Journal of Symbolic Computation 80 (2017) 665–706

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Binomial difference ideals

Xiao-Shan Gao, Zhang Huang, Chun-Ming Yuan

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

ARTICLE INFO

Article history:
Received 6 January 2016
Accepted 7 July 2016
Available online 25 July 2016

Keywords:
Laurent binomial difference ideal
Binomial difference ideal
$\mathbb{Z}[x]$-lattice
Difference characteristic set
Gröbner basis of $\mathbb{Z}[x]$-module
Generalized Hermite normal form

ABSTRACT

In this paper, binomial difference ideals are studied. Three canonical representations for Laurent binomial difference ideals are given in terms of the reduced Gröbner basis of $\mathbb{Z}[x]$-lattices, regular and coherent difference ascending chains, and partial characters on $\mathbb{Z}[x]$-lattices, respectively. Criteria for a Laurent binomial difference ideal to be reflexive, prime, well-mixed, and perfect are given in terms of their support lattices. The reflexive, well-mixed, and perfect closures of a Laurent binomial difference ideal are shown to be binomial. Most of the properties of Laurent binomial difference ideals are extended to the case of binomial difference ideals. Finally, algorithms are given to check whether a given Laurent binomial difference ideal $\mathcal{I}$ is reflexive, prime, well-mixed, or perfect, and in the negative case, to compute the reflexive, well-mixed, and perfect closures of $\mathcal{I}$. An algorithm is given to decompose a finitely generated perfect binomial difference ideal as the intersection of reflexive prime binomial difference ideals.

1. Introduction

A polynomial ideal is called binomial if it is generated by polynomials with at most two terms. Binomial ideals were first studied by Eisenbud and Sturmfels (1996), which were further studied in Barile et al. (2001), Dickenstein et al. (2010), Martínez de Castilla and Sánchez (2000), Koppenhagen and Mayr (1996), Peeva and Sturmfels (1998) and were applied in algebraic statistics (Pachter and

E-mail address: xgao@mmrc.iss.ac.cn (X.-S. Gao).

http://dx.doi.org/10.1016/j.jsc.2016.07.029
0747-7171/

Sturmfels, 2005), chemical reactions (Millán et al., 2012), and error-correcting codes (Saleemi and Zimmermann, 2010).

In this paper, we initiate the study of binomial difference ideals and hope that they will play similar roles in difference algebraic geometry to their algebraic counterparts. Difference algebra and difference algebraic geometry were founded by Ritt and Doob (1933) and Cohn (1965), who aimed to study algebraic difference equations in the way polynomial equations were studied in commutative algebra and algebraic geometry (Cohn, 1965; Hrushovski, 2012; Levin, 2008; Wibmer, 2013).

We now describe the main results of this paper. In Section 3, we prove basic properties of $\mathbb{Z}[x]$-lattices. By a $\mathbb{Z}[x]$-lattice, we mean a $\mathbb{Z}[x]$-module in $\mathbb{Z}[x]^n$. $\mathbb{Z}[x]$-lattices play the same role as $\mathbb{Z}$-lattices do in the study of binomial ideals. Here, x is used to denote the difference operator σ. For instance, $a^3\sigma(a)^2$ is denoted as a^{2x+3}. Since $\mathbb{Z}[x]$ is not a PID, the Hermite normal form for a matrix with entries in $\mathbb{Z}[x]$ does not exist. In this section, we introduce the concept of generalized Hermite normal form and show that a matrix is a generalized Hermite normal form if and only if its columns form a reduced Gröbner basis for a $\mathbb{Z}[x]$-lattice.

In Section 4, we give three canonical representations for Laurent binomial difference ideals in terms of reduced Gröbner bases of $\mathbb{Z}[x]$-lattices, difference characteristic sets, and partial characters. Gröbner bases play an important role in the study of binomial ideals (Eisenbud and Sturmfels, 1996). In general, a binomial difference ideal is not finitely generated and does not have a finite Gröbner basis. Instead, the theory of characteristic set for difference polynomial systems (Gao et al., 2009a) is used for similar purposes. It is shown that any Laurent binomial difference ideal can be written as $[\mathcal{A}]$, where $\mathcal{A}$ is a regular and coherent difference ascending chain consisting of difference binomials.

Let $\mathcal{I}$ be a proper Laurent binomial difference ideal in the Laurent difference polynomial ring $\mathcal{F}\{\mathbb{Y}^{\pm}\}$, where $\mathbb{Y} = \{y_1, y_2, \ldots, y_n\}$ is a set of difference indeterminants. Then $\mathbb{L}(\mathcal{I}) := \{\mathbf{f} \in \mathbb{Z}[x]^n \mid \mathbb{Y}^{\mathbf{f}} - c_{\mathbf{f}} \in \mathcal{I}\}$, called the *support lattice* of $\mathcal{I}$, is a $\mathbb{Z}[x]$-lattice. In Section 5, we give criteria for $\mathcal{I}$ to be prime, reflexive, well-mixed, and perfect in terms of its support lattice $\mathbb{L}(\mathcal{I})$. The criterion for prime ideals is similar to the algebraic case, but the criteria for reflexive, well-mixed, and perfect difference ideals are unique to difference algebra and are first proposed in this paper. Furthermore, it is shown that the reflexive, well-mixed, and perfect closures of a Laurent binomial difference ideal $\mathcal{I}$ with support lattice L are still binomial, whose support lattices are the x-, M-, and the P-saturation of L, respectively. It is further shown that any perfect Laurent binomial difference ideal $\mathcal{I}$ can be written as the intersection of Laurent reflexive prime binomial difference ideals whose support lattices are the x-$\mathbb{Z}$-saturation of the support lattice of $\mathcal{I}$.

In Section 6, binomial difference ideals are studied. It is shown that a large portion of the properties for binomial ideals proved in Eisenbud and Sturmfels (1996) can be easily extended to the difference case. We also identify a class of normal binomial difference ideals which are in a one to one correspondence with Laurent binomial difference ideals. With the help of this correspondence, most properties proved for Laurent binomial difference ideals are extended to the non-Laurent case. Finally, a criterion is given for a difference variety to be defined by a set of difference binomials.

In Section 7, algorithms are given to check whether a $\mathbb{Z}[x]$-lattice L is $\mathbb{Z}$-, x-, M-, or P-saturated, or equivalently, whether a Laurent binomial difference ideal $\mathcal{I}$ is prime, reflexive, well-mixed, or perfect. If the answer is negative, we can also compute the $\mathbb{Z}$-, x-, M-, or P-saturation of L and the reflexive, well-mixed, or perfect closures of $\mathcal{I}$. Based on these algorithms, we give an algorithm to decompose a finitely generated perfect binomial difference ideal as the intersection of reflexive prime binomial difference ideals. This algorithm is stronger than the general decomposition algorithm in that for general difference polynomials, it is still open on how to decompose a finitely generated perfect difference ideal as the intersection of reflexive prime difference ideals (Gao et al., 2009a).

A distinctive feature of the algorithms presented in this paper is that problems about binomial difference ideals are reduced to problems about $\mathbb{Z}[x]$-lattices which are pure algebraic and have simpler structures.

2. Preliminaries about difference algebra

In this section, some basic notations about difference algebra will be given. For more details about difference algebra, please refer to Cohn (1965), Gao et al. (2009a), Hrushovski (2012), Levin (2008), Wibmer (2013).

2.1. Difference polynomial and Laurent difference polynomial

An ordinary difference field, or simply a σ-field, is a field $\mathcal{F}$ with a third unitary operation σ satisfying: 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 $a^{(1)}$. For $n \in \mathbb{Z}_{>0}$, $\sigma^n(a) = \sigma^{n-1}(\sigma(a))$ is called the n-th transform of a and denoted by $a^{(n)}$, with the usual assumption $a^{(0)} = a$. If $\sigma^{-1}(a)$ is defined for each $a \in \mathcal{F}$, $\mathcal{F}$ is called *inversive*. Every σ-field has an inversive closure (Cohn, 1965). A typical example of inversive σ-field is the field of rational functions $\mathbb{Q}(\lambda)$ with $\sigma(f(\lambda)) = f(\lambda+1)$.

In this paper, $\mathcal{F}$ is assumed to be of characteristic zero. Furthermore, we use σ- as the abbreviation for difference or transformally.

We introduce the following useful notation. Let x be an algebraic indeterminate and $p = \sum_{i=0}^{s} c_i x^i \in \mathbb{Z}[x]$. For a in any σ-extension field of $\mathcal{F}$, denote

$$a^p = \prod_{i=0}^{s} (\sigma^i a)^{c_i}.$$

For instance, $a^{x^2-2} = a^{(2)}/a^2$. It is easy to check that for $p, q \in \mathbb{Z}[x]$, we have

$$a^{p+q} = a^p a^q, a^p b^p = (ab)^p, a^{pq} = (a^p)^q.$$

By $a^{[n]}$ we mean the set $\{a, a^{(1)}, \ldots, a^{(n)}\}$. If S is a set of elements, we denote $S^{[n]} = \cup_{a \in S} a^{[n]}$.

Let S be a subset of a σ-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 σ-subring, and the smallest σ-subfield of $\mathcal{G}$ containing $\mathcal{F}$ and S. If we denote $\Theta(S) = \{\sigma^k a | k \geq 0, a \in S\}$, then we have $\mathcal{F}\{S\} = \mathcal{F}[\Theta(S)]$ and $\mathcal{F}\langle S\rangle = \mathcal{F}(\Theta(S))$.

Now suppose $\mathbb{Y} = \{y_1, \ldots, y_n\}$ is a set of σ-indeterminates over $\mathcal{F}$. The elements of $\mathcal{F}\{\mathbb{Y}\} = \mathcal{F}[y_j^{(k)} : j = 1, \ldots, n; k \in \mathbb{N}]$ are called *σ-polynomials* over $\mathcal{F}$ in $\mathbb{Y}$, and $\mathcal{F}\{\mathbb{Y}\}$ itself is called the *σ-polynomial ring* over $\mathcal{F}$ in $\mathbb{Y}$. A *σ-polynomial ideal*, or simply a σ-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 σ-ideal*. A prime σ-ideal is a σ-ideal which is prime as an ordinary algebraic polynomial ideal. For convenience, a prime σ-ideal is assumed not to be the unit ideal in this paper. A σ-ideal $\mathcal{I}$ is called *well-mixed* if $fg \in \mathcal{I}$ implies $fg^x \in \mathcal{I}$ for $f, g \in \mathcal{F}\{\mathbb{Y}\}$. A σ-ideal $\mathcal{I}$ is called *perfect* if for any $a \in \mathbb{N}[x] \setminus \{0\}$ and $p \in \mathcal{F}\{\mathbb{Y}\}$, $p^a \in \mathcal{I}$ implies $p \in \mathcal{I}$. If S is a subset of $\mathcal{F}\{\mathbb{Y}\}$, we use (S), $[S]$, $\langle S\rangle$, and $\{S\}$ to denote the algebraic ideal, the σ-ideal, the well-mixed σ-ideal, and the perfect σ-ideal generated by S.

An n-tuple over $\mathcal{F}$ is an n-tuple of the form $\eta = (\eta_1, \ldots, \eta_n)$ where the η_i are selected from a σ-extension field of $\mathcal{F}$. For a σ-polynomial $f \in \mathcal{F}\{\mathbb{Y}\}$, η is called a *σ-zero* of f if when substituting $y_i^{(j)}$ by $\eta_i^{(j)}$ in f, the result is 0.

For $\mathbf{f} = (f_1, \ldots, f_n)^\tau \in \mathbb{Z}[x]^n$, we define $\mathbb{Y}^{\mathbf{f}} = \prod_{i=1}^{n} y_i^{f_i}$. $\mathbb{Y}^{\mathbf{f}}$ is called a *Laurent σ-monomial* in $\mathbb{Y}$ and $\mathbf{f}$ is called its *support*. A nonzero vector $\mathbf{f} = (f_1, \ldots, f_n)^\tau \in \mathbb{Z}[x]^n$ is said to be *normal* if the leading coefficient of f_s is positive, where s is the largest subscript such that $f_s \neq 0$.

A *Laurent σ-polynomial* over $\mathcal{F}$ in $\mathbb{Y}$ is an $\mathcal{F}$-linear combination of Laurent σ-monomials in $\mathbb{Y}$. Clearly, the set of all Laurent σ-polynomials form a commutative σ-ring under the obvious sum, product, and the usual transforming operator σ, where all Laurent σ-monomials are invertible. We denote the σ-ring of Laurent σ-polynomials with coefficients in $\mathcal{F}$ by $\mathcal{F}\{\mathbb{Y}^{\pm}\}$. Let p be a Laurent σ-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 called a *nonzero σ-solution* of p if $p(a_1, \ldots, a_n) = 0$.

2.2. Characteristic set for a difference polynomial system

In this section, a brief introduction to the difference characteristic set method (Gao et al., 2009a) is presented, which will be one of the main tools used in this paper.

Let f be a σ-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 $\mathrm{ord}(f, y_i)$. If y_i does not appear in f, then we set $\mathrm{ord}(f, y_i) = -\infty$. 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 *elimination ranking* $\mathcal{R}$ on $\Theta(\mathbb{Y}) = \{\sigma^k y_i | 1 \le i \le n, k \ge 0\}$ is used in this paper: $\sigma^k y_i > \sigma^l y_j$ if and only if $i > j$ or $i = j$ and $k > l$, which is a total order over $\Theta(\mathbb{Y})$. By convention, $1 < \theta y_j$ for all $\theta y_j \in \Theta(\mathbb{Y})$.

Let f be a σ-polynomial in $\mathcal{F}\{\mathbb{Y}\}$. The greatest $y_j^{(k)}$ w.r.t. $\mathcal{R}$ 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.

Let p and q be two σ-polynomials in $\mathcal{F}\{\mathbb{Y}\}$. q is said to be of *higher rank* than p if $\mathrm{ld}(q) > \mathrm{ld}(p)$ or $\mathrm{ld}(q) = \mathrm{ld}(p) = y_j^{(k)}$ and $\deg(q, y_j^{(k)}) > \deg(p, y_j^{(k)})$. Suppose $\mathrm{ld}(p) = y_j^{(k)}$. q is said to be *reduced* w.r.t. p if $\deg(q, y_j^{(k+l)}) < \deg(p, y_j^{(k)})$ for all $l \in \mathbb{N}$.

A finite sequence of nonzero σ-polynomials $\mathcal{A} : A_1, \ldots, A_m$ is said to be a *difference ascending chain*, or simply a *σ-chain*, if $m = 1$ and $A_1 \neq 0$ or $m > 1$, $A_j > A_i$ and A_j is reduced w.r.t. A_i for $1 \le i < j \le m$.

