laurent σ-monomials. We now introduce a new algebraic indeterminate x and let $d_{ij} = \sum_{k=0}^s d_{ijk}x^k$ $(i = 1, \ldots, m; j = 1, \ldots, n)$ be univariate polynomials in $\mathbb{Z}[x]$. If y_j and its transforms do not occur in B_i, 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 $M = (d_{ij})_{m\times n}$ is called the *symbolic support matrix* of $B_1, \ldots, B_m$.

Definition 3.12 *A matrix $M = (d_{ij})_{m\times n}$ over $\mathbb{Q}(x)$ is called* normal upper-triangular of rank r *if for each $i \leq r$, $d_{ii} \neq 0$ and $d_{i,i-k} = 0$ $(1 \leq k \leq i-1)$, and the last $m - r$ rows are zero vectors.*

Definition 3.13 *A set of Laurent σ-monomials $B_1, \ldots, B_m$ is said to be in r-*upper-triangular *form if its symbolic support matrix is a normal upper-triangular matrix of rank r.*

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

Lemma 3.14 *Let $B_1, \ldots, B_m$ be an r-upper-triangular set. Then $\triangle\mathrm{tr.deg}\,\mathbb{Q}\langle B_1, \ldots, B_m\rangle/\mathbb{Q} = r$.*

Proof: Clearly, for each $i \leq r$, $B_i = \prod_{j=i}^n \prod_{k\geq 0}(y_j^{(k)})^{d_{ijk}}$ with $\mathrm{ord}(B_i, y_i) \geq 0$, and $B_{r+k} = 1\,(k > 0)$. Let $B'_i = \prod_{j=i}^r \prod_{k\geq 0}(y_j^{(k)})^{d_{ijk}}$. Then $r \geq \triangle\mathrm{tr.deg}\,\mathbb{Q}\langle B_1, \ldots, B_m\rangle/\mathbb{Q} \geq \triangle\mathrm{tr.deg}\,\mathbb{Q}\langle B'_1, \ldots, B'_r\rangle/\mathbb{Q}$. So it suffices to prove that $\triangle\mathrm{tr.deg}\,\mathbb{Q}\langle B'_1, \ldots, B'_r\rangle/\mathbb{Q} = r$.

It is clear for $r = 1$. Suppose it holds for $r-1$. Let $B''_i = \prod_{j=i}^{r-1} \prod_{k\geq 0}(y_j^{(k)})^{d_{ijk}}$, then $\triangle\mathrm{tr.deg}\,\mathbb{Q}\langle B''_1, \ldots, B''_{r-1}\rangle/\mathbb{Q} = r-1$. Thus, $\triangle\mathrm{tr.deg}\,\mathbb{Q}\langle B'_1, \ldots, B'_r\rangle/\mathbb{Q} = \triangle\mathrm{tr.deg}\,\mathbb{Q}\langle B'_r\rangle/\mathbb{Q} + \triangle\mathrm{tr.deg}\,\mathbb{Q}\langle B'_1, \ldots, B'_r\rangle/\mathbb{Q}\langle B'_r\rangle \geq 1 + \triangle\mathrm{tr.deg}\,\mathbb{Q}\langle B''_1, \ldots, B''_{r-1}\rangle/\mathbb{Q} = r$. So $\triangle\mathrm{tr.deg}\mathbb{Q}\langle B_1, \ldots, B_m\rangle/\mathbb{Q} = r$ follows. □

In the following, we will show that each set of Laurent difference monomials can be transformed to an upper-triangular set with the same σ-transcendence degree. Here we use three types of elementary matrix transformations. For a matrix M over $\mathbb{Q}[x]$, Type 1 (resp. Type 3) operations consist of interchanging two rows (resp. columns) of M; and Type 2 operations consist of adding an $f(x)$-multiple of the j-th row to the i-th row, where $f(x) \in \mathbb{Q}[x]$. Note that these operations correspond to certain transformations of the σ-monomials. For example, multiplying the i-th row of M by a polynomial $f(x) = a_dx^d + \cdots + a_0$ and adding the result to the j-th row means changing B_j to $\prod_{k=0}^d (\sigma^k B_i)^{a_k} B_j$.

Lemma 3.15 *Let $C_1, \ldots, C_m$ be obtained from $B_1, \ldots, B_m$ by performing a series of transformations. Then*
$\triangle\mathrm{tr.deg}\,\mathbb{Q}\langle B_1, \ldots, B_m\rangle/\mathbb{Q} = \triangle\mathrm{tr.deg}\,\mathbb{Q}\langle C_1, \ldots, C_m\rangle/\mathbb{Q}$.

Proof: It suffices to show Type 2 operations keep the σ-transcendence degree. Indeed, given $\sum_{i=0}^d \frac{p_i}{q}x^i \in \mathbb{Q}[x]$ with $p_i, q \in \mathbb{Z}^*$, $\triangle\mathrm{tr.deg}\,\mathbb{Q}\langle B_1, \prod_{k=0}^d (B_1^{(k)})^{a_k}B_2\rangle/\mathbb{Q} = \triangle\mathrm{tr.deg}\,\mathbb{Q}\langle \prod_{k=0}^d (B_1^{(k)})^{p_k}, \prod_{k=0}^d (B_1^{(k)})^{p_k}B_2^q\rangle/\mathbb{Q} = \triangle\mathrm{tr.deg}\,\mathbb{Q}\langle B_1, B_2\rangle/\mathbb{Q}$. □