A σ-chain $\mathcal{A}$ can be written in the following form

$$\mathcal{A} : A_{11}, \ldots, A_{1k_1}, \ldots, A_{p1}, \ldots, A_{pk_p} \tag{1}$$

where $\mathrm{lvar}(A_{ij}) = y_{c_i}$ for $j = 1, \ldots, k_i$ and $\mathrm{ord}(A_{ij}, y_{c_i}) < \mathrm{ord}(A_{il}, y_{c_i})$ for $j < l$. The following σ-chain will be used in several places of this paper.

$$\mathcal{A}_1 \ : \ y_1^2 + 1, \ y_1^x - y_1, \ y_2^2 + 1, \ y_2^x + y_2 \tag{2}$$

Let $\mathcal{A} : A_1, A_2, \ldots, A_t$ be a σ-chain with I_i as the initial of A_i, and f any σ-polynomial. Then there exists an algorithm, which reduces f w.r.t. $\mathcal{A}$ to a polynomial r that is reduced w.r.t. $\mathcal{A}$ and satisfies the relation

$$\prod_{i=1}^{t} \mathrm{I}_i^{e_i} \cdot f \equiv r, \mathrm{mod}\,[\mathcal{A}], \tag{3}$$

where the $e_i \in \mathbb{N}[x]$ and $r = \mathrm{prem}(f, \mathcal{A})$ is called the *σ-remainder* of f w.r.t. $\mathcal{A}$ (Gao et al., 2009a).

A σ-chain $\mathcal{C}$ contained in a σ-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. $\mathcal{C}$. Any σ-polynomial set has a characteristic set. All elements of a σ-ideal $\mathcal{I}$ can be reduced to zero by the characteristic set $\mathcal{C}$ of a σ-ideal $\mathcal{I}$ (Gao et al., 2009a).

Let $\mathcal{A} : A_1, \ldots, A_t$ be a σ-chain, $I_i = \mathrm{I}(A_i)$, $y_{l_i}^{(o_i)} = \mathrm{ld}(A_i)$. $\mathcal{A}$ is called *regular* if for any $j \in \mathbb{N}$, $I_i^{x^j}$ is *invertible* w.r.t. $\mathcal{A}$ (Gao et al., 2009a) in the sense that $[A_1, \ldots, A_{i-1}, I_i^{x^j}]$ contains a nonzero σ-polynomial involving no $y_{l_i}^{(o_i+k)}, k = 0, 1, \ldots$. To introduce the concept of coherent σ-chain, we need to define the *Δ-polynomial* first. If A_i and A_j have distinct leading variables, we define $\Delta(A_i, A_j) = 0$. If A_i and A_j $(i < j)$ have the same leading variable y_l, then $o_i = \mathrm{ord}(A_i, y_l) < o_j = \mathrm{ord}(A_j, y_l)$. Define

$$\Delta(A_i, A_j) = \mathrm{prem}((A_i)^{x^{o_j - o_i}}, A_j). \tag{4}$$

Then $\mathcal{A}$ is called *coherent* if $\mathrm{prem}(\Delta(A_i, A_j), \mathcal{A}) = 0$ for all $i < j$ (Gao et al., 2009a).

Let $\mathcal{A}$ be a σ-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 to be

$$\mathrm{sat}(\mathcal{A}) = [\mathcal{A}] : \mathbb{I}_{\mathcal{A}} = \{p \in \mathcal{F}\{\mathbb{Y}\} : \exists h \in \mathbb{I}_{\mathcal{A}}, \ \mathrm{s.t.}\, hp \in [A]\}. \tag{5}$$

The following result is needed in this paper.

Theorem 1. *(Gao et al., 2009a, Theorem 3.3) A σ-chain $\mathcal{A}$ is a characteristic set of* $\mathrm{sat}(A)$ *if and only if $\mathcal{A}$ is regular and coherent.*

3. $\mathbb{Z}[x]$-lattice

In this section, we prove basic properties of $\mathbb{Z}[x]$-lattices, which will play the role of lattices in the study of binomial ideals.

For brevity, a $\mathbb{Z}[x]$-module in $\mathbb{Z}[x]^n$ is called a $\mathbb{Z}[x]$-*lattice*. Since $\mathbb{Z}[x]$ is a Noetherian ring, any $\mathbb{Z}[x]$-lattice L has a finite set of generators $\mathbb{f} = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\} \subset \mathbb{Z}[x]^n$:

$$L = \mathrm{Span}_{\mathbb{Z}[x]}\{\mathbf{f}_1, \ldots, \mathbf{f}_s\} \triangleq (\mathbf{f}_1, \ldots, \mathbf{f}_s).$$

A *matrix representation* of $\mathbb{f}$ or L is

$$M = [\mathbf{f}_1, \ldots, \mathbf{f}_s]_{n\times s},$$

with $\mathbf{f}_i$ to be the i-th column of M. We also denote $L = (M)$. The *rank* of a $\mathbb{Z}[x]$-lattice L is defined to be the rank of any matrix representation of L, which is clearly well-defined.

We list some basic concepts and properties of Gröbner bases of modules. For details, please refer to Cox et al. (1998).

Denote $\boldsymbol{\epsilon}_i$ to be the i-th standard basis vector $(0, \ldots, 0, 1, 0, \ldots, 0)^\tau \in \mathbb{Z}[x]^n$, where 1 lies in the i-th row of $\boldsymbol{\epsilon}_i$. A *monomial* in $\mathbb{Z}[x]^n$ is an element of the form $x^k\boldsymbol{\epsilon}_i \in \mathbb{Z}[x]^n$, where $k \in \mathbb{N}$. The following *monomial order* $>$ of $\mathbb{Z}[x]^n$ will be used in this paper: $x^\alpha\boldsymbol{\epsilon}_i > x^\beta\boldsymbol{\epsilon}_j$ if $i > j$, or $i = j$ and $\alpha > \beta$. A *term* in $\mathbb{Z}[x]^n$ is the product of a nonzero element c in $\mathbb{Z}$ and a monomial $\mathfrak{m}$ in $\mathbb{Z}[x]^n$, that is $c\mathfrak{m}$. For two terms $c_1\mathfrak{m}_1$ and $c_2\mathfrak{m}_2$, we say $c_1\mathfrak{m}_1 > c_2\mathfrak{m}_2$ if $\mathfrak{m}_1 > \mathfrak{m}_2$ or $\mathfrak{m}_1 = \mathfrak{m}_2$ and $|c_1| > |c_2|$.

With the above order, any $\mathbf{f} \in \mathbb{Z}[x]^n$ can be written in a unique way: $\mathbf{f} = \sum_{i=1}^{l} c_i\mathbf{h}_i$, where $c_i \in \mathbb{Z}$, $\mathbf{h}_i$ are monomials such that $\mathbf{h}_1 > \mathbf{h}_2 > \cdots > \mathbf{h}_l$. $\mathbf{LT}(\mathbf{f}) := c_1\mathbf{h}_1$ is called the *leading term* of $\mathbf{f}$. For any $\mathbb{G} \subset \mathbb{Z}[x]^n$, we denote by $\mathbf{LT}(\mathbb{G})$ the set of leading terms of $\mathbb{G}$.

The order $>$ can be extended to elements of $\mathbb{Z}[x]^n$ as follows: for $\mathbf{f}, \mathbf{g} \in \mathbb{Z}[x]^n$, $\mathbf{f} < \mathbf{g}$ if and only if $\mathbf{LT}(\mathbf{f}) < \mathbf{LT}(\mathbf{g})$.

Let $\mathbb{G} \subset \mathbb{Z}[x]^n$ and $\mathbf{f} \in \mathbb{Z}[x]^n$. We say that $\mathbf{f}$ is *G-reduced* w.r.t. $\mathbb{G}$ if for any term $c\mathbf{h}$ of $\mathbf{f}$ and any $\mathbf{g} \in \mathbb{G}$, $c\mathbf{h}$ is not a multiple of $\mathbf{LT}(\mathbf{g}) = a\mathfrak{m}$ by an element in $\mathbb{Z}[x]$ and $0 < c < |a|$ when $\mathbf{h} = x^e\mathfrak{m}$ for certain $e \in \mathbb{N}$. For instance, $-x^2\boldsymbol{\epsilon}_1$ is not G-reduced w.r.t. $3x\boldsymbol{\epsilon}_1$, but $2x^2\boldsymbol{\epsilon}_1 = -x^2\boldsymbol{\epsilon}_1 + x \cdot 3x\boldsymbol{\epsilon}_1$ is.

Definition 2. A finite set $\mathbb{f} = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\} \subset \mathbb{Z}[x]^n$ is called a *Gröbner basis* for the $\mathbb{Z}[x]$-lattice L generated by $\mathbb{f}$ if for any $\mathbf{g} \in L$, there exists an i, such that $\mathbf{LT}(\mathbf{f}_i)|\mathbf{LT}(\mathbf{g})$. In this paper, it is always assumed that $\mathbf{f}_1 < \mathbf{f}_2 < \cdots < \mathbf{f}_s$. A Gröbner basis $\mathbb{f}$ is called *reduced* if for any $\mathbf{f} \in \mathbb{f}$, $\mathbf{f}$ is G-reduced with respect to $\mathbb{f} \setminus \{\mathbf{f}\}$.

Let $\mathbb{f}$ be a Gröbner basis. Then any $\mathbf{f} \in \mathbb{Z}[x]^n$ can be reduced to a unique normal form by $\mathbb{f}$, denoted by $\mathrm{grem}(\mathbf{f}, \mathbb{f})$, which is G-reduced with respect to $\mathbb{f}$.

Definition 3. Let $\mathbf{f}, \mathbf{g} \in \mathbb{Z}[x]^n$, $\mathbf{LT}(\mathbf{f}) = ax^k\mathbf{e}_i$, $\mathbf{LT}(\mathbf{g}) = bx^s\mathbf{e}_j$, $s \le k$. Then the S-polynomial of $\mathbf{f}$ and $\mathbf{g}$ is defined as follows: if $i \neq j$ then $S(\mathbf{f}, \mathbf{g}) = 0$; otherwise $S(\mathbf{f}, \mathbf{g}) =$

$$\begin{cases} \mathbf{f} - \frac{a}{b}x^{k-s}\mathbf{g}, & \text{if } b \mid a; \\ \frac{b}{a}\mathbf{f} - x^{k-s}\mathbf{g}, & \text{if } a \mid b; \\ u\mathbf{f} + vx^{k-s}\mathbf{g}, & \text{if } a \nmid b \text{ and } b \nmid a, \ \textit{where } \gcd(a, b) = ua + vb. \end{cases} \tag{6}$$

The following basic property for Gröbner basis is obviously true for $\mathbb{Z}[x]$-lattices and a polynomial-time algorithm to compute Göbner bases for $\mathbb{Z}[x]$-lattices is given in Jing et al. (2016).

Theorem 4 *(Buchberger's Criterion). The following statements are equivalent.*

1) $\mathbb{f} = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\} \subset \mathbb{Z}[x]^n$ *is a Gröbner basis.*
2) $\operatorname{grem}(S(\mathbf{f}_i, \mathbf{f}_j), \mathbb{f}) = 0$ *for all* i, j.
3) $\mathbf{f} \in (\mathbb{f})$ *if and only if* $\operatorname{grem}(\mathbf{f}, \mathbb{f}) = 0$.

We will study the structure of a Gröbner basis for a $\mathbb{Z}[x]$-lattice by introducing the concept of generalized Hermite normal form. First, we consider the case of $n = 1$.

Lemma 5. *Let* $B = \{b_1, \ldots, b_k\}$ *be a reduced Gröbner basis of a* $\mathbb{Z}[x]$*-module in* $\mathbb{Z}[x]$, $b_1 < \cdots < b_k$, *and* $\mathbf{LT}(b_i) = c_i x^{d_i} \in \mathbb{N}[x]$. *Then*
1) $0 \le d_1 < d_2 < \cdots < d_k$.
2) $c_k | \cdots | c_2 | c_1$ *and* $c_i \ne c_{i+1}$ *for* $1 \le i \le k-1$.
3) $\frac{c_i}{c_k} | b_i$ *for* $1 \le i < k$. *If* $\widetilde{b}_1$ *is the primitive part of* b_1, *then* $\widetilde{b}_1 | b_i$ *for* $1 < i \le k$.
4) The S-polynomial $S(b_i, b_j)$ *can be reduced to zero by* B *for any* i, j.

Proof. 1) and 4) are consequences of Theorem 4. To prove 2), assume that there exists an l such that $c_{l-1} | \cdots | c_2 | c_1$ but $c_l \not| c_{l-1}$. Let $r = \gcd(c_l, c_{l-1}) = p_1 c_l + p_2 c_{l-1}$, where $p_1, p_2 \in \mathbb{Z}$. Then $|r| < |c_{l-1}|$ and $|r| < |c_l|$. Since $c_{l-1} | \cdots | c_2 | c_1$, we have $|r| < |c_i|$, $i = 1, \ldots, l$. Let $g = p_1 b_l + p_2 x^{d_l - d_{l-1}} b_{l-1}$. Then $\mathbf{LT}(g) = r x^{d_l}$ which is reduced w.r.t. B and $g \in (B)$, contradicting to the definition of Gröbner bases.