Theorem 3.16 *Suppose M is the symbolic support matrix of $B_1, \ldots, B_m$. Then $\triangle\mathrm{tr.deg}\,\mathbb{Q}\langle B_1, \ldots, B_m\rangle/\mathbb{Q} = \mathrm{rk}(M)$.*

Proof: Since $\mathbb{Q}[x]$ is an Euclidean domain, it is clear that each matrix M can be reduced to a normal upper-triangular matrix by performing a series of elementary transformations. By Lemma 3.14 and Lemma 3.15, the theorem follows. □

Example 3.17 *Let $B_1 = y_1y_2$ and $B_2 = y_1^{(a)}y_2^{(b)}$. Then $M = \begin{pmatrix} 1 & 1 \\ x^a & x^b \end{pmatrix}$ and $\mathrm{rk}(M) = \begin{cases} 1 & \text{if } a = b \\ 2 & \text{if } a \neq b. \end{cases}$ Thus, by Theorem 3.16, if $a \neq b$, B_1 and B_2 are σ-independent over $\mathbb{Q}$. Otherwise, they are σ-dependent over $\mathbb{Q}$.*

Consider the set of generic Laurent σ-polynomials defined in (1). 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 $M_{\mathbb{P}}$ whose

rows are $w_0, \ldots, w_n$ is called the *symbolic support matrix* of $\mathbb{P}_0, \ldots, \mathbb{P}_n$.

Now, we give the main theorem in this section.

Theorem 3.18 *$\mathbb{P}_0, \ldots, \mathbb{P}_n$ form a Laurent σ-essential system if and only if* $\mathrm{rk}(M_{\mathbb{P}}) = n$.

Proof: By Theorem 3.16 and Definition 3.4, $\mathbb{P}_0, \ldots, \mathbb{P}_n$ are Laurent σ-essential iff there exist M_{ik_i} with $1 \leq k_i \leq l_i$ s.t. the symbolic support matrix of $M_{0k_0}/M_{00}, \ldots, M_{nk_n}/M_{n0}$ is of rank n. And the latter is equivalent to $\mathrm{rk}(M_{\mathbb{P}}) = n$. □

We will end this section by introducing a new notion, namely super-essential systems. Let $\mathbb{T} \subset \{0, 1, \ldots, n\}$. We denote by $\mathbb{P}_{\mathbb{T}}$ the Laurent σ-polynomial set consisting of $\mathbb{P}_i$ $(i \in \mathbb{T})$, and $M_{\mathbb{P}_{\mathbb{T}}}$ its symbolic support matrix.

Definition 3.19 *Let $\mathbb{T} \subset \{0, 1, \ldots, n\}$. Then we call $\mathbb{T}$ or $\mathbb{P}_{\mathbb{T}}$* super-essential *if* $\mathrm{card}(\mathbb{T}) - \mathrm{rk}(\mathrm{M}_{\mathbb{P}_{\mathbb{T}}}) = 1$ *and for each $\mathbb{J} \subsetneq \mathbb{T}$,* $\mathrm{card}(\mathbb{J}) = \mathrm{rk}(\mathrm{M}_{\mathbb{P}_{\mathbb{J}}})$.

Note that super-essential systems are the difference analogue of essential systems introduced in [27] and also that of rank essential systems introduced in [21].

Theorem 3.20 *If $\{\mathbb{P}_0, \ldots, \mathbb{P}_n\}$ is a Laurent σ-essential system, then for any $\mathbb{T} \subset \{0, 1, \ldots, n\}$,* $\mathrm{card}(\mathbb{T}) - \mathrm{rk}(\mathrm{M}_{\mathbb{P}_{\mathbb{T}}}) \leq 1$ *and there exists a unique $\mathbb{T}$ which is super-essential. In this case, the sparse σ-resultant of $\mathbb{P}_0, \ldots, \mathbb{P}_n$ involves only the coefficients of $\mathbb{P}_i$ $(i \in \mathbb{T})$.*

Proof: By [22, Theorem 3.24], the theorem follows. □

Using this property, one can determine which polynomial is needed for computing the sparse σ-resultant, which will eventually reduce the computation complexity.

Example 3.21 *Continue from Example 3.9. It is easy to show that $\mathbb{P}_0, \mathbb{P}_1$ constitute a super-essential system. Recall that the sparse σ-resultant is free from the coefficients of $\mathbb{P}_2$.*

4. BASIC PROPERTIES OF SPARSE DIFFERENCE RESULTANT

In this section, we will prove some basic properties for the sparse σ-resultant $\mathbf{R}(\mathbf{u}_0, \ldots, \mathbf{u}_n)$.

4.1 Sparse difference resultant is transformally homogeneous

We introduce the concept of σ-homogeneous polynomials.

Definition 4.1 *A σ-polynomial $f \in \mathcal{F}\{y_0, \ldots, y_n\}$ is called* transformally homogeneous *if for a new σ-indeterminate λ, there exists a σ-monomial $M(\lambda)$such that $f(\lambda y_0, \ldots, \lambda y_n) = M(\lambda) f(y_0, \ldots, y_n)$. And f is called σ-homogeneous of degree m if $\deg(M(\lambda)) = m$.*

The difference analogue of Euler's theorem related to homogeneous polynomials is valid.

Lemma 4.2 *$f \in \mathcal{F}\{y_0, y_1, \ldots, y_n\}$ is σ-homogeneous if and only if for each $r \in \mathbb{N}_0$, there exists $m_r \in \mathbb{N}_0$ such that*

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

Sparse σ-resultants have the following property.

Theorem 4.3 *The sparse σ-resultant is σ-homogeneous in each $\mathbf{u}_i$ which is the coefficient set of $\mathbb{P}_i$.*

Proof: Suppose $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) = h_i \geq 0$. Follow the notations used in Theorem 3.5. By Lemma 3.7, $\mathbf{R}(\mathbf{u}; \zeta_0, \ldots, \zeta_n) = 0$. Differentiating this identity w.r.t. $u_{ij}^{(k)}$ $(j = 1, \ldots, l_i)$ respectively, we have

$$\overline{\frac{\partial \mathbf{R}}{\partial u_{ij}^{(k)}}} + \overline{\frac{\partial \mathbf{R}}{\partial u_{i0}^{(k)}}} \Big(- \frac{M_{ij}(\eta)}{M_{i0}(\eta)} \Big)^{(k)} = 0. \tag{4}$$

In the above equations, $\overline{\frac{\partial \mathbf{R}}{\partial u_{ij}^{(k)}}} = \frac{\partial \mathbf{R}}{\partial u_{ij}^{(k)}}\Big|_{(u_{00}, \ldots, u_{n0}) = (\zeta_0, \ldots, \zeta_n)}$.

Multiplying (4) by $u_{ij}^{(k)}$ and for j from 1 to l_i, adding them together, we get $\overline{\frac{\partial \mathbf{R}}{\partial u_{i0}^{(k)}}} \zeta_i^{(k)} + \sum_{j=1}^{l_i} u_{ij}^{(k)} \overline{\frac{\partial \mathbf{R}}{\partial u_{ij}^{(k)}}} = 0$. Thus, $f_k = \sum_{j=0}^{l_i} u_{ij}^{(k)} \frac{\partial \mathbf{R}}{\partial u_{ij}^{(k)}}$ vanishes at $(\zeta_0, \ldots, \zeta_n)$. Since $\mathrm{ord}(f_k, u_{i0}) \leq \mathrm{ord}(\mathbf{R}, u_{i0})$ and $\deg(f_k) = \deg(\mathbf{R})$, by Lemma 3.7, there exists an $m_k \in \mathbb{Z}$ such that $f_k = m_k \mathbf{R}$. Thus, by Lemma 4.2, $\mathbf{R}$ is σ-homogeneous in $\mathbf{u}_i$. □

4.2 Order bound in terms of Jacobi number

In this section, we will give an order bound for the sparse σ-resultant in terms of the Jacobi number of the given system.

Consider a generic Laurent σ-essential system $\{\mathbb{P}_0, \ldots, \mathbb{P}_n\}$ defined in (1) with $\mathbf{u}_i$ being the coefficient vector of $\mathbb{P}_i$. Suppose $\mathbf{R}$ is the sparse σ-resultant of $\mathbb{P}_0, \ldots, \mathbb{P}_n$. Denote $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) = \max_k \mathrm{ord}(\mathbf{R}, u_{ik})$. If $\mathbf{u}_i$ does not occur in $\mathbf{R}$, then set $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) = -\infty$.

Lemma 4.4 *For fixed i and s, if there exists a k_0 such that $\deg(\mathbf{R}, u_{ik_0}^{(s)}) > 0$, then for all $k \in \{0, \ldots, l_i\}$, $\deg(\mathbf{R}, u_{ik}^{(s)}) > 0$. In particular,* $\mathrm{ord}(\mathbf{R}, u_{ik}) = \mathrm{ord}(\mathbf{R}, \mathbf{u}_i)$ $(k = 0, \ldots, l_i)$.

Proof: By (4) and lemma 3.7, the lemma follows. □

Let $s_{ij} = \mathrm{ord}(\mathrm{N}(\mathbb{P}_i), y_j)$ 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 $\mathbb{P}_0, \ldots, \mathbb{P}_n$. By $A_{\hat{i}}$, we mean the submatrix of A obtained by deleting the $(i+1)$-th row from A. We use $\mathbb{P}$ to denote the set $\{\mathrm{N}(\mathbb{P}_0), \ldots, \mathrm{N}(\mathbb{P}_n)\}$ and by $\mathbb{P}_{\hat{i}}$, we mean the set $\mathbb{P} \backslash \{\mathrm{N}(\mathbb{P}_i)\}$. For a matrix $B = (a_{ij})_{n \times n}$, the *Jacobi number* is $\mathrm{Jac}(B) = \max_{\tau \in S_n} \{a_{1\tau(1)} + \cdots + a_{n\tau(n)}\}$, where S_n is the set of all permutations of $\{1, \ldots, n\}$. We call $J_i = \mathrm{Jac}(A_{\hat{i}})$ the *Jacobi number* of the system $\mathbb{P}_{\hat{i}}$, also denoted by $\mathrm{Jac}(\mathbb{P}_{\hat{i}})$.

The following theorem shows that Jacobi numbers are order bounds for sparse σ-resultants.

Theorem 4.5 *Let $\mathbb{P}$ be a Laurent σ-essential system and $\mathbf{R}$ the sparse σ-resultant of $\mathbb{P}$. Then*

$$\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) = \begin{cases} -\infty & \text{if} \quad J_i = -\infty, \\ h_i \leq J_i & \text{if} \quad J_i \geq 0. \end{cases}$$

Proof: For details, see [22, Theorem 4.14]. □

Example 4.6 *Let $n = 2$ and $\mathbb{P}_i$ have the form $\mathbb{P}_0 = u_{00} + u_{01} y_1 y_1^{(1)}$, $\mathbb{P}_1 = u_{10} + u_{11} y_1$, $\mathbb{P}_2 = u_{10} + u_{11} y_2^{(1)}$. In this example, $J_0 = 1, J_1 = 2, J_2 = -\infty$. And $\mathrm{ord}(\mathbf{R}, \mathbf{u}_0) = 0 < J_0, \mathrm{ord}(\mathbf{R}, \mathbf{u}_1) = 1 < J_1, \mathrm{ord}(\mathbf{R}, \mathbf{u}_2) = -\infty$.*

5. SINGLE EXPONENTIAL ALGORITHM

In this section, we give an algorithm to compute the sparse σ-resultant for a Laurent σ-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.