We prove 3) by induction on k. When $k = 2$, let $b_1 = c_1 x^{d_1} + s_{11} x^{d_1 - 1} + \cdots + s_{1 d_1}$ and $b_2 = c_2 x^{d_2} + s_{21} x^{d_2 - 1} + \cdots + s_{2 d_2}$. Then, $c_2 | c_1$ and $d_1 < d_2$. Let $c_1 = c_2 t$, we need to show $t | b_1$. Since the S-polynomial $S(b_1, b_2) = t b_2 - x^{d_2 - d_1} b_1$ can be reduced to zero by b_1, we have $t b_2 - x^{d_2 - d_1} b_1 = u(x) b_1$, where $u(x) \in \mathbb{Z}[x]$ and $\deg(u(x)) < d_2 - d_1$. Then, $t b_2 = (x^{d_2 - d_1} + u(x)) b_1$, and $t | b_1$ follows since $x^{d_2 - d_1} + u(x)$ is a primitive polynomial in $\mathbb{Z}[x]$. Thus for $k = 2$, $\widetilde{b}_1 | b_2$. Assume that for $k = l - 1$, the claim is true, then $\widetilde{b}_1 | b_i$ for $1 \le i \le l - 1$. We will prove the claim for $k = l$. Since $S(b_1, b_l) = \frac{c_1}{c_l} b_l - x^{d_l - d_1} b_1$ can be reduced to zero by B. We have $\frac{c_1}{c_l} b_l - x^{d_l - d_1} b_1 = \sum_{i=1}^{l-1} f_i b_i$ with $f_i \in \mathbb{Z}[x]$ and $\deg(f_i b_i) \le d_l - 1$. Then, $\frac{c_1}{c_l} b_l = x^{d_l - d_1} b_1 + \sum_{i=1}^{l-1} f_i b_i$. By induction, $\widetilde{b}_1$ is a factor of the right hand side of the above equation. Thus $\widetilde{b}_1 | b_l$. Let $b_i = s_i b_1'$ for $1 \le i \le l$, we have $\frac{c_1}{c_l} s_l = x^{d_l - d_1} s_1 + \sum_{i=1}^{l-1} f_i s_i$ where $\deg(s_i) = d_i - d_1$ and $s_1 \in \mathbb{Z}$. Since $\deg(f_i s_i) \le d_l - d_1 - 1$, we have $\frac{c_1}{c_l} | s_1$ and $\frac{c_1}{c_l} | b_1$. For any $1 \le i < j < l$, assume $\frac{c_i}{c_l} | b_i$. We will show that $\frac{c_j}{c_l} | b_j$. Since $S(b_{j-1}, b_j) = \frac{c_{j-1}}{c_j} b_j - x^{d_j - d_{j-1}} b_{j-1} = \sum_{i=1}^{j-1} f_i b_i$, we have $\frac{c_{j-1}}{c_l}$ is a factor of the right hand side of the above equation, for $c_{j-1} | c_{j-2} | \cdots | c_1$. Then, $\frac{c_{j-1}}{c_l} | \frac{c_{j-1}}{c_j} b_j$ and $\frac{c_j}{c_l} | b_j$. The claim is proved. □

Example 6. Here are three Gröbner bases in $\mathbb{Z}[x]$: $\{2, x\}$, $\{12, 6x + 6, 3x^2 + 3x, x^3 + x^2\}$, $\{9x + 3, 3x^2 + 4x + 1\}$.

Motivated by the structure of the three reduced Gröbner bases in Example 6, we introduce the concept of generalized Hermite normal form. Let

$$\mathcal{C} = \begin{bmatrix}
c_{1,1} & \ldots & c_{1,l_1} & c_{1,l_1+1} & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
c_{r_1,1} & \ldots & c_{r_1,l_1} & c_{r_1,l_1+1} & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & \ldots & 0 & c_{r_1+1,1} & \ldots & c_{r_1+1,l_2} & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & \ldots & 0 & c_{r_2,1} & \ldots & c_{r_2,l_2} & \ldots & \ldots & \ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & \ldots & 0 & 0 & \ldots & 0 & \ldots & 0 & c_{r_{t-1}+1,1} & \ldots & c_{r_{t-1}+1,l_t} \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
0 & \ldots & 0 & 0 & \ldots & 0 & \ldots & 0 & c_{r_t,1} & \ldots & c_{r_t,l_t}
\end{bmatrix}_{m \times s} \tag{7}$$

be an $m \times s$-matrix whose elements are in $\mathbb{Z}[x]$. It is clear that $m = r_t$ and $s = \sum_{i=1}^{t} l_i$. We denote by $\mathbf{c}_{r_i,j}$ to be the column of the matrix $\mathcal{C}$ whose last nonzero element is

$$c_{r_i,j} = c_{i,j,0}x^{d_{ij}} + \cdots + c_{i,j,d_{ij}}. \tag{8}$$

Then the leading term of $\mathbf{c}_{r_i,j}$ is $c_{r_i,j,0}x^{d_{r_i,j}}\boldsymbol{\epsilon}_{r_i}$. It is clear that $\mathrm{rk}(L) = t$.

Definition 7. The matrix $\mathcal{C}$ in (7) is called a *generalized Hermite normal form* if it satisfies the following conditions:

1) $0 \le d_{r_i,1} < d_{r_i,2} < \cdots < d_{r_i,l_i}$ for any i.
2) $c_{r_i,l_i,0} | \cdots | c_{r_i,2,0} | c_{r_i,1,0}$.
3) $S(\mathbf{c}_{r_i,j_1}, \mathbf{c}_{r_i,j_2}) = x^{d_{r_i,j_2} - d_{r_i,j_1}}\mathbf{c}_{r_i,j_1} - \frac{c_{r_i,j_1,0}}{c_{r_i,j_2,0}}\mathbf{c}_{r_i,j_2}$ can be reduced to zero by the column vectors of the matrix for any $1 \le i \le t, 1 \le j_1 < j_2 \le l_i$.
4) $\mathbf{c}_{r_i,j}$ is G-reduced w.r.t. the column vectors of the matrix other than $\mathbf{c}_{r_i,j}$, for any $1 \le i \le t, 1 \le j \le l_i$.

It is clear that $\{\mathbf{c}_{r_i,1}, \ldots, \mathbf{c}_{r_i,l_i} | i = 1, \ldots, t\}$ is a reduced Gröbner basis in $\mathbb{Z}[x]$. Then, as a consequence of Theorem 4 and Lemma 5, we have

Theorem 8. *$\mathbb{f} = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\} \subset \mathbb{Z}[x]^n$ is a reduced Gröbner basis such that $\mathbf{f}_1 < \mathbf{f}_2 < \cdots < \mathbf{f}_s$ if and only if $[\mathbf{f}_1, \ldots, \mathbf{f}_s]$ is a generalized Hermite normal form.*

Example 9. The following matrices are generalized Hermite normal forms

$$M_1 = \begin{bmatrix} x & 2 & 0 \\ 0 & 2 & x \end{bmatrix}, \; M_2 = \begin{bmatrix} 2 & x-1 & 0 & 0 \\ 0 & 0 & 2 & x-1 \end{bmatrix}$$

whose columns constitute the reduced Gröbner bases of the $\mathbb{Z}[x]$-lattices.

Let $\mathbb{f} = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$ be a reduced Gröbner basis. Let $S(\mathbf{f}_i, \mathbf{f}_j) = m_{ij}\mathbf{f}_i - m_{ji}\mathbf{f}_j$ be the S-polynomial of $\mathbf{f}_i, \mathbf{f}_j$ and $\mathrm{grem}(S(\mathbf{f}_i, \mathbf{f}_j), \mathbb{f}) = \sum_k c_k\mathbf{f}_k$ be the normal representation of $S(\mathbf{f}_i, \mathbf{f}_j)$ in terms of the Gröbner basis $\mathbb{f}$. Then the *syzygy polynomial* $\widetilde{S}(\mathbf{f}_i, \mathbf{f}_j)$

$$\widetilde{S}(\mathbf{f}_i, \mathbf{f}_j) = m_{ij}\boldsymbol{\epsilon}_i - m_{ji}\boldsymbol{\epsilon}_j - \sum_k c_k\boldsymbol{\epsilon}_k,$$

is an element in $\mathbb{Z}[x]^s$, where $\boldsymbol{\epsilon}_k$ is the k-th standard basis vector of $\mathbb{Z}[x]^s$. Define a monomial order in $\mathbb{Z}[x]^s$ as follows: $x^\alpha\boldsymbol{\epsilon}_i \prec x^\beta\boldsymbol{\epsilon}_j$ if $\mathbf{LT}(x^\alpha\mathbf{f}_i) < \mathbf{LT}(x^\beta\mathbf{f}_j)$ in $\mathbb{Z}[x]^n$ or $\mathbf{LT}(x^\alpha\mathbf{f}_i) = \mathbf{LT}(x^\beta\mathbf{f}_j)$ and $i > j$. By Schreyer's Theorem (Cox et al., 1998, p. 212), we have

Theorem 10. *Let $F = [\mathbf{f}_1, \ldots, \mathbf{f}_s]_{n\times s} \in \mathbb{Z}[x]^{n\times s}$ be a generalized Hermite normal form. Then the syzygy polynomials $\widetilde{S}(\mathbf{f}_i, \mathbf{f}_j)$ form a Gröbner basis of the $\mathbb{Z}[x]$-lattice $\ker(F) = \{X \in \mathbb{Z}[x]^s | FX = \mathbf{0}\}$ under the newly defined order $\prec$.*

Let $\mathcal{C}$ be defined in (7) and $k \in \mathbb{N}$. Introduce the following notations:

$$\begin{aligned} \mathcal{C}_- &= \cup_{i=1}^{t} \cup_{k=1}^{l_i-1} \{\mathbf{c}_{r_i,k}, x\mathbf{c}_{r_i,k}, \ldots, x^{\deg(c_{r_i,k+1}) - \deg(c_{r_i,k}) - 1}\mathbf{c}_{r_i,k}\}, \\ \mathcal{C}^+ &= \cup_{i=1}^{t} \cup_{k=0}^{\infty} \{x^k\mathbf{c}_{r_i,l_i}\}, \\ \mathcal{C}_\infty &= \mathcal{C}_- \cup \mathcal{C}^+. \end{aligned} \tag{9}$$

Example 11. Let $\mathcal{C} = \begin{bmatrix} 6 & 3x & 0 & 3 & 2x \\ 0 & 0 & 6 & 3x & x^3+x \end{bmatrix}$. Then $\mathcal{C}_- = \begin{bmatrix} 6 & 0 & 3 & 3x \\ 0 & 6 & 3x & 3x^2 \end{bmatrix}$ and

$$\mathcal{C}_\infty = \begin{bmatrix} 6 & 3x & 3x^2 & 3x^3 & \cdots & 0 & 3 & 3x & 2x & 2x^2 & \cdots \\ 0 & 0 & 0 & 0 & \cdots & 6 & 3x & 3x^2 & x^3+x & x^4+x^2 & \cdots \end{bmatrix}.$$

By saying the infinite set $\mathcal{C}_\infty$ is linearly independent over $\mathbb{Z}$, we mean any finite subset of $\mathcal{C}_\infty$ is linearly independent over $\mathbb{Z}$. Otherwise, $\mathcal{C}_\infty$ is said to be linearly dependent. We need the following properties of $\mathcal{C}_\infty$.

Lemma 12. *The columns of $\mathcal{C}_\infty$ in (9) are linearly independent over $\mathbb{Z}$.*

Proof. Suppose $\mathcal{C}$ is given in (7). The leading term of $\mathbf{c} \in \mathcal{C}_\infty$ is $\mathbf{LT}(\mathbf{c}) = ax^l \boldsymbol{\epsilon}_{r_i}$ for $i = 1, \ldots, t$ and $l \in \mathbb{N}$. Furthermore, for two different $\mathbf{c}_1$ and $\mathbf{c}_2$ in $\mathcal{C}_\infty$ such that $\mathbf{LT}(\mathbf{c}_1) = ax^{l_1}\boldsymbol{\epsilon}_{r_i}$ and $\mathbf{LT}(\mathbf{c}_2) = bx^{l_2}\boldsymbol{\epsilon}_{r_i}$, we have $l_1 \neq l_2$. Then $\mathbf{LT}(\mathcal{C}_\infty) = \{a_{il_i}x^{l_i}\boldsymbol{\epsilon}_{r_i} \mid i = 1, \ldots, t; l_i = d_{i1}, d_{i1}+1, \ldots; a_{il_i} \in \mathbb{Z}\}$ is linearly independent over $\mathbb{Z}$, where d_{i1} are the same as in (8). Then $\mathcal{C}_\infty$ are also linearly independent over $\mathbb{Z}$. □

Lemma 13. *Let $\mathcal{C}$ be a generalized Hermite normal form. Then any $\mathbf{g} \in (\mathcal{C})$ can be written uniquely as a linear combination of finitely many elements of $\mathcal{C}_\infty$ over $\mathbb{Z}$.*

Proof. $\mathbf{g} \in (\mathcal{C})$ can be written as a linear combination of elements of $\mathcal{C}_\infty$ over $\mathbb{Z}$ by the procedure to compute $\mathrm{grem}(\mathbf{g}, \mathcal{C}) = 0$ (Cox et al., 1998). The uniqueness is a consequence of Lemma 12. □

4. Canonical representations for Laurent binomial σ-ideal

In this section, we will give three canonical representations for a proper Laurent binomial σ-ideal.

4.1. Laurent binomial σ-ideal

In this section, several basic properties of Laurent binomial σ-ideals will be proved.

By a *Laurent σ-binomial* in $\mathbb{Y}$, we mean a σ-polynomial with two terms, that is, $a\mathbb{Y}^{\mathbf{g}} + b\mathbb{Y}^{\mathbf{h}}$ where $a, b \in \mathcal{F}^* = \mathcal{F} \setminus \{0\}$ and $\mathbf{g}, \mathbf{h} \in \mathbb{Z}[x]^n$. A Laurent σ-binomial of the following form is said to be in *normal form*

$$p = \mathbb{Y}^{\mathbf{f}} - c_{\mathbf{f}}$$

where $c_{\mathbf{f}} \in \mathcal{F}^* = \mathcal{F} \setminus \{0\}$ and $\mathbf{f} \in \mathbb{Z}[x]^n$ is normal. The vector $\mathbf{f}$ is called the *support* of p. For $p = \mathbb{Y}^{\mathbf{f}} - c_{\mathbf{f}}$, we denote $\widehat{p} = -c_{\mathbf{f}}^{-1}\mathbb{Y}^{-\mathbf{f}}p = \mathbb{Y}^{-\mathbf{f}} - c_{\mathbf{f}}^{-1}$ which is called the *inverse* of p. It is clear that any Laurent σ-binomial f can be written uniquely as $f = aM(\mathbb{Y}^{\mathbf{f}} - c_{\mathbf{f}})$ where $a \in \mathcal{F}^*$, M is a Laurent σ-monomial, and $\mathbb{Y}^{\mathbf{f}} - c_{\mathbf{f}}$ is in normal form. Since aM is a unit in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$, we can use the normal σ-binomial $\mathbb{Y}^{\mathbf{f}} - c_{\mathbf{f}}$ to represent f, and when we say a Laurent σ-binomial we always use its normal representation.

Definition 14. A Laurent σ-ideal is called *binomial* if it is generated by (possibly infinitely many) Laurent σ-binomials.