The following result gives an upper bound for the degree of the sparse σ-resultant.

Theorem 5.1 *Let $\mathbb{P}_0, \ldots, \mathbb{P}_n$ be a Laurent σ-essential system of form (1) with $\mathrm{ord}(\mathrm{N}(\mathbb{P}_i)) = s_i$ and $\deg(\mathrm{N}(\mathbb{P}_i), \mathbb{Y}) = m_i$. Suppose $\mathrm{N}(\mathbb{P}_i) = \sum_{k=0}^{l_i} u_{ik} N_{ik}$ and $J_i = \mathrm{Jac}(\mathbb{P}_{\hat{i}})$. Denote $m = \max_i\{m_i\}$. Let $\mathbf{R}$ be the sparse difference resultant of $\mathbb{P}_i$ $(i = 0, \ldots, n)$. Suppose $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) = h_i$ for each i. Then*

1) $\deg(\mathbf{R}) \leq \prod_{i=0}^{n}(m_i+1)^{h_i+1} \leq (m+1)^{\sum_{i=0}^{n}(J_i+1)}$.

2) $\mathbf{R}$ *has a representation*

$$\prod_{i=0}^{n}\prod_{k=0}^{n}(N_{i0}^{(k)})^{\deg(\mathbf{R})} \cdot \mathbf{R} = \sum_{i=0}^{n}\sum_{k=0}^{h_i} G_{ik}\mathrm{N}(\mathbb{P}_i)^{(k)} \qquad (5)$$

where $G_{ik} \in \mathbb{Q}[\mathbf{u}_0^{[h_0]}, \ldots, \mathbf{u}_n^{[h_n]}, \mathbb{Y}^{[h]}]$ and $h = \max\{h_i + e_i\}$ such that $\deg(G_{ik}\mathrm{N}(\mathbb{P}_i)^{(k)}) \leq [m + 1 + \sum_{i=0}^{n}(h_i + 1)\deg(N_{i0})]\deg(\mathbf{R})$.

Proof: We sketch the proof here. In $\mathbf{R}$, replace u_{i0} by $\big(\mathrm{N}(\mathbb{P}_i) - \sum_{k=1}^{l_i} u_{ik}N_{ik}\big)/N_{i0}$ for each $i = 0, \ldots, n$ and let $\mathbf{R}$ be expanded as a σ-polynomial in $\mathrm{N}(\mathbb{P}_i)$ and their transforms. (5) follows from the fact that $\mathcal{I} \cap \mathbb{Q}\{\mathbf{u}, \mathbb{Y}\} = \{0\}$. To obtain the degree bound of $\mathbf{R}$, we consider the algebraic ideal $\mathcal{J} = \big(\mathrm{N}(\mathbb{P}_0)^{[h_0]}, \ldots, \mathrm{N}(\mathbb{P}_n)^{[h_n]}\big) : \mathbf{m}^{[h]}$. By Bézout theorem, $\deg(\mathcal{J}) \leq \prod_{i=0}^{n}(m_i+1)^{h_i+1}$. Since $\mathcal{J} \cap \mathbb{Q}[\mathbf{u}_0^{[h_0]}, \ldots, \mathbf{u}_n^{[h_n]}] = (\mathbf{R})$, by [20, Theorem 2.1], $\deg(\mathbf{R}) \leq \deg(\mathcal{J})$ and 1) follows. In order to estimate $\deg(G_{ik}\mathrm{N}(\mathbb{P}_i)^{(k)})$ and a_{ik}, it suffices to consider each monomial M in $\mathbf{R}$ and substitute u_{i0} by $\big(\mathrm{N}(\mathbb{P}_i) - \sum_{k=1}^{l_i} u_{ik}N_{ik}\big)/N_{i0}$ into M and then expand it. □

With given order and degree bounds, we can give the algorithm **SDResultant** to compute sparse σ-resultants based on linear algebra techniques.

Theorem 5.2 *Let $\mathbb{P}_0, \ldots, \mathbb{P}_n$ be a Laurent σ-essential system of form (1). Denote $\mathbb{P} = \{\mathrm{N}(\mathbb{P}_0), \ldots, \mathrm{N}(\mathbb{P}_n)\}$, $J_i = \mathrm{Jac}(\mathbb{P}_{\hat{i}})$, $J = \max_i J_i$ and $m = \max_{i=0}^{n}\deg(\mathbb{P}_i, \mathbb{Y})$. Algorithm* **SDResultant** *computes sparse σ-resultant $\mathbf{R}$ of $\mathbb{P}_0, \ldots, \mathbb{P}_n$ with the following complexities:*

1) In terms of a given degree bound D of $\mathbf{R}$, the algorithm needs at most $O(D^{O(lJ)}(nJ)^{O(lJ)})$ $\mathbb{Q}$-arithmetic operations, where $l = \sum_{i=0}^{n}(l_i + 1)$ is the size of all $\mathbb{P}_i$.

2) The algorithm needs at most $O(m^{O(nlJ^2)}(nJ)^{O(lJ)})$ $\mathbb{Q}$-arithmetic operations.