Lemma 15. *Let $\mathbb{Y}^{\mathbf{f}_i} - c_i$, $i = 1, \ldots, s$ be contained in a Laurent binomial σ-ideal $\mathcal{I}$ and $\mathbf{f} = a_1\mathbf{f}_1 + \cdots + a_s\mathbf{f}_s$, where $a_i \in \mathbb{Z}[x]$. Then $\mathbb{Y}^{\mathbf{f}} - \prod_{i=1}^{s} c_i^{a_i}$ is in $\mathcal{I}$.*

Proof. It suffices to show that if $p_1 = \mathbb{Y}^{\mathbf{f}_1} - c_1 \in \mathcal{I}$ and $p_2 = \mathbb{Y}^{\mathbf{f}_2} - c_2 \in \mathcal{I}$, then $\mathbb{Y}^{n\mathbf{f}_1} - c_1^n \in \mathcal{I}$ for $n \in \mathbb{N}$, $\mathbb{Y}^{-\mathbf{f}_1} - c_1^{-1} \in \mathcal{I}$, $\mathbb{Y}^{x\mathbf{f}_1} - \sigma(c_1) \in \mathcal{I}$, and $\mathbb{Y}^{\mathbf{f}_1+\mathbf{f}_2} - c_1c_2 \in \mathcal{I}$, which are indeed true since $\mathbb{Y}^{n\mathbf{f}_1} - c_1^n = (\mathbb{Y}^{\mathbf{f}_1})^n - c_1^n$ contains p_1 as a factor, $\mathbb{Y}^{-\mathbf{f}_1} - c_1^{-1} = -c_1^{-1}\mathbb{Y}^{-\mathbf{f}_1}(\mathbb{Y}^{\mathbf{f}_1} - c_1) \in \mathcal{I}$, $\mathbb{Y}^{x\mathbf{f}_1} - \sigma(c_1) = \sigma(\mathbb{Y}^{\mathbf{f}_1} - c_1) \in \mathcal{I}$, and $\mathbb{Y}^{\mathbf{f}_1+\mathbf{f}_2} - c_1c_2 = \mathbb{Y}^{\mathbf{f}_1}(\mathbb{Y}^{\mathbf{f}_2} - c_2) + c_2(\mathbb{Y}^{\mathbf{f}_1} - c_1) \in \mathcal{I}$. □

Definition 16. Let $\mathcal{I}$ be a proper Laurent binomial σ-ideal and

$$\mathbb{L}(\mathcal{I}) := \{\mathbf{f} \in \mathbb{Z}[x]^n \mid \exists c_{\mathbf{f}} \in \mathcal{F}^* \, s.t. \, \mathbb{Y}^{\mathbf{f}} - c_{\mathbf{f}} \in \mathcal{I}\}. \tag{10}$$

By Lemma 15, $\mathbb{L}(\mathcal{I})$ is a $\mathbb{Z}[x]$-lattice, which is called the *support lattice* of $\mathcal{I}$.

As a direct consequence, we have

Proposition 17. *Let the support lattice of $\mathcal{I}$ be $\mathbb{L}(\mathcal{I}) = (\mathbf{f}_1, \ldots, \mathbf{f}_s)$. Then $\mathcal{I} = [\mathbb{Y}^{\mathbf{f}_1} - c_{\mathbf{f}_1}, \ldots, \mathbb{Y}^{\mathbf{f}_s} - c_{\mathbf{f}_s}]$, that is, a Laurent binomial σ-ideal is finitely generated. $[\mathbf{f}_1, \ldots, \mathbf{f}_s]$ is called a* matrix representation *for $\mathcal{I}$.*

Proof. Let $\mathcal{I}_1 = [\mathbb{Y}^{\mathbf{f}_1} - c_{\mathbf{f}_1}, \ldots, \mathbb{Y}^{\mathbf{f}_s} - c_{\mathbf{f}_s}]$. It suffices to show $\mathcal{I} \subset \mathcal{I}_1$. Since $\mathcal{I}$ is Laurent binomial, it has a set of generators of the form $f_{\mathbf{h}} = \mathbb{Y}^{\mathbf{h}} - c_{\mathbf{h}}$. Then $\mathbf{h} \in \mathbb{L}(\mathcal{I}) = (\mathbf{f}_1, \ldots, \mathbf{f}_s)$. By Lemma 15, there exists a $\widetilde{c}_{\mathbf{h}} \in \mathcal{F}$ such that $\widetilde{f}_{\mathbf{h}} = \mathbb{Y}^{\mathbf{h}} - \widetilde{c}_{\mathbf{h}} \in \mathcal{I}_1$. Then $f_{\mathbf{h}} - \widetilde{f}_{\mathbf{h}} = \widetilde{c}_{\mathbf{h}} - c_{\mathbf{h}} \in \mathcal{I}$. Since $\mathcal{I}$ is proper, we have $f_{\mathbf{h}} - \widetilde{f}_{\mathbf{h}} = 0$ or $f_{\mathbf{h}} \in \mathcal{I}_1$ and hence $\mathcal{I} \subset \mathcal{I}_1$. □

Similarly, we can prove

Corollary 18. *Let $\mathcal{I} = [\mathbb{Y}^{\mathbf{f}_1} - c_1, \ldots, \mathbb{Y}^{\mathbf{f}_s} - c_s]$ be a proper Laurent binomial σ-ideal and let $\mathbf{h}_1, \ldots, \mathbf{h}_r$ be another set of generators of $(\mathbf{f}_1, \ldots, \mathbf{f}_s)$, and $\mathbf{h}_i = \sum_{k=1}^{s} a_{i,k}\mathbf{f}_k$, $i = 1, \ldots, r$, where $a_{i,k} \in \mathbb{Z}[x]$. Then $\mathcal{I} = [\mathbb{Y}^{\mathbf{h}_1} - \prod_{i=1}^{s} c_i^{a_{1,i}}, \ldots, \mathbb{Y}^{\mathbf{h}_r} - \prod_{i=1}^{s} c_i^{a_{r,i}}]$.*

We now show how to check whether a Laurent binomial σ-ideal is proper.

Proposition 19. *Let $\mathcal{I} = [\mathbb{Y}^{\mathbf{f}_1} - c_1, \ldots, \mathbb{Y}^{\mathbf{f}_s} - c_s]$ be a Laurent binomial σ-ideal and $M = [\mathbf{f}_1, \ldots, \mathbf{f}_s] \in \mathbb{Z}[x]^{n \times s}$. Let $\ker(M) = \{\mathbf{h} \in \mathbb{Z}[x]^s \mid M\mathbf{h} = 0\}$ be generated by $\mathbf{u}_1, \ldots, \mathbf{u}_t$, where $\mathbf{u}_i = (u_{i,1}, \ldots, u_{i,s})$. Then $\mathcal{I} \neq [1]$ if and only if $\prod_{i=1}^{s} c_i^{u_{l,i}} = 1$ for $l = 1, \ldots, t$.*

Proof. "⇒" Let $f_i = \mathbb{Y}^{\mathbf{f}_i} - c_i$. Suppose $c = \prod_{i=1}^{s} c_i^{u_{l,i}} \neq 1$ for some l. Replacing c_i by $\mathbb{Y}^{\mathbf{f}_i} - f_i$ in the above equation and noting that $\mathbf{u}_l \in \ker(M)$, we have $c = \prod_{i=1}^{s} c_i^{u_{l,i}} = \prod_{i=1}^{s} (\mathbb{Y}^{\mathbf{f}_i} - f_i)^{u_{l,i}} = \mathbb{Y}^{M \cdot \mathbf{u}_l} + g = 1 + g$ where $g \in \mathcal{I}$. Then $0 \neq c - 1 \in \mathcal{I}$ and $\mathcal{I} = [1]$, a contradiction.

"⇐" Suppose the contrary. Then there exist $g_i \in \mathcal{F}\{\mathbb{Y}^{\pm}\}$ such that

$$g_1 f_1 + \cdots + g_s f_s = 1. \tag{11}$$

Let l be the maximal c such that $y_c^{(k)}$ occurs in some f_i, o the largest j such that $y_l^{(j)}$ occurs in some f_k, and $d = \max_{k=1}^{s} \deg(f_k, y_l^{(o)})$. Let $f_k = \mathbb{Y}^{\mathbf{f}_k} - c_k = I_k y_l^{dx^o} - c_k$. Since (11) is an identity about the algebraic variables $y_i^{x^j}$, we can set $y_l^{dx^o} = c_k / I_k$ in (11) to obtain a new identity. In the new identity, f_k becomes zero and the left hand side of (11) has at most $s - 1$ summands. We will show that this procedure can be continued for the new identity. Then the left hand side of (11) will eventually becomes zero, and a contradiction is obtained and the lemma is proved.

If $\mathrm{ord}(f_i, y_l) < o$ or $\mathrm{ord}(f_i, y_l) = o$ and $\deg(f_i, y_l^{x^o}) < d$ for some i, then f_i is not changed in the above procedure. Let us assume that for some v, $\deg(f_v, y_l^{x^o}) = d$ and $f_v = \mathbb{Y}^{\mathbf{f}_v} - c_v = I_v y_l^{dx^o} - c_v$. Then after the substitution, $f_v = c_k I_v / I_k - c_v = c_k \widetilde{f}_v$ where $\widetilde{f}_v = I_v / I_k - c_v / c_k$. We claim that either $\widetilde{f}_v = 0$ or I_v / I_k is a proper monomial, and as a consequence, the above substitution can continue. To prove the claim, it suffices to show that if $I_v = I_k$ then $c_v = c_k$. If $I_v = I_k$, then $\mathbf{f}_v = \mathbf{f}_k$, that is, $\mathbf{f}_v - \mathbf{f}_k = 0$ is a syzygy among $\mathbf{f}_i$. Let $\boldsymbol{\epsilon}_{vk}$ be the corresponding syzygy vector. Then $\boldsymbol{\epsilon}_{vk} \in \ker(M)$ can be written as a linear combination of $\mathbf{u}_1, \ldots, \mathbf{u}_s$. Let $\mathbf{c} = (c_1, \ldots, c_s)^\tau$. Then $c_v c_k^{-1} = \mathbf{c}^{\boldsymbol{\epsilon}_{vk}}$ can be written as a product of $\mathbf{c}^{\mathbf{u}_l} = \prod_{i=1}^{s} c_i^{u_{l,i}} = 1$, and thus $c_v c_k^{-1} = 1$. □

4.2. Characteristic set of Laurent binomial σ-ideal

We show how to modify the characteristic set method presented in section 2.2 in the case of Laurent binomial σ-ideals. First, assume that all Laurent σ-binomials are in normal form, which makes the concepts of order and leading variables well-defined.

Second, when defining the concept of rank and the concept that a σ-polynomial p is reduced w.r.t. a σ-polynomial q, we need to replace $\deg(p, y_j^{(o)})$ by $|\deg(p, y_j^{(o)})|$. Precisely, q is said to be *reduced* w.r.t. p if $|\deg(q, y_j^{(k+l)})| < |\deg(p, y_j^{(k)})|$ for all $l \in \mathbb{N}$, where $\mathrm{ld}(p) = y_j^{(k)}$. For instance, $y_1^{-2x} y_2 - 1$ is not reduced w.r.t. $y_1^2 - 1$. With these changes, we can define the concepts of *Laurent σ-chain* and characteristic set in the Laurent σ-binomial case. For instance, the σ-chain $\mathcal{A}_1$ in (2) becomes the following Laurent σ-chain:

$$\widetilde{\mathcal{A}}_1 \ : \ y_1^2 + 1, \ y_1^{x-1} - 1, \ y_2^2 + 1, \ y_2^{x-1} + 1 \tag{12}$$

Third, the σ-remainder for two Laurent σ-binomials need to be modified as follows. We first consider how to compute $\mathrm{prem}(f, g)$ in the simple case: $o = \mathrm{ord}(f, y_l) = \mathrm{ord}(g, y_l)$, where $y_l = \mathrm{lvar}(g)$. Let $g = I_g (y_l^{(o)})^{d_g} - c_g$, where $d_g = \deg(g, y_l^{(o)})$ and I_g is the initial of g. As mentioned above, g is in normal form, that is $d_g > 0$. Let $d_f = \deg(f, y_l^{(o)})$ and $f = I_f (y_l^{(o)})^{d_f} - c_f$. We consider two cases.

In the first case, let us assume $d_f \geq 0$. We define a new operation $\mathrm{prem}_1(f, g)$ below. If $d_f < d_g$, then set $r = \mathrm{prem}_1(f, g)$ to be f. Otherwise, perform the following basic step

$$r := \mathrm{prem}_1(f, g) = (f - g \frac{I_f}{I_g} (y_l^{(o)})^{d_f - d_g}) / c_g = \frac{I_f}{I_g} (y_l^{(o)})^{d_f - d_g} - \frac{c_f}{c_g}. \tag{13}$$

Let $\mathbf{h}_r, \mathbf{h}_f, \mathbf{f}_g$ be the supports of r, f, g, respectively. Then

$$\mathbf{h}_r = \mathbf{h}_f - \mathbf{h}_g. \tag{14}$$

Set $f = r$ and repeat the procedure prem_1 for f and g. Since d_f decreases strictly after each iteration, the procedure will end and return $\mathrm{prem}(f, g) = r$ which satisfies

$$r = \frac{f}{c_g^k} - hg = \frac{I_f}{I_g^k} (y_l^{(o)})^{d_f - k d_g} - \frac{c_f}{c_g^k} \tag{15}$$

$$\mathbf{h}_r = \mathbf{h}_f - k \mathbf{h}_g \tag{16}$$

where $k = \lfloor \frac{d_f}{d_g} \rfloor$ and $h \in \mathcal{F}\{\mathbb{Y}^{\pm}\}$.

In the second case, we assume $d_f < 0$. The σ-remainder can be computed similar to the first case. Instead of g, we consider $\widehat{g} = (I_g)^{-1} (y_l^{(o)})^{-d_g} - c_g^{-1}$. If $|d_f| < d_g$, then set $r = \mathrm{prem}(f, g)$ to be f. Otherwise, perform the following basic step

$$r := \mathrm{prem}_1(f, g) = c_g (f - \widehat{g} I_g I_f (y_l^{(o)})^{d_f + d_g}) = I_f I_g (y_l^{(o)})^{d_f + d_g} - c_f c_g.$$

In this case, equation (14) becomes $\mathbf{h}_r = \mathbf{h}_f + \mathbf{h}_g$. To compute $\mathrm{prem}(f, g)$, repeat the above basic step for $f = r$ until $|d_f| < d_g$.

For two general Laurent σ-binomials f and g, $\mathrm{prem}(f, g)$ is defined as follows: if f is reduced w.r.t. g, set $\mathrm{prem}(f, g) = f$. Otherwise, let $y_l = \mathrm{lvar}(g)$, $o_f = \mathrm{ord}(f, y_l)$, and $o_g = \mathrm{ord}(g, y_l)$. Define

$$\mathrm{prem}(f, g) = \mathrm{prem}(\ldots, \mathrm{prem}(\mathrm{prem}(f, g^{(o_f - o_g)}), g^{(o_f - o_g - 1)}), \ldots, g).$$

Let $\mathcal{A} : A_1, \ldots, A_s$ be a Laurent binomial σ-chain and f a σ-binomial. Then define

$$\mathrm{prem}(f, \mathcal{A}) = \mathrm{prem}(\ldots, \mathrm{prem}(\mathrm{prem}(f, A_s), A_{s-1}), \ldots, A_1).$$

In summary, we have

Lemma 20. *Let $\mathcal{A}: A_1, \ldots, A_s$ be a Laurent binomial σ-chain, f a σ-binomial, and $r = \mathrm{prem}(f, \mathcal{A})$. Then r is reduced w.r.t. $\mathcal{A}$ and satisfies*

$$cf \equiv r, \mathrm{mod}\,[\mathcal{A}], \tag{17}$$

where $c \in \mathcal{F}^*$. Furthermore, let the supports of r and f be $\mathbf{h}_r$ and $\mathbf{h}_f$, respectively. Then $\mathbf{h}_f - \mathbf{h}_r$ is in the $\mathbb{Z}[x]$-lattice generated by the supports of A_i.

Similar to section 2.2, the concepts of coherent and regular σ-chains can be extended to the Laurent case. Since any σ-monomial is a unit in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$, the concept of regular σ-chain need to be strengthened as follows. A σ-chain $\mathcal{A}$ is called *Laurent regular* if $\mathcal{A}$ is regular and any σ-monomial is invertible w.r.t. $\mathcal{A}$. Then, following Gao et al. (2009a, Theorem 3.3), Theorem 1 can be extended to the following Laurent version straightforwardly.

Theorem 21. *A Laurent σ-chain $\mathcal{A}$ is a characteristic set of* $\mathrm{sat}(A)$ *if and only if $\mathcal{A}$ is coherent and Laurent regular.*

For Laurent binomial σ-chains, we have

Lemma 22. *Any Laurent binomial σ-chain $\mathcal{A}$ is Laurent regular.*

Proof. In this proof, without loss of generality, all Laurent σ-polynomials are assumed to be in $\mathbb{K}\{\mathbb{Y}\}$. Since the initials of $\mathcal{A}$ are σ-monomials, it suffices to show that any σ-monomial is invertible w.r.t. $\mathcal{A}$. By Gao et al. (2009a, p. 248), a σ-monomial M is invertible w.r.t. $\mathcal{A}$ if M is invertible w.r.t. an extension $\mathcal{A}_M$ (the definition of $\mathcal{A}_M$ can be found in formula (4) in Gao et al., 2009a, p. 247) of $\mathcal{A}$ when both M and $\mathcal{A}_M$ are treated as algebraic polynomials in $y_i^{x^j}$, where $\mathcal{A}_M$ is an algebraic Laurent binomial triangular set. By Gao et al. (2009b, p. 1150), M is invertible w.r.t. $\mathcal{A}_M$ if the successive Sylvester resultant $\mathrm{Resl}(M, \mathcal{A}_M)$ of M and $\mathcal{A}_M$ is nonzero. Since $\mathcal{A}$ is Laurent binomial, $B \in \mathcal{A}_M$ has the form $B = I(y_k^{x^o})^m + U$, where I is the initial of B and U is a σ-monomial not containing $y_k^{x^o}$. Let $N = J(y_k^{x^o})^n$ be any σ-monomial with J as the initial. Then the Sylvester resultant of M and B w.r.t. $y_k^{x^o}$ is $J^m U^n$ which is a nonzero σ-monomial. As a consequence, $\mathrm{Resl}(M, \mathcal{A}_M)$ is also a nonzero σ-monomial and hence $\mathcal{A}$ is Laurent regular. □

We now give the first canonical representation for Laurent binomial σ-ideals.

Theorem 23. *$\mathcal{I}$ is a proper Laurent binomial σ-ideal if and only if there exists a Laurent coherent σ-chain $\mathcal{A}$ such that $\mathcal{I} = \mathrm{sat}(\mathcal{A}) = [\mathcal{A}]$.*

Proof. Let $\mathcal{I} \neq [1]$ and $\mathcal{A}$ the characteristic set of $\mathcal{I}$. Then $[\mathcal{A}] \subset \mathcal{I} \subset \mathrm{sat}(\mathcal{A})$. From (17), we have $\mathrm{sat}(\mathcal{A}) \subset [\mathcal{A}]$ and then $\mathcal{I} = \mathrm{sat}(\mathcal{A}) = [\mathcal{A}]$. By Theorem 21, $\mathcal{A}$ is coherent. To prove the other implication of the theorem, let $\mathcal{A}$ be a Laurent coherent binomial σ-chain. By Lemma 22, $\mathcal{A}$ is also Laurent regular. By Theorem 21, $\mathcal{A}$ is a characteristic set of $\mathcal{I} = \mathrm{sat}(\mathcal{A})$. Then $\mathcal{I}$ is proper. □

Corollary 24. *Let $\mathcal{I}$ be a Laurent reflexive prime binomial σ-ideal in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$. Then* $\dim(\mathcal{I}) = n - \mathrm{rk}(\mathbb{L}(\mathcal{I}))$.

Proof. By Theorem 23, $\mathcal{I} = [\mathcal{A}]$, where $\mathcal{A}: \mathbb{Y}^{\mathbf{c}_1} - c_1, \ldots \mathbb{Y}^{\mathbf{c}_s} - c_s$. Let $\mathcal{C} = [\mathbf{c}_1, \ldots, \mathbf{c}_s]$ be the matrix representation for $\mathcal{I}$ and in the form of (7). Since $\mathcal{I}$ is reflexive and prime, by Theorem 4.3 of Gao et al. (2009a), $\dim(\mathcal{I}) = n - t = n - \mathrm{rk}(\mathbb{L}(\mathcal{I}))$, where t is defined in (7). □

Corollary 25. *A Laurent binomial σ-ideal is radical.*

Proof. By Theorem 23, $\mathcal{I} = [\mathcal{A}]$, where $\mathcal{A} = \{\mathbb{Y}^{\mathbf{h}_1} - c_1, \ldots, \mathbb{Y}^{\mathbf{h}_r} - c_r\}$ is the characteristic set of $\mathcal{I}$. Let $A_i = \mathbb{Y}^{\mathbf{h}_i} - c_i$ and $y_{l_i}^{(o_i)} = \mathrm{ld}(A_i)$. $\mathcal{A}$ is also *saturated* in the sense that its separants $\frac{\partial A_i}{\partial y_{l_i}^{(o_i)}}$ are

σ-monomials and hence units in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$. Then similar to the differential case (Bouziane et al., 2001), it can be shown that $\mathrm{sat}(\mathcal{A}) = [\mathcal{A}]$ is a radical σ-ideal.

Let $\mathbf{f}_1 < \mathbf{f}_2 < \cdots < \mathbf{f}_s$ be elements in $\mathbb{Z}[x]^n$, $c_i \in \mathcal{F}^*$, and

$$\mathbb{f} = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\} \subset \mathbb{Z}[x]^n \tag{18}$$
$$\mathcal{A}_{\mathbb{f}} = \{A_1, \ldots, A_s\} \subset \mathcal{F}\{\mathbb{Y}^{\pm}\} \text{ with } A_i = \mathbb{Y}^{\mathbf{f}_i} - c_i, i = 1, \ldots, s, \text{ and } c_i \in \mathcal{F}^*$$

In the rest of this section, we will establish a connection between $\mathbb{f}$ and $\mathcal{A}_{\mathbb{f}}$. From Definition 7, we have

Lemma 26. *For $i < j$, A_j is reduced w.r.t. A_i if and only if $\mathbf{f}_j$ is G-reduced w.r.t. $\mathbf{f}_i$.*

Lemma 27. *For $\mathbb{f}$ and $\mathcal{A}_{\mathbb{f}}$ in (18) and a Laurent σ-binomial $f = \mathbb{Y}^{\mathbf{f}} - c$, if $\mathrm{prem}(f, \mathcal{A}_{\mathbb{f}}) = \mathbb{Y}^{\mathbf{g}} - c_{\mathbf{g}}$, then $\mathbf{g} = \mathrm{grem}(\mathbf{f}, \mathbb{f})$.*

Proof. Let us first consider prem_1 in (13) for f and $A_i = \mathbb{Y}^{\mathbf{f}_i} - c_i = I_i(y_{l_i}^{(o_i)})^{d_i} - c_i$, where $\mathrm{ld}(A_i) = y_{l_i}$ and I_i is the initial of A_i. From (14), the support of $r = \mathrm{prem}_1(f, A_i)$ is $\mathbf{f} - \mathbf{f}_i$. It is clear that $\mathbf{LT}(\mathbf{f}_i) = d_i x^{o_i} \boldsymbol{\epsilon}_{l_i}$. Let $\mathbf{f}_i = d_i x^{o_i} \boldsymbol{\epsilon}_{l_i} + \overline{\mathbf{f}}_i$. Similarly, write $\mathbf{f} = d_f x^{o_i} \boldsymbol{\epsilon}_{l_i} + \overline{m}$ where $d_f x^{o_i} \boldsymbol{\epsilon}_{l_i}$ is the leading term of $\mathbf{f}$ w.r.t. $\boldsymbol{\epsilon}_{l_i}$ and $d_f \geq d_i \geq 0$. Then a basic step to compute $\mathrm{grem}(\mathbf{f}, \mathbf{f}_i)$ is to compute $\mathrm{grem}_1(\mathbf{f}, \mathbf{f}_i) = \mathbf{f} - \mathbf{f}_i = (d_f - d_i) x^{o_i} \boldsymbol{\epsilon}_{l_i} + \overline{\mathbf{f}} - \overline{\mathbf{f}}_i$, which is the support of $\mathrm{prem}_1(f, A_i)$.

Using the basic step grem_1 to compute $\mathrm{grem}(\mathbf{f}, \mathbb{f})$, we have a sequence of elements in $\mathbb{Z}[x]^n$: $\mathbf{g}_0 = \mathbf{f}, \mathbf{g}_1 = \mathrm{grem}(\mathbf{f}, \mathbf{f}_1), \ldots, \mathbf{g}_t = \mathrm{grem}(\mathbf{f}, \mathbb{f})$. Correspondingly, using the basic step prem_1 to compute $\mathrm{prem}(\mathbf{f}, \mathcal{A}_{\mathbb{f}})$, we have a sequence of σ-binomials $f_0 = f, f_1 = \mathrm{prem}(f, A_1), \ldots, f_t = \mathrm{prem}(f, \mathcal{A}_{\mathbb{f}})$ such that the support of f_i is $\mathbf{g}_i$ for $i = 1, \ldots, t$. □

Lemma 28. *If $\mathbb{f}$ in (18) is a reduced Gröbner basis and $[\mathcal{A}_{\mathbb{f}}] \neq [1]$, then $\mathcal{A}_{\mathbb{f}}$ is a coherent σ-chain.*

Proof. By Lemma 26, $\mathcal{A}_{\mathbb{f}}$ is a σ-chain. Let $A_i = \mathbb{Y}^{\mathbf{f}_i} - c_i$ and $A_j = \mathbb{Y}^{\mathbf{f}_j} - c_j$ $(i < j)$ have the same leading variable y_l, and $A_i = I_i y_l^{d_i x^{o_i}} - c_i$, $A_j = I_j y_l^{d_j x^{o_j}} - c_j$. From Definition 7, we have $o_i < o_j$ and $d_j | d_i$. Let $d_i = t d_j$ where $t \in \mathbb{N}$. According to (15), we have

$$\Delta(A_i, A_j) = \mathrm{prem}((A_i)^{x^{o_j - o_i}}, A_j) = \frac{(I_i)^{x^{o_j - o_i}}}{I_j^t} - \frac{(c_i)^{x^{o_j - o_i}}}{c_j^t}. \tag{19}$$

Then the support of $\Delta(A_i, A_j)$ is $x^{o_j - o_i} \mathbf{f}_i - \frac{d_i}{d_j} \mathbf{f}_j$.

Since $\mathbf{LT}(A_i) = d_i x^{o_i} \boldsymbol{\epsilon}_l$ and $\mathbf{LT}(A_j) = d_j x^{o_j} \boldsymbol{\epsilon}_l$, we have $N = \mathrm{lcm}(d_i x^{o_i}, d_j x^{o_j}) = d_i x^{o_j}$. According to Definition 3, the S-polynomial of $\mathbf{f}_i$ and $\mathbf{f}_j$ is

$$S(\mathbf{f}_i, \mathbf{f}_j) = x^{o_j - o_i} \mathbf{f}_i - \frac{d_i}{d_j} \mathbf{f}_j.$$

Since $\mathbb{f}$ is a Gröbner basis, we have $\mathbf{g} = \mathrm{grem}(S(\mathbf{f}_i, \mathbf{f}_j), \mathbb{f}) = 0$. Since the support of $\Delta(A_i, A_j)$ is $S(\mathbf{f}_i, \mathbf{f}_j)$, by Lemma 27, $R = \mathrm{prem}(\Delta(A_i, A_j), \mathcal{A}_{\mathbb{f}}) = \mathbb{Y}^{\mathbf{g}} - c = 1 - c$ for some $c \in \mathcal{F}$. Since $[\mathcal{A}_{\mathbb{f}}]$ is proper and $R = 1 - c \in [\mathcal{A}_{\mathbb{f}}]$, we have $R = 0$ and hence $\mathcal{A}_{\mathbb{f}}$ is coherent. □

We now give the second canonical representation for a Laurent binomial σ-ideal.

Theorem 29. *For $\mathbb{f}$ and $\mathcal{A}_{\mathbb{f}}$ defined in (18), $\mathcal{A}_{\mathbb{f}}$ is a coherent σ-chain if and only if $\mathbb{f}$ is a reduced Gröbner basis and $[\mathcal{A}_{\mathbb{f}}] \neq [1]$.*

Proof. Lemma 28 proves one side of the theorem. For the other direction, let $\mathcal{A}_{\mathbb{f}}$ be a coherent σ-chain. By Lemma 26, $\mathbf{f}_i$ is G-reduced w.r.t. $\mathbf{f}_j$ for $i \neq j$. By Theorem 23, $[\mathcal{A}_{\mathbb{f}}]$ is proper. Use the notations introduced in the proof of Lemma 28. Since $S(\mathbf{f}_i, \mathbf{f}_j)$ is the support of $\Delta(A_i, A_j)$, by Lemma 27, $\mathbf{f}_{ij} = \mathrm{grem}(S(\mathbf{f}_i, \mathbf{f}_j), \mathbb{f})$ is the support of $\mathrm{prem}(\Delta(A_i, A_j), \mathcal{A}_{\mathbb{f}})$. Since $\mathcal{A}_{\mathbb{f}}$ is coherent, $\mathrm{prem}(\Delta(A_i, A_j), \mathcal{A}_{\mathbb{f}}) = \mathbb{Y}^{\mathbf{f}_{ij}} - c = 0$ for any i and j, and this is possible only when $\mathbf{f}_{ij} = \mathrm{grem}(S(\mathbf{f}_i, \mathbf{f}_j), \mathbb{f}) = 0$ and $c = 1$ due to the fact $[\mathcal{A}_{\mathbb{f}}] \neq [1]$. Hence $\mathbb{f}$ is a reduced Gröbner basis. □

4.3. Partial character and Laurent binomial σ-ideal

In this section, we will show that proper Laurent binomial σ-ideals can be described uniquely with their partial characters.