Proof: In each loop of Step 3, the complexity 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 $\mathbf{c}_{ij}$. $\mathcal{P} = 0$ is a linear system with $N = \binom{d+L-1}{L-1} + \sum_{i=0}^{n}(h_i+1)\binom{d_1-m_i-1+L+n(h+1)}{L+n(h+1)}$ variables and $M = \binom{d_1+L+n(h+1)}{L+n(h+1)}$ equations, where $L = \sum_{i=0}^{n}(h_i+1)(l_i+1)$. So we need at most $(\max\{M, N\})^{\omega}$ arithmetic operations over $\mathbb{Q}$ to solve it, where ω is the matrix multiplication exponent and the currently best known ω is 2.376.

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

Input: A generic Laurent σ-essential system $\mathbb{P}_0, \ldots, \mathbb{P}_n$.
Output: The sparse σ-resultant $\mathbf{R}$ of $\mathbb{P}_0, \ldots, \mathbb{P}_n$.

1. Set $\mathrm{N}(\mathbb{P}_i) = \sum_{k=0}^{l_i} u_{ik}N_{ik}$ with $\deg(N_{i0}) \leq \deg(N_{ik})$.
   Set $m_i = \deg(\mathrm{N}(\mathbb{P}_i))$, $m_{i0} = \deg(N_{i0})$, $\mathbf{u}_i = \mathrm{coeff}(\mathbb{P}_i)$.
   Set $s_{ij} = \mathrm{ord}(\mathrm{N}(\mathbb{P}_i), y_j)$, $A = (s_{ij})$, $J_i = \mathrm{Jac}(A_{\hat{i}})$.
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 $h_i \leq J_i$ do
      3.1.1. $U = \cup_{i=0}^{n}\mathbf{u}_i^{[h_i]}$, $h = \max_i\{h_i + e_i\}$, $d = 1$.
      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 GHPol of degree d in U.
         3.1.2.2. Set $\mathbf{c}_0 = \mathrm{coeff}(\mathbf{R}_0, U)$.
         3.1.2.3. Set H_{ij} to be GPols in $\mathbb{Y}^{[h]}, U$ of degree $[m + 1 + \sum_{i=0}^{n}(h_i+1)m_{i0}]d - m_i - 1$.
         3.1.2.4. Set $\mathbf{c}_{ij} = \mathrm{coeff}(H_{ij}, \mathbb{Y}^{[h]} \cup U)$.
         3.1.2.5. Set $\mathcal{P}$ to be the set of coefficients of $\prod_{i=0}^{n}\prod_{k=0}^{h_i}(N_{i0}^{(k)})^d\mathbf{R}_0 - \sum_{i=0}^{n}\sum_{j=0}^{h_i} H_{ij}(\mathrm{N}(\mathbb{P}_i))^{(j)}$ as a polynomial in $\mathbb{Y}^{[h]}, U$.
         3.1.2.6. Solve linear equations $\mathcal{P}(\mathbf{c}_0, \mathbf{c}_{ij}) = 0$.
         3.1.2.7. If $\mathbf{c}_0$ has a nonzero solution $\bar{\mathbf{c}}_0$, then $\mathbf{R} = \mathbf{R}_0(\bar{\mathbf{c}}_0)$ and goto 4., else $\mathbf{R} = 0$.
         3.1.2.8. d:=d+1.
   3.2. o:=o+1.
4. Return $\mathbf{R}$.

/*/ GPol(GHpol) stands for generic (homogenous) poly.
/*/ $\mathrm{coeff}(P, V)$ returns coefficients of P in variables V.

The iteration in Step 3.1.2 may go through 1 to $\prod_{i=0}^{n}(m_i+1)^{h_i+1}$, and the iteration in Step 3.1 at most will repeat $\prod_{i=0}^{n}(J_i+1)$ times. And by Theorem 5.1, Step 3 may loop from $o = 0$ to $\sum_{i=0}^{n}(J_i+1)$. Thus, the complexity follows. □

6. DIFFERENCE RESULTANT

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

Definition 6.1 *Let $\mathbf{m}_{s,r}$ be the set of all σ-monomials in $\mathbb{Y}$ of order $\leq s$ and degree $\leq r$. Let $\mathbf{u} = \{u_M\}_{M \in \mathbf{m}_{s,r}}$ be a set of σ-indeterminates over $\mathbb{Q}$. Then, $\mathbb{P} = \sum_{M \in \mathbf{m}_{s,r}} u_M M$ is called a* generic σ-polynomial *of order s and degree r.*

Throughout this section, a generic σ-polynomial is assumed to be of degree greater than zero. Let

$$\mathbb{P}_i = u_{i0} + \sum_{\substack{\alpha \in \mathbb{Z}_{\geq 0}^{n(s_i+1)} \\ 1 \leq |\alpha| \leq m_i}} u_{i\alpha}(\mathbb{Y}^{[s_i]})^{\alpha} \; (i = 0, \ldots, n) \qquad (6)$$

be generic σ-polynomials of order s_i, degree m_i, and coefficients $\mathbf{u}_i$ respectively. Clearly, they form a super-essential system. We define the sparse σ-resultant $\mathrm{Res}_{\mathbb{P}_0,\ldots,\mathbb{P}_n}$ to be the *difference resultant* of $\mathbb{P}_0, \ldots, \mathbb{P}_n$. That is, The *difference resultant* of $\mathbb{P}_0, \ldots, \mathbb{P}_n$ is defined as the irreducible σ-polynomial of minimal order in each $\mathbf{u}_i$ which is contained in $[\mathbb{P}_0, \ldots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$.