Definition 30. A *partial character* ρ on $\mathbb{Z}[x]^n$ is a homomorphism from a $\mathbb{Z}[x]$-lattice L_ρ to the multiplicative group $\mathcal{F}^*$ satisfying $\rho(x\mathbf{f}) = (\rho(\mathbf{f}))^x = \sigma(\rho(\mathbf{f}))$ for $\mathbf{f} \in L_\rho$.

Let ρ be a partial character on $\mathbb{Z}[x]^n$ and $L_\rho = (\mathbf{f}_1, \ldots, \mathbf{f}_s)$, where $\mathbb{f} = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$ is a reduced Gröbner basis. Define

$$\mathcal{I}(\rho) := [\mathbb{Y}^{\mathbf{f}} - \rho(\mathbf{f}) \mid \mathbf{f} \in L_\rho], \tag{20}$$

$$\mathcal{A}(\rho) := \mathbb{Y}^{\mathbf{f}_1} - \rho(\mathbf{f}_1), \ldots, \mathbb{Y}^{\mathbf{f}_s} - \rho(\mathbf{f}_s). \tag{21}$$

The Laurent binomial σ-ideal $\mathcal{I}(\rho)$ has the following properties.

Lemma 31. *$\mathcal{I}(\rho) = [\mathcal{A}(\rho)] \neq [1]$ and $\mathcal{A}(\rho)$ is a characteristic set of $\mathcal{I}(\rho)$.*

Proof. By Lemma 15 and the definition of partial character, $\mathcal{I}(\rho) = [\mathcal{A}(\rho)]$. By Proposition 19, in order to prove $\mathcal{I}(\rho) \neq [1]$, it suffices to show that for any syzygy $\sum_i a_i \mathbf{f}_i = 0$ among $\mathbf{f}_i$, we have $\prod_i \rho(\mathbf{f}_i)^{a_i} = 1$. Indeed, $\rho(\sum_i a_i \mathbf{f}_i) = \prod_i \rho(\mathbf{f}_i)^{a_i} = 1$, since ρ is a homomorphism from the $\mathbb{Z}[x]$-module L_ρ to $\mathcal{F}^*$. Since $\mathbb{f}$ is a reduced Gröber basis, by Theorem 29, $\mathcal{A}$ is a characteristic set of $\mathcal{I}(\rho)$. □

Lemma 32. *A Laurent σ-binomial $\mathbb{Y}^{\mathbf{f}} - c_{\mathbf{f}}$ is in $\mathcal{I}(\rho)$ if and only if $\mathbf{f} \in L_\rho$ and $c_{\mathbf{f}} = \rho(\mathbf{f})$.*

Proof. By Lemma 31, $\mathcal{A}(\rho)$ is a characteristic set of $\mathcal{I}(\rho)$. Since $f = \mathbb{Y}^{\mathbf{f}} - c_{\mathbf{f}}$ is a σ-binomial in $\mathcal{I}(\rho)$, we have $r = \mathrm{prem}(f, \mathcal{A}) = 0$. By Lemma 20, $\mathbf{f}$ is in the $\mathbb{Z}[x]$-module L_ρ. The other side is obviously true and the lemma is proved. □

We now give the third canonical representation for a Laurent binomial σ-ideal.

Theorem 33. *The map $\rho \Rightarrow \mathcal{I}(\rho)$ gives a one to one correspondence between the set of proper Laurent binomial σ-ideals and partial characters on $\mathbb{Z}[X]^n$.*

Proof. By Lemma 31, a partial character defined a proper Laurent binomial σ-ideal. On the other side, let $\mathcal{I} \subseteq \mathcal{F}\{\mathbb{Y}^{\pm}\}$ be a proper Laurent binomial σ-ideal. $\mathcal{I}$ is generated by its members of the form $\mathbb{Y}^{\mathbf{f}} - c_{\mathbf{f}}$ for $\mathbf{f} \in \mathbb{Z}[x]^n$ and $c_{\mathbf{f}} \in \mathcal{F}^*$. Let $L_\rho = \mathbb{L}(\mathcal{I})$ which is defined in (10) and $\rho(\mathbf{f}) = c_{\mathbf{f}}$. Since $\mathcal{I}$ is proper, $c_{\mathbf{f}}$ is uniquely determined by $\mathbf{f}$. By Lemma 15 and Proposition 17, ρ is a partial character which is uniquely determined by $\mathcal{I}$. It is clear that $\mathcal{I}(\rho) = \mathcal{I}$. To show the correspondence is one to one, it suffices to show $\rho(\mathcal{I}(\rho)) = \rho$ which is a consequence of Lemma 32. The theorem is proved. □

As a summary of this section, we have the following canonical representations for a proper Laurent binomial σ-ideal, which follows directly from Theorems 23, 29, and 33.

Theorem 34. *$\mathcal{I}$ is a proper Laurent binomial σ-ideal if and only if one of the following statements holds.*

(1) *$\mathcal{I} = [\mathcal{A}]$, where $\mathcal{A}$ is a coherent Laurent binomial σ-chain.*
(2) *$\mathcal{I} = [\mathcal{A}]$, where $\mathcal{A} = \{\mathbb{Y}^{\mathbf{f}_1} - c_1, \ldots, \mathbb{Y}^{\mathbf{f}_s} - c_s\}$, $\mathbf{f}_i \in \mathbb{Z}[x]^n$, $c_i \in \mathcal{F}^*$, $\mathbb{f} = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$ is a reduced Gröbner basis of a $\mathbb{Z}[x]$-lattice, and $[\mathcal{A}] \neq [1]$.*
(3) *$\mathcal{I} = \mathcal{I}(\rho) = [\mathcal{A}]$, where ρ is a partial character on $\mathbb{Z}[x]^n$ and $\mathcal{A} = \mathcal{A}(\rho)$.*

Furthermore, $\mathcal{A}$ is a characteristic set of $\mathcal{I}$ and $(\mathbb{f})$ is the support lattice of $\mathcal{I}$.

5. Criteria for prime, reflexive, well-mixed, and perfect Laurent binomial σ-ideals

In this section, we give criteria for a Laurent binomial σ-ideal to be prime, reflexive, well-mixed, and perfect in terms of its support lattice and prove that the reflexive, well-mixed, and perfect closures for a Laurent binomial σ-ideal are still binomial. Decomposition theorems for well-mixed and perfect Laurent binomial σ-ideals are also given.

5.1. Reflexive and prime Laurent binomial σ-ideals

For the σ-indeterminates $\mathbb{Y} = \{y_1, \ldots, y_n\}$ and $t \in \mathbb{N}$, we will treat the elements of $\mathbb{Y}^{[t]} = \{y_1, y_1^x, \ldots, y_1^{x^t}, \ldots, y_n, y_1^x, \ldots, y_n^{x^t}\}$ as algebraic indeterminates, and $\mathcal{F}[\mathbb{Y}^{[\pm t]}]$ is the Laurent polynomial ring in $\mathbb{Y}^{[t]}$. Let $\mathcal{I}$ be a Laurent binomial σ-ideal in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$. Then it is easy to check that

$$\mathcal{I}_t = \mathcal{I} \cap \mathcal{F}[\mathbb{Y}^{[\pm t]}]$$

is a Laurent binomial ideal in $\mathcal{F}[\mathbb{Y}^{[\pm t]}]$.

Denote $\mathbb{Z}[x]_t$ to be the set of elements in $\mathbb{Z}[x]$ with degrees $\leq t$. Then $\mathbb{Z}[x]_t^n$ is the $\mathbb{Z}$-module generated by $x^i \boldsymbol{\epsilon}_l$ for $i = 0, \ldots, t, l = 1, \ldots, n$. It is clear that $\mathbb{Z}[x]_t^n$ is isomorphic to $\mathbb{Z}^{n(t+1)}$ as $\mathbb{Z}$-modules by mapping $x^i \boldsymbol{\epsilon}_l$ to the $((l-1)(t+1)+i+1)$-th standard basis vector in $\mathbb{Z}^{n(t+1)}$. Hence, we treat them as the same in this section. Let L be a $\mathbb{Z}[x]$-lattice and $t \in \mathbb{N}$. Then

$$L_t = L \cap \mathbb{Z}[x]_t^n = L \cap \mathbb{Z}^{n(t+1)}$$

is a $\mathbb{Z}$-module in $\mathbb{Z}^{n(t+1)}$. Similarly, it can be shown that when restricted to $\mathbb{Z}[x]_t^n$, a partial character ρ on $\mathbb{Z}[x]^n$ becomes a partial character ρ_t on $\mathbb{Z}^{n(t+1)}$.

Lemma 35. *With the notations introduced above and suppose that $\mathcal{I}(\rho_t)$ is the ideal in $\mathcal{F}[\mathbb{Y}^{[\pm t]}]$ defined by the partial character ρ_t on $\mathbb{Z}^{n(t+1)}$, we have $\mathcal{I}_t = \mathcal{I} \cap \mathcal{F}[\mathbb{Y}^{[\pm t]}] = \mathcal{I}(\rho_t)$.*

Proof. It suffices to show that the support lattice of $\mathcal{I}_t$ is $L_{\rho_t} = L_t$. By Lemma 32, $\mathbb{Y}^{\mathbf{f}} - c_m \in \mathcal{I}_t$ if and only if $\mathbf{f} \in L \cap \mathbb{Z}[x]_t^n$, or equivalently, $\max_{m \in \mathbf{f}} \deg(m, x) \leq t$, which is equivalent to $\mathbf{f} \in L_t$. □

Definition 36. Let L be a $\mathbb{Z}[x]$-module in $\mathbb{Z}[x]^n$.

- L is called *$\mathbb{Z}$-saturated* if, for any $0 \neq a \in \mathbb{Z}$ and $\mathbf{f} \in \mathbb{Z}[x]^n$, $a\mathbf{f} \in L$ implies $\mathbf{f} \in L$.
- L is called *x-saturated* if, for any $\mathbf{f} \in \mathbb{Z}[x]^n$, $x\mathbf{f} \in L$ implies $\mathbf{f} \in L$.
- L is called *saturated* if it is both $\mathbb{Z}$- and x- saturated.

Theorem 37. *Let ρ be a partial character on $\mathbb{Z}[x]^n$. If $\mathcal{F}$ is algebraically closed and inversive, then*

(a) *L_ρ is $\mathbb{Z}$-saturated if and only if $\mathcal{I}(\rho)$ is prime;*
(b) *L_ρ is x-saturated if and only if $\mathcal{I}(\rho)$ is reflexive;*
(c) *L_ρ is saturated if and only if $\mathcal{I}(\rho)$ is reflexive prime.*

Proof. It is clear that (c) comes from (a) and (b). Let $\mathcal{I} = \mathcal{I}(\rho)$ and $L = L_\rho$.

(*a*): $\mathcal{I}$ is a Laurent prime σ-ideal if and only if $\mathcal{I}_t$ is a Laurent prime ideal for all t. From Lemma 35, the support of $\mathcal{I}_t$ is L_t. Since $\mathcal{F}$ is algebraically closed, by Eisenbud and Sturmfels (1996, Theorem 2.1),

$\mathcal{I}_t$ is a Laurent prime ideal if and only if L_t is a $\mathbb{Z}$-saturated $\mathbb{Z}$-module. Furthermore, a $\mathbb{Z}[x]$-lattice L is $\mathbb{Z}$-saturated if and only if L_t is a $\mathbb{Z}$-saturated $\mathbb{Z}$-module for all t. Thus, (a) is valid.

(b): Suppose $\mathcal{I}$ is reflexive. For $x\mathbf{f} \in L$, by Lemma 32, there is a $\mathbb{Y}^{x\mathbf{f}} - c \in \mathcal{I}$. Since $\mathcal{F}$ is inversive, $c = d^x$ for $d \in \mathcal{F}$. Then $\sigma(\mathbb{Y}^{\mathbf{f}} - d) \in \mathcal{I}$ and hence $\mathbb{Y}^{\mathbf{f}} - d \in \mathcal{I}$ since $\mathcal{I}$ is reflexive. By Lemma 32 again, $\mathbf{f} \in L$ and L is x-saturated. To prove the other direction, assume L is x-saturated. For $f^x \in \mathcal{I}$, we have an expression

$$f^x = \sum_{i=1}^{s} f_i(\mathbb{Y}^{\mathbf{f}_i} - c_i) \tag{22}$$

where $\mathbb{Y}^{\mathbf{f}_i} - c_i \in \mathcal{I}$ and $0 \neq f_i \in \mathcal{F}\{\mathbb{Y}^{\pm}\}$. Let $d = \max_{i=1}^{s} \deg(\mathbb{Y}^{\mathbf{f}_i} - c_i, y_1)$ and assume $\mathbb{Y}^{\mathbf{f}_1} = M_1 y_1^d$. Replace y_1^d by c_1/M_1 in (22). Since (22) is an identity for the variables $y_i^{(j)}$, this replacement is meaningful and we obtain a new identity. $\mathbb{Y}^{\mathbf{f}_1} - c_1$ becomes zero after the replacement. Due to the way to choose d, if another summand, say $\mathbb{Y}^{\mathbf{f}_2} - c_2$, is affected by the replacement, then $\mathbb{Y}^{\mathbf{f}_2} = M_2 y_1^d$. After the replacement, $\mathbb{Y}^{\mathbf{f}_2} - c_2$ becomes $c_1(M_2/M_1 - c_2/c_1)$ which is also in $\mathcal{I}$ by Lemma 32. In summary, after the replacement, the right hand side of (22) has less than s nonzero summands and the left hand side of (22) does not changed. Repeat the above procedure, we will eventually obtain a new identity

$$f^x = \sum_{i=1}^{\bar{s}} \bar{f}_i(\mathbb{Y}^{x\mathbf{g}_i} - \bar{c}_i) \tag{23}$$

where $\mathbb{Y}^{x\mathbf{g}_i} - \bar{c}_i \in \mathcal{I}$ and $\bar{f}_i \in \mathcal{F}\{\mathbb{Y}^{\pm}\}$. We may assume that any y_i does not appear in $\bar{f}_i$. Otherwise, by setting y_i to be 1, the left hand side of (23) is not changes and a new identity is obtained. Since $\mathcal{F}$ is inversive, $\bar{c}_i = e_i^x$ and $\bar{f}_i = g_i^x$ for $e_i \in \mathcal{F}$ and $g_i \in \mathcal{F}\{\mathbb{Y}^{\pm}\}$. By Lemma 32, $\mathbb{Y}^{x\mathbf{g}_i} - e_i^x \in \mathcal{I}$ implies $x\mathbf{g}_i \in L$. Since L is x-saturated, $x\mathbf{g}_i \in L$ implies $\mathbf{g}_i \in L$ and hence $\mathbb{Y}^{\mathbf{g}_i} - e_i \in \mathcal{I}$ by Lemma 32 again. From (23), $\sigma(f - \sum_{i=1}^{\bar{s}} g_i(\mathbb{Y}^{\mathbf{g}_i} - e_i)) = 0$ and hence $f = \sum_{i=1}^{\bar{s}} g_i(\mathbb{Y}^{\mathbf{g}_i} - e_i) \in \mathcal{I}$. (b) is proved. □

Example 38. This example is used to show that the condition for $\mathcal{F}$ to be algebraically closed and inversive is necessary for Theorem 37 to be valid. If $\mathcal{F} = \mathbb{Q}(\lambda)$ and $\sigma(f(\lambda)) = f(\lambda+1)$, then $[y_1^2 y_2^2 - \lambda]$ is prime but its support lattice $([2,2]^\tau)$ is not $\mathbb{Z}$-saturated; if $\mathcal{F} = \mathbb{Q}(\lambda)$ and $\sigma(f(\lambda)) = f(\lambda^2)$, then $[y_1^x y_2^x - \lambda]$ is reflexive but its support lattice $([x,x]^\tau)$ is not x-saturated.

Definition 39. Let $L \subset \mathbb{Z}[x]^n$ be a $\mathbb{Z}[x]$-lattice. The *$\mathbb{Z}$-saturation* of L is $\mathrm{sat}_{\mathbb{Z}}(L) := \{\mathbf{f} \in \mathbb{Z}[x]^n \mid \exists a \in \mathbb{Z},\ \text{s.t. } a \neq 0 \text{ and } a\mathbf{f} \in L\}$. The *$x$-saturation* of L is $\mathrm{sat}_x(L) := \{\mathbf{f} \in \mathbb{Z}[x]^n \mid x\mathbf{f} \in L\}$. The *saturation* of L is $\mathrm{sat}(L) := \mathrm{sat}_{\mathbb{Z}}(\mathrm{sat}_x(L))$.

It is clear that $\mathrm{sat}_{\mathbb{Z}}(L)$ is $\mathbb{Z}$-saturated, $\mathrm{sat}_x(L)$ is x-saturated, and $\mathrm{sat}(L)$ is both x- and $\mathbb{Z}$-saturated since $\mathrm{sat}_{\mathbb{Z}}(\mathrm{sat}_x(L)) = \mathrm{sat}_x(\mathrm{sat}_{\mathbb{Z}}(L))$.

Theorem 40. *Let $\mathcal{I}$ be a Laurent binomial σ-ideal and L the support lattice of $\mathcal{I}$. If $\mathcal{F}$ is inversive, then the reflexive closure of $\mathcal{I}$ is also a Laurent binomial σ-ideal whose support lattice is the x-saturation of L.*

Proof. Let $\mathcal{I}_x$ be the reflexive closure of $\mathcal{I}$ and $L_x = \mathrm{sat}_x(L)$. Suppose $\mathcal{I} = [f_1, \ldots, f_r]$, where $f_i = \mathbb{Y}^{\mathbf{f}_i} - c_i$. Then $L = (\mathbf{f}_1, \ldots, \mathbf{f}_r)$. If L is x-saturated, by Theorem 37, $\mathcal{I}$ is reflexive. Otherwise, there exist $k_1 \in \mathbb{N}$, $b_i \in \mathbb{Z}[x]$, and $\mathbf{h}_1 \in \mathbb{Z}[x]^n$ such that $\mathbf{h}_1 \notin L$ and

$$x^{k_1}\mathbf{h}_1 = \sum_{i=1}^{r} b_i \mathbf{f}_i \in L. \tag{24}$$

By Lemma 15, $\mathbb{Y}^{x^{k_1}\mathbf{h}_1} - \widetilde{a}$ is in $\mathcal{I}$, where $\widetilde{a} = \prod_{i=1}^{r} c_i^{b_i}$. Since $\mathcal{F}$ is inversive, $\overline{a} = \sigma^{-k_1}(\widetilde{a}) \in \mathcal{F}$. Then, $\sigma^{k_1}(\mathbb{Y}^{\mathbf{h}_1} - \overline{a}) \in \mathcal{I}$, and hence $\mathbb{Y}^{\mathbf{h}_1} - \overline{a} \in \mathcal{I}_x$. Let $\mathcal{I}_1 = [f_1, \ldots, f_r, \mathbb{Y}^{\mathbf{h}_1} - \overline{a}]$. It is clear that

$L_1 = (\mathbf{f}_1, \ldots, \mathbf{f}_r, \mathbf{h}_1)$ is the support lattice of $\mathcal{I}_1$. Then $\mathcal{I} \subsetneq \mathcal{I}_1 \subset \mathcal{I}_x$ and $L \subsetneq L_1 \subset L_x$. Repeating the above procedure for $\mathcal{I}_1$ and L_1, we obtain $\mathcal{I}_2$ and $L_2 = (\mathbf{f}_1, \ldots, \mathbf{f}_r, \mathbf{h}_1, \mathbf{h}_2)$ such that $\mathbf{h}_2 \notin L_1$ and $x^{k_2}\mathbf{h}_2 \in L_1$. We claim that $L_2 \subset L_x$. Indeed, let $x^{k_2}\mathbf{h}_2 = \sum_{i=1}^r e_i\mathbf{f}_i + e_0\mathbf{h}_1$. Then by (24), $x^{k_1+k_2}\mathbf{h}_2 = x^{k_1}(x^{k_2}\mathbf{h}_2) = x^{k_1}\sum_{i=1}^r e_i\mathbf{f}_i + e_0(x^{k_1}\mathbf{h}_1) = x^{k_1}\sum_{i=1}^r e_i\mathbf{f}_i + e_0\sum_{i=1}^r b_i\mathbf{f}_i \in L$ and the claim is proved. As a consequence, $\mathcal{I}_2 \subset \mathcal{I}_x$.

Continuing the process, we have $\mathcal{I} \subsetneq \mathcal{I}_1 \subsetneq \cdots \subsetneq \mathcal{I}_t \subset \mathcal{I}_x$ and $L \subsetneq L_1 \subsetneq \cdots \subsetneq L_t \subset L_x$ such that L_i is the support lattice of $\mathcal{I}_i$. The process will terminate, since $\mathbb{Z}[x]^n$ is Noetherian. The final $\mathbb{Z}[x]$-lattice L_t is x-saturated and hence $\mathcal{I}_t$ is reflexive by Theorem 37. Since L_x is the smallest x-saturated $\mathbb{Z}[x]$-lattice containing L and $L \subset L_t \subset L_x$, we have $L_t = L_x$ and $\mathcal{I}_t = \mathcal{I}_x$. □

Corollary 41. *Let $L \subset \mathbb{Z}[x]^n$ be a $\mathbb{Z}[x]$-lattice. Then* $\mathrm{rk}(L) = \mathrm{rk}(\mathrm{sat}_x(L))$ *and* $\mathrm{rk}(L) = \mathrm{rk}(\mathrm{sat}_{\mathbb{Z}}(L))$.

Proof. From the proof of Theorem 40, $\mathrm{sat}_x(L) = (L, \mathbf{h}_1, \ldots, \mathbf{h}_t)$ and for each $\mathbf{h}_i$, there is a positive integer n_i such that $x^{n_i}\mathbf{h}_i \in L$. Let A be a representation matrix of L. Then a representation matrix B of L_x can be obtained by adding to A a finite number of new columns which are linear combinations of columns of A divided by some x^d. Therefore, $\mathrm{rk}(A) = \mathrm{rk}(B)$. We can prove $\mathrm{rk}(L) = \mathrm{rk}(\mathrm{sat}_{\mathbb{Z}}(L))$ similarly. □

We now give a decomposition theorem for perfect σ-ideals.

Theorem 42. *Let $\mathcal{I}$ be a Laurent binomial σ-ideal, L the support lattice of $\mathcal{I}$, and L_S the saturation of L. If $\mathcal{F}$ is algebraically closed and inversive, then $\{\mathcal{I}\}$ is either* [1] *or can be written as the intersection of Laurent reflexive prime binomial σ-ideals whose support lattice is L_S.*

Proof. Let $\mathcal{I}_x$ be the reflexive closure of $\mathcal{I}$ and $L_x = \mathrm{sat}_x(L)$. By Theorem 40, L_x is the support lattice of $\mathcal{I}_x$. Suppose $\mathcal{I}_x = [f_1, \ldots, f_r]$, $f_i = \mathbb{Y}^{\mathbf{f}_i} - c_i, i = 1, \ldots, r$, and $L_x = (\mathbf{f}_1, \ldots, \mathbf{f}_r)$. If L_x is $\mathbb{Z}$-saturated, then by Theorem 37, $\mathcal{I}_x$ is reflexive prime. Otherwise, there exist $k_1 \in \mathbb{N}$, $a_i \in \mathbb{Z}[x]$, and $\mathbf{h}_1 \in \mathbb{Z}[x]^n$ such that $\mathbf{h}_1 \notin L_x$ and

$$k_1\mathbf{h}_1 = a_1\mathbf{f}_1 + \cdots + a_r\mathbf{f}_r \in L_x. \tag{25}$$

By Lemma 15, $\mathbb{Y}^{k_1\mathbf{h}_1} - \widetilde{a} \in \mathcal{I}$, where $\widetilde{a} = \prod_{i=1}^r c_i^{a_i}$. Since $\mathcal{F}$ is algebraically closed,

$$\mathbb{Y}^{k_1\mathbf{h}_1} - \widetilde{a} = \prod_{l=1}^{k_1}(\mathbb{Y}^{\mathbf{h}_1} - \widetilde{a}_l) \in \mathcal{I}_x$$

where $\widetilde{a}_l, l = 1, \ldots, k_1$ are the k_1-th roots of $\widetilde{a}$. By Lemma II in Cohn (1965, p. 83), we have the following decomposition

$$\{\mathcal{I}\} = \{\mathcal{I}_x\} = \cap_{l_1=1}^{k_1}\{\mathcal{I}_{1l_1}\}$$

where $\mathcal{I}_{1l} = [f_1, \ldots, f_r, \mathbb{Y}^{\mathbf{h}_1} - \widetilde{a}_l]$. Remove those $\mathcal{I}_{1l_1}$ satisfying $\mathcal{I}_{1l_1} = [1]$. If $\mathcal{I}_{1l_1} = [1]$ for all l_1, then $\{\mathcal{I}\} = [1]$. Then the support lattice for any of $\mathcal{I}_{1l}$ is $L_1 = (\mathbf{f}_1, \ldots, \mathbf{f}_r, \mathbf{h}_1)$. Similar to the proof of Theorem 40, we can show that $\mathcal{I}_x \subsetneq \mathcal{I}_{1l}$ and $L_x \subsetneq L_1 \subset L_S$.

Repeating the process, we have $\mathcal{I}_x \subsetneq \mathcal{I}_{1l_1} \subsetneq \cdots \subsetneq \mathcal{I}_{tl_t}$ for $l_i = 1, \ldots, k_i$ and $L_x \subsetneq L_1 \subsetneq L_2 \subsetneq \cdots \subsetneq L_t \subset L_S$ such that L_i is the support lattice of $\mathcal{I}_{il_i}$ for $l_i = 1, \ldots, k_i$ and

$$\{\mathcal{I}\} = \cap_{l_i=1}^{k_i}\{\mathcal{I}_{il_i}\}, i = 1, \ldots, t.$$

The process will terminate, since $\mathbb{Z}[x]^n$ is Noetherian. Since L_S is the smallest $\mathbb{Z}$-saturated $\mathbb{Z}[x]$-lattice containing L_x and $L_x \subset L_t \subset L_S$, we have $L_t = \mathrm{sat}_{\mathbb{Z}}(L_x) = \mathrm{sat}_{\mathbb{Z}}(\mathrm{sat}_x(L)) = L_S$. Then $\mathcal{I}_{tl_t}$ is reflexive prime and the theorem is proved. □

Since the reflexive prime components of $\mathcal{I}$ have the same support lattice, by Corollary 24, they also have the same dimension.

Corollary 43. *A Laurent binomial σ-ideal $\mathcal{I}$ is dimensionally unmixed, that is, the reflexive prime components of $\mathcal{I}$ have the same dimension.*

Example 44. We use this example to show that $\{\mathcal{I}\} = [1]$ can indeed happen in Theorem 42. Let $\mathcal{I} = [\mathcal{A}_1]$, where $\mathcal{A}_1$ is from (12). We have $y_2^2 - y_1^2 = y_2^2 + 1 - (y_1^2 + 1) \in \mathcal{I}$. Then $\{\mathcal{I}\} = \{\mathcal{I}, y_2 - y_1\} \cap \{\mathcal{I}, y_2 + y_1\}$ and it is easy to check that $\{\mathcal{I}, y_2 - y_1\} = \{\mathcal{I}, y_2 + y_1\} = [1]$.

Also, if $\mathcal{F}$ is not algebraically closed, then $\{\mathcal{I}\}$ may not be decomposed as the intersection of binomial ideals. For instance, if $\mathcal{F} = \mathbb{Q}$, then $\{y_1^3 - 1\} = [y_1 - 1] \cap [y_1^2 + y_1 + 1, y_1^x - y_1] \cap [y_1^2 + y_1 + 1, y_1^x + y_1 + 1]$.

5.2. Well-mixed and perfect Laurent binomial σ-ideals

For $S \subset \mathcal{F}\{\mathbb{Y}^{\pm}\}$, let $S' = \{fg^x | fg \in S\}$. We define inductively: $S_0 = S, S_n = [S_{n-1}]', n = 1, 2, \ldots$. The union of the S_n is clearly a well-mixed σ-ideal and is contained in every well-mixed σ-ideal containing S. Hence this union is $\langle S \rangle$. If $\mathcal{I} \subset \mathcal{F}\{\mathbb{Y}^{\pm}\}$ is a Laurent σ-ideal, then $\langle \mathcal{I} \rangle$ is called the *well-mixed closure* of $\mathcal{I}$. We first prove some basic properties of well-mixed σ-ideals. Note that these properties are also valid in $\mathcal{F}\{\mathbb{Y}\}$.