Difference resultants satisfy all the properties we have proved for sparse σ-resultants in previous sections. Apart from these, in the following, we will show σ-resultants possess other better properties. Firstly, we will give the precise degree for the σ-resultant, which is of BKK-type [1, 6]. Here, we need results about algebraic sparse resultants from [27]. For what needed here, please refer to [22, Sec. 6].

Theorem 6.2 *Let $\mathbf{R}(\mathbf{u}_0, \ldots, \mathbf{u}_n)$ be the σ-resultant of the $n+1$ generic σ-polynomials $\mathbb{P}_0, \ldots, \mathbb{P}_n$ in (6). Denote $s = \sum_{i=0}^n s_i$. Then $\mathrm{ord}(\mathbf{R}, \mathbf{u}_i) = s - s_i$ and $\mathbf{R}(\mathbf{u}_0, \ldots, \mathbf{u}_n)$ is also the algebraic sparse resultant of $\mathbb{P}_0^{[s-s_0]}, \ldots, \mathbb{P}_n^{[s-s_n]}$ as polynomials in $\mathbb{Y}^{[s]}$. In particular, for each i and k, $\deg(\mathbf{R}, \mathbf{u}_i^{(k)})$ is equal to the mixed volume of the* Newton *polytopes of $\bigcup_{j=0}^n \mathbb{P}_j^{[s-s_j]} \backslash \{\mathbb{P}_i^{(k)}\}$.*

Proof: Regard $\mathbb{P}_i^{(k)}$ as polynomials in the $n(s+1)$ variables $\mathbb{Y}^{[s]}$, and we denote its support by $\mathcal{B}_{ik}$. Since the coefficients of $\mathbb{P}_i^{(k)}$ are algebraic indeterminates, $\mathbb{P}_i^{(k)}$ are generic sparse polynomials with supports $\mathcal{B}_{ik}$ respectively. We claim that:

C1) $\overline{\mathcal{B}} = \{\mathcal{B}_{ik} : 0 \le i \le n; 0 \le k \le s - s_i\}$ is essential.

C2) $\overline{\mathcal{B}}$ 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 $l \in \{0, \ldots, s - s_0\}$,

$$S_l = \{(\mathbb{P}_i^{[s-s_i]})_{1 \le i \le n}, \mathbb{P}_0, \ldots, \mathbb{P}_0^{(l-1)}, \mathbb{P}_0^{(l+1)}, \ldots, \mathbb{P}_0^{(s-s_0)}\}$$

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

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

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

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

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

So $m(S_l)$ is equal to $\{y_j^{[s]} : 1 \le j \le n\}$, which are algebraically independent over $\mathbb{Q}$. Thus, by the algebraic version of Lemma 2.1,the $n(s+1)$ members of S_l are algebraically independent over $\mathbb{Q}$ and 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 $(\mathbb{P}_i^{[s-s_i]})_{0 \le i \le n}$ exists and we denote it by G. Then $\mathrm{ord}(G, \mathbf{u}_i) = s - s_i$ and $G \in [\mathbb{P}_0, \ldots, \mathbb{P}_n]$. By Lemma 3.7 and C1) again, $\mathbf{R} = c \cdot G$ for some $c \in \mathbb{Q}$. Thus, $\mathbf{R}$ is equal to the algebraic sparse resultant of $\mathbb{P}_0^{[s-s_0]}, \ldots, \mathbb{P}_n^{[s-s_n]}$ and the theorem follows. □

As a direct consequence of the above theorem and the determinant representation for algebraic sparse resultant given by D'Andrea [7], we have the following result.

Corollary 6.3 *The σ-resultant of $\mathbb{P}_i$ can be written as the form $\det(M_1)/\det(M_0)$ where M_1 and M_0 are matrices whose elements are coefficients of $\mathbb{P}_i$ and their transforms up to the order $s - s_i$ and M_0 is a minor of M_1.*

Based on the matrix representation given as above, the single exponential algorithms given by Canny, Emiris, and Pan [10, 11] can be used to compute σ-resultants.

Now, we proceed to give a Poisson-type product formula for σ-resultant. Let $\tilde{\mathbf{u}} = \cup_{i=0}^n \mathbf{u}_i \setminus \{u_{00}\}$ and $\mathbb{Q}\langle\tilde{\mathbf{u}}\rangle$ be the σ-transcendental extension of $\mathbb{Q}$ in the usual sense. Let $\mathbb{Q}_0 = \mathbb{Q}\langle\tilde{\mathbf{u}}\rangle(u_{00}, \ldots, u_{00}^{(s-s_0-1)})$. Here, $\mathbb{Q}_0$ is not necessarily a σ-overfield of $\mathbb{Q}$, for the transforms of u_{00} are not defined. Consider $\mathbf{R}$ as an irreducible polynomial $r(u_{00}^{(s-s_0)})$ in $\mathbb{Q}_0[u_{00}^{(s-s_0)}]$. In a suitable algebraic extension field of $\mathbb{Q}_0$, $\mathbf{R}(\mathbf{u}_0, \mathbf{u}_1, \ldots, \mathbf{u}_n) = A \prod_{\tau=1}^{t_0} (u_{00}^{(s-s_0)} - \gamma_\tau)$, where $A \in \mathbb{Q}_0$. Let $\mathcal{I}_{\mathbf{u}} = [\mathbb{P}_0, \ldots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$. Then by the definition of difference resultant, $\mathcal{I}_{\mathbf{u}}$ is an essential reflexive prime σ-ideal in the decomposition of $\{\mathbf{R}\}$ which is not held by any σ-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[1] of $\mathbf{R}$ corresponding to $\mathcal{I}_{\mathbf{u}}$. That is, $\mathcal{I}_{\mathbf{u}} = \bigcup_{k \ge 0} \mathrm{asat}(\mathbf{R}, \mathbf{R}_1, \ldots, \mathbf{R}_k)$. Let $(\gamma_\tau, \gamma_{\tau 1}, \ldots, \gamma_{\tau k})$ be a generic zero of $\mathrm{asat}(\mathbf{R}, \mathbf{R}_1, \ldots, \mathbf{R}_k)$ for each k. Let $\mathcal{G}_\tau = \mathbb{Q}_0(\gamma_\tau, \gamma_{\tau 1}, \ldots)$. Then $\mathcal{G}_\tau$ is isomorphic to the quotient field of $\mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}/\mathcal{I}_{\mathbf{u}}$, which is also a σ-field. So we can introduce a transforming operator σ_τ into $\mathcal{G}_\tau$ to make it a difference field such that the 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 $F \in \mathbb{Q}\{\mathbf{u}_0, \ldots, \mathbf{u}_n\}$. By saying F vanishes at $u_{00}^{(s-s_0)} = \gamma_\tau$, we mean $F|_{u_{00}^{(s-s_0+k)} = \gamma_{\tau k}, k \ge 0} = 0$. The following lemma is a direct consequence of the above discussion.

Lemma 6.4 *$F \in \mathcal{I}_{\mathbf{u}}$ iff F vanishes at $u_{00}^{(s-s_0)} = \gamma_\tau$.*

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

Difference resultants have a Poisson-type product formula which is similar to their algebraic and differential analogues.

Theorem 6.5 *Let $\mathbf{R}$ be the σ-resultant of $\mathbb{P}_0, \ldots, \mathbb{P}_n$. Let $\deg(\mathbf{R}, u_{00}^{(s-s_0)}) = t_0$. Then there exist $\xi_{\tau k}$ $(\tau = 1, \ldots, t_0; k = 1, \ldots, n)$ in overfields $(\mathcal{G}_\tau, \sigma_\tau)$ of $(\mathbb{Q}\langle\tilde{\mathbf{u}}\rangle, \sigma)$ such that*

$$\mathbf{R} = A \prod_{\tau=1}^{t_0} \mathbb{P}_0(\xi_{\tau 1}, \ldots, \xi_{\tau n})^{(s-s_0)}, \tag{7}$$

and the points $\xi_\tau = (\xi_{\tau 1}, \ldots, \xi_{\tau n})$ $(\tau = 1, \ldots, t_0)$ in (7) are generic zeroes of the σ-ideal $[\mathbb{P}_1, \ldots, \mathbb{P}_n] \subset \mathbb{Q}\langle\mathbf{u}_1, \ldots, \mathbf{u}_n\rangle\{\mathbb{Y}\}$. Note that (7) is formal and should be understood in the following precise meaning: $\mathbb{P}_0(\xi_{\tau 1}, \ldots, \xi_{\tau n})^{(s-s_0)} \triangleq \sigma^{s-s_0} u_{00} + \sigma_\tau^{s-s_0}(\sum_\alpha u_{0\alpha}(\xi_\tau^{[s-s_0]})^\alpha)$.

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

Proof: By Theorem 4.3, there exists $m \in \mathbb{N}$ s.t. $u_{00}\frac{\partial \mathbf{R}}{\partial u_{00}} + \sum_\alpha u_{0\alpha}\frac{\partial \mathbf{R}}{\partial u_{0\alpha}} = m\mathbf{R}$. Let $\xi_{\tau\alpha} = (\frac{\partial \mathbf{R}}{\partial u_{0\alpha}}/\frac{\partial \mathbf{R}}{\partial u_{00}})\big|_{u_{00}^{(s-s_0)}=\gamma_\tau}$. 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, we have $\mathbf{R} = A\prod_{\tau=1}^{t_0}(u_{00} + \sum_\alpha u_{0\alpha}\xi_{\tau\alpha})^{(s-s_0)}$. For $j = 1, \ldots, n$, let $\xi_{\tau j} = (\frac{\partial \mathbf{R}}{\partial u_{0j0}}/\frac{\partial \mathbf{R}}{\partial u_{00}})\big|_{u_{00}^{(s-s_0)}=\gamma_\tau}$, where u_{0j0} is the coefficient of y_j in $\mathbb{P}_0$. Let $\xi_\tau = (\xi_{\tau 1}, \ldots, \xi_{\tau n})$. Similar to the proof of [13, Theorem 6.4] and by Lemma 6.4, we can show that $\xi_{\tau\alpha} = (\xi_\tau^{[s_0]})^\alpha$. Thus, (7) follows. And by Lemma 6.4, it is easy to show that ξ_τ are generic zeroes of the σ-ideal $[\mathbb{P}_1, \ldots, \mathbb{P}_n] \subset \mathbb{Q}\langle \mathbf{u}_1, \ldots, \mathbf{u}_n\rangle\{\mathbb{Y}\}$. □

7. CONCLUSION AND PROBLEM

In this paper, we first introduce the concept of Laurent σ-essential systems and give a criterion for Laurent σ-essential systems in terms of their supports. Then the sparse σ-resultant for a Laurent σ-essential system is defined and its basic properties are proved. In particular, order and degree bounds are given. Based on these bounds, an algorithm to compute the sparse σ-resultant is proposed, which is single exponential in terms of the order, the number of variables, and the size of the system. Besides these, the σ-resultant is introduced and its precise order, degree, determinant representation and the Poisson-type product formula are given.

Below, we propose several questions for further study.

It is useful to represent the sparse σ-resultant as the quotient of two determinants, as done in [7, 10] in the algebraic case. In the difference case, Theorem 6.2 shows that σ-resultant has such a matrix formula, but for sparse σ-resultant, we do not have such a formula yet.

The degree of the algebraic sparse resultant is equal to the mixed volume of the Newton polytopes of certain polynomials [24] or [15, p.255]. A similar degree bound is given [21, Theorem 1.3] for the differential resultant. And Theorem 6.2 shows that the degree of σ-resultants is exactly of such BKK-type. We conjecture that sparse σ-resultant has such degree bounds.

There exist very efficient algorithms to compute algebraic sparse resultants [9, 10, 11, 7] based on matrix representations. How to apply the principles behind these algorithms to compute sparse σ-resultants is an important problem.

8. REFERENCES

[1] D. N. Bernshtein. The Number of Roots of a System of Equations. *Funct. Anal. Appl.*, 9(3), 183-185, 1975.

[2] D. Bouziane, A. Kandri Rody, and H. Maârouf. Unmixed-dimensional Decomposition of a Finitely Generated Perfect Differential Ideal. *J. Symb. Comput.*, 31(6), 631-649, 2001.

[3] J. F. Canny. Generalized Characteristic Polynomials. *J. Symb. Comput.*, 9, 241-250, 1990.

[4] R. M. Cohn. Manifolds of Difference Polynomials. *Trans. Amer. Math. Soc.*, 64(1), 1948.

[5] R. M. Cohn. *Difference Algebra*. Interscience Publishers, New York, 1965.

[6] D. Cox, J. Little, D. O'Shea. *Using Algebraic Geometry*. Springer, 1998.

[7] C. D'Andrea. Macaulay Style Formulas for Sparse Resultants. *Trans. Amer. Math. Soc.*, 354(7), 2595-2629, 2002.

[8] D. Eisenbud, F. O. Schreyer, and J. Weyman. Resultants and Chow Forms via Exterior Syzygies. *J. Amer. Math. Soc.*, 16(3), 537-579, 2004.

[9] I. Z. Emiris. On the Complexity of Sparse Elimination. *J. Complexity*, 12, 134-166, 1996.

[10] I. Z. Emiris and J. F. Canny. Efficient Incremental Algorithms for the Sparse Resultant and the Mixed Volume. *J. Symb. Comput.*, 20(2), 117-149, 1995.

[11] I. Z. Emiris and V. Y. Pan. Improved Algorithms for Computing Determinants and Resultants. *J. Complexity*, 21, 43-71, 2005.

[12] X. S. Gao and S. C. Chou. On the Dimension for Arbitrary Ascending Chains. *Chinese Bull. of Sciences,* vol. 38, 396-399, 1993.

[13] X. S. Gao, W. Li, C. M. Yuan. Intersection Theory in Differential Algebraic Geometry: Generic Intersections and the Differential Chow Form. Accepted by *Trans. of Amer. Math. Soc.*, http://dx.doi.org/10.1090/S0002-9947-2013-05633-4.

[14] X. S. Gao, Y. Luo, C. M. Yuan. A Characteristic Set Method for Ordinary difference Polynomial Systems. *J. Symb. Comput.*, 44(3), 242-260, 2009.

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

[16] W.V.D. Hodge and D. Pedoe. *Methods of Algebraic Geometry, Volume I*. Cambridge Univ. Press, 1968.

[17] J. P. Jouanolou. Le formalisme du rèsultant. *Advances in Mathematics*, 90(2), 117-263, 1991.

[18] M. Kapranov, B. Sturmfels, and A Zelevinsky. Chow Polytopes and General Resultants. *Duke Math. J.*, 67, 189-218, 1992.

[19] A. Levin. *Difference Algebra*. Springer, 2008.

[20] W. Li, X. S. Gao, C. M. Yuan. Sparse Differential Resultant. *Proc. ISSAC 2011*, 225-232, ACM Press, New York, 2011.

[21] W. Li, C. M. Yuan, X. S. Gao. Sparse Differential Resultant for Laurent Differential Polynomials. *ArXiv:1111.1084v3,* 1-70, 2012.

[22] W. Li, C. M. Yuan, X. S. Gao. Sparse Difference Resultant. *ArXiv:1212.3090v1,* 1-34, 2012.

[23] Z.M. Li. A Subresultant Theory for Linear Differential, Linear Difference and Ore Polynomials, with Applications. PhD thesis, Johannes Kepler University, Linz, 1996.

[24] P. Pedersen and B. Sturmfels. Product Formulas for Resultants and Chow Forms. *Mathematische Zeitschrift*, 214(1), 377-396, 1993.

[25] S. L. Rueda. Linear Sparse Differential Resultant Formulas. *Linear Algebra and its Applications*, 438(11), 4296-4321, 2013.

[26] B. Sturmfels. Sparse Elimination Theory. In *Computational Algebraic Geometry and Commutative Algebra*, Eisenbud, D., Robbiano, L. eds. 264-298, Cambridge University Press, 1993.

[27] B. Sturmfels. On The Newton Polytope of the Resultant. *J. Algebraic Comb.*, 3, 207-236, 1994.

[28] Z. Y. Zhang, C. M. Yuan, X. S. Gao. Matrix Formula of Differential Resultant for First Order Generic Ordinary Differential Polynomials. ArXiv:1204.3773, 2012.