Lemma 45. *Let S_1, S_2 be two subsets of $\mathcal{F}\{\mathbb{Y}^{\pm}\}$ which satisfy the condition that $a \in S_i$ implies $\sigma(a) \in S_i$, $i = 1, 2$. Then $[S_1]_n[S_2]_n \subset [S_1 S_2]_n$.*

Proof. Let $s \in [S_1]_1$ and $t \in [S_2]_1$. Then $s = f_1 g_1^x$ and $t = f_2 g_2^x$ where $f_1 g_1 \in [S_1]$, $f_2 g_2 \in [S_2]$. Then, $f_1 g_1 f_2 g_2 \in [S_1 S_2]$, and $st = f_1 f_2 (g_1 g_2)^x \in [S_1 S_2]_1$. Hence, $[S_1]_1[S_2]_1 \subset [S_1 S_2]_1$. By induction, $[S_1]_n[S_2]_n \subset [S_1 S_2]_n$. □

Lemma 46. *Let S_1, S_2 be two subsets of $\mathcal{F}\{\mathbb{Y}^{\pm}\}$ which satisfy the condition that $a \in S_i$ implies $\sigma(a) \in S_i$, $i = 1, 2$. Then $\sqrt{[S_1 S_2]_n} = \sqrt{[S_1]_n \cap [S_2]_n}$ for $n \geq 1$, and $\sqrt{\langle S_1 \rangle} \cap \sqrt{\langle S_2 \rangle} = \sqrt{\langle S_1 S_2 \rangle}$.*

Proof. The last statement is an immediate consequence of the first one. Since $[S_1 S_2] \subset [S_i]$, we have $[S_1 S_2]_n \subset [S_i]_n$ for $i = 1, 2$, and $[S_1 S_2]_n \subset [S_1]_n \cap [S_2]_n$ follows. Hence, $\sqrt{[S_1 S_2]_n} \subset \sqrt{[S_1]_n \cap [S_2]_n}$. Let $a \in [S_1]_n \cap [S_2]_n$ we have $a^2 \in [S_1]_n[S_2]_n$. By Lemma 45, $a^2 \in [S_1 S_2]_n$. Hence $a \in \sqrt{[S_1 S_2]_n}$, and $\sqrt{[S_1]_n \cap [S_2]_n} \subset \sqrt{[S_1 S_2]_n}$ follows. □

Lemma 47. *Let $\mathcal{I}_1, \ldots, \mathcal{I}_m$ be Laurent σ-ideals. Then $\sqrt{\langle \cap_{i=1}^m \mathcal{I}_i \rangle} = \cap_{i=1}^m \sqrt{\langle \mathcal{I}_i \rangle}$.*

Proof. Let $\mathcal{I} = \cap_{i=1}^m \mathcal{I}_i$. By Lemma 46, we have $\sqrt{\langle \prod_{i=1}^m \mathcal{I}_i \rangle} = \sqrt{\prod_{i=1}^{m-1} \langle \mathcal{I}_i \rangle} \cap \sqrt{\langle \mathcal{I}_m \rangle} = \ldots = \cap_{i=1}^m \sqrt{\langle \mathcal{I}_i \rangle}$. Now we show that $\sqrt{\langle \mathcal{I} \rangle} = \sqrt{\langle \prod_{i=1}^m \mathcal{I}_i \rangle}$. Since $\prod_{i=1}^m \mathcal{I}_i \subset \mathcal{I}$, we have $\sqrt{\langle \prod_{i=1}^m \mathcal{I}_i \rangle} \subset \sqrt{\langle \mathcal{I} \rangle}$. By Lemma 46, $\sqrt{\langle \mathcal{I} \rangle} = \sqrt{\langle \mathcal{I} \rangle} \cap \cdots \cap \sqrt{\langle \mathcal{I} \rangle} = \sqrt{\langle \mathcal{I}^m \rangle} \subset \sqrt{\langle \prod_{i=1}^m \mathcal{I}_i \rangle}$, and hence $\sqrt{\langle \mathcal{I} \rangle} = \sqrt{\langle \prod_{i=1}^m \mathcal{I}_i \rangle}$. Then, $\sqrt{\langle \mathcal{I} \rangle} = \cap_{i=1}^m \sqrt{\langle \mathcal{I}_i \rangle}$. □

Now, we prove a basic property for a σ-field $\mathcal{F}$.

Lemma 48. *Let $\zeta_m = e^{\frac{2\pi \mathrm{i}}{m}}$ be the primitive m-th root of unity, where $\mathrm{i} = \sqrt{-1}$ and $m \in \mathbb{Z}_{\geq 2}$. If $\zeta_m \in \mathcal{F}$, then there exists an $o_m \in [0, m-1]$ such that $\gcd(o_m, m) = 1$ and $\sigma(\zeta_m) = \zeta_m^{o_m}$. Furthermore, the perfect σ-ideal $\{y^m - 1\}$ in $\mathcal{F}\{y\}$ is*

$$\{y^m - 1\} = [y^m - 1, y^x - y^{o_m}] \tag{26}$$

where y is a σ-indeterminate.

Proof. Since $\zeta_m \in \mathcal{F}$, we have $y^m - 1 = \prod_{j=0}^{m-1}(y - \zeta_m^j)$. From $(\zeta_m)^m - 1 = \prod_{j=0}^{m-1}(\zeta_m - \zeta_m^j) = 0$, we have $\sigma(\zeta_m)^m - 1 = \prod_{j=0}^{m-1}(\sigma(\zeta_m) - \zeta_m^j) = 0$. Then, there exists an o_m such that $0 \le o_m \le m-1$ and $\sigma(\zeta_m) = \zeta_m^{o_m}$. Suppose $\gcd(o_m, m) = d > 1$ and let $o_m = dk, m = ds$, where $s \in [1, m-1]$. Then $\sigma(\zeta_m^s) = \zeta_m^{o_m s} = \zeta_m^{dks} = \zeta_m^{km} = 1$, which implies $\zeta_m^s = 1$, a contradiction.

By Lemma II in Cohn (1965, p. 83), we have $\{y^m - 1\} = \cap_{j=0}^{m-1}[y - \zeta_m^j]$. In order to show (26), it suffices to show $\cap_{j=0}^{m-1}[y - \zeta_m^j] = [y^m - 1, y^x - y^{o_m}]$. Since $y^x - y^{o_m} = (y - \zeta_m^j)^x + \zeta_m^{xj} - y^{o_m} = (y - \zeta_m^j)^x + \zeta_m^{jo_m} - y^{o_m} \in [y - \zeta_m^j]$ for any $0 \le j \le m-1$, we have $y^x - y^{o_m} \in \cap_{j=0}^{m-1}[y - \zeta_m^j]$ and hence $[y^m - 1, y^x - y^{o_m}] \subset \cap_{j=0}^{m-1}[y - \zeta_m^j]$. Let $f \in \cap_{j=0}^{m-1}[y - \zeta_m^j]$. Since $y^x - y^{o_m} \in [y - \zeta_m^j]$, for $j = 0, \ldots, m-1$, from $f \in [y - \zeta_m^j]$, we have $f = g_j(y - \zeta_m^j) + \sum_k h_{jk}(y^x - y^{o_m})^{x^k}$, where $g_j, h_{jk} \in \mathcal{F}\{y\}$. Then $f^m = \prod_{j=0}^{m-1}(g_j(y - \zeta_m^j) + \sum_k h_{jk}(y^x - y^{o_m})^{kx}) = (\prod_{j=0}^{m-1} g_j)(y^m - 1) + p$, where $p \in [y^x - y^{o_m}]$. Hence, $f \in [y^m - 1, y^x - y^{o_m}]$ and $\cap_{j=0}^{m-1}[y - \zeta_m^j] \subset [y^m - 1, y^x - y^{o_m}]$. The lemma is proved. □

The following example shows how a perfect σ-ideal depends on o_m.

Example 49. Let $\mathcal{F} = \mathbb{Q}(\sqrt{-3})$ and $p = y_1^3 - 1$. Following Lemma 48, if $\sigma(\sqrt{-3}) = \sqrt{-3}$, then $o_3 = 1$ and $\{p\} = [p, y_1^x - y_1]$. If $\sigma(\sqrt{-3}) = -\sqrt{-3}$, then $o_3 = 2$ and $\{p\} = [p, y_1^x - y_1^2]$.

The number o_m introduced in Lemma 48 depends on $\mathcal{F}$ only and is called the *m-th transforming degree* of unity. In the following corollaries, $\mathcal{F}$ is assumed to be algebraically closed and hence o_m is defined for any $m \in \mathbb{N}$. From the proof of Lemma 48, we have

Corollary 50. $y^x - y^{o_m} \in \cap_{j=0}^{m-1}[y - \zeta_m^j]$.

Corollary 51. *For n, m, k in $\mathbb{N}$, if $n = km$ then $o_n = o_m \bmod m$.*

Proof. By definition, $\zeta_n^k = \zeta_m$. Then, $\sigma(\zeta_n^k) = \zeta_n^{ko_n} = \zeta_m^{o_n}$. From, $\sigma(\zeta_n^k) = \sigma(\zeta_m) = \zeta_m^{o_m}$, we have $\zeta_m^{o_n} = \zeta_m^{o_m}$. Then $o_n = o_m \bmod m$. □

Lemma 52. $\langle y^m - 1\rangle = \{y^m - 1\} = [y^m - 1, y^x - y^{o_m}]$.

Proof. By Lemma 48, it suffices to show $y^x - y^{o_m} \in \langle y^m - 1\rangle$. Since $y^m - 1 = \prod_{j=0}^{m-1}(y - \zeta_m^j)$ and $(y - \zeta_m^i)^x = (y^x - \zeta_m^{o_m i})$, we have $f_i = (y^x - \zeta_m^{o_m i})\prod_{0\le j\le m-1, j\ne i}(y - \zeta_m^j) \in \langle y^m - 1\rangle$ for $i = 0, \ldots, m-1$. We will show that $y^x - y^{o_m} \in (f_0, \ldots, f_{m-1})$. To show this, we need the formula $\frac{1}{y^m-1} = \sum_{i=0}^{m-1} \frac{1}{m(\zeta_m^i)^{m-1}(y-\zeta_m^i)} = \frac{1}{m}\sum_{i=0}^{m-1} \frac{\zeta_m^i}{y-\zeta_m^i}$ from Geddes et al. (1992, p. 494). We have

$$\begin{aligned}
\frac{1}{m}\sum_{i=0}^{m-1}\zeta_m^i f_i &= \frac{1}{m}\sum_{i=0}^{m-1}\zeta_m^i \frac{y^m-1}{y-\zeta_m^i}(y^x - \zeta_m^{o_m i}) \\
&= \frac{1}{m}\sum_{i=0}^{m-1}\zeta_m^i \frac{y^m-1}{y-\zeta_m^i}y^x - \frac{1}{m}\sum_{i=0}^{m-1}\zeta_m^i \frac{y^m-1}{y-\zeta_m^i}\zeta_m^{o_m i} \\
&= y^x - \frac{1}{m}\sum_{i=0}^{m-1}\frac{y^m-1}{y-\zeta_m^i}\zeta_m^{(o_m+1)i}.
\end{aligned}$$

Let $g(y) = \frac{1}{m}\sum_{i=0}^{m-1}\frac{y^m-1}{y-\zeta_m^i}\zeta_m^{(o_m+1)i}$ and note that $\prod_{1\le i\le m-1}(\zeta_m^i - 1) = (-1)^{m-1}m$. Then, we have $g(\zeta_m^j) = \frac{1}{m}\zeta_m^{(o_m+1)j}\frac{y^m-1}{y-\zeta_m^j}\big|_{y=\zeta_m^j} = \frac{1}{m}\zeta_m^{(o_m+1)j}\prod_{0\le i\le m-1, i\ne j}(\zeta_m^j - \zeta_m^i) = \frac{1}{m}\zeta_m^{(o_m+1)j}\zeta_m^{j(m-1)}(-1)^{m-1} \times$

$\prod_{1\le i\le m-1}(\zeta_m^i - 1) = \frac{1}{m}\zeta_m^{o_m j} m = (\zeta_m^j)^{o_m}$. Since $\deg(g(y)) \le m-1$ and $g(\zeta_m^j) = (\zeta_m^j)^{o_m}$ for $j = 0, \ldots, m-1$, we have $g(y) = y^{o_m}$. Hence $y^x - y^{o_m} \in (f_0, \ldots, f_{m-1}) \subset \langle y^m - 1\rangle$. □

Corollary 53. *For $m \in \mathbb{N}$, $a \in \mathcal{F}^*$, and $\mathbf{f} \in \mathbb{Z}[x]^n$, we have $\mathbb{Y}^{(x-o_m)\mathbf{f}} - a^{x-o_m} \in \langle \mathbb{Y}^{m\mathbf{f}} - a^m\rangle$.*

Proof. Let $z = \frac{\mathbb{Y}^{\mathbf{f}}}{a}$ and $\mathcal{I} = [\mathbb{Y}^{m\mathbf{f}} - a^m]$. Then $z^m - 1 \in \mathcal{I}$. By Lemma 52, $z^{x-o_m} - 1 \in \langle z^m - 1\rangle \subset \langle \mathcal{I}\rangle$. Then $(\frac{\mathbb{Y}^{\mathbf{f}}}{a})^{x-o_m} - 1 \in \langle \mathcal{I}\rangle$ or $\mathbb{Y}^{(x-o_m)\mathbf{f}} - a^{x-o_m} \in \langle \mathcal{I}\rangle$. □

Motivated by Corollary 53, we have the following definition.

Definition 54. A $\mathbb{Z}[x]$-lattice L is called M-*saturated* if it satisfies

$$m\mathbf{f} \in L \Rightarrow (x - o_m)\mathbf{f} \in L \tag{27}$$

where $m \in \mathbb{N} \setminus \{0, 1\}$, $\mathbf{f} \in \mathbb{Z}[x]^n$, and o_m is defined in Lemma 48. For any $\mathbb{Z}[x]$-lattice L, the smallest M-saturated $\mathbb{Z}[x]$-lattice containing L is called the M-saturation of L and is denoted by $\mathrm{sat}_M(L)$.

The following result gives an effective version for condition (27).

Lemma 55. *A $\mathbb{Z}[x]^n$-lattice L is M-saturated if and only if the following condition is true: Let $L_1 = \mathrm{sat}_{\mathbb{Z}}(L) = (\mathbf{g}_1, \ldots, \mathbf{g}_s)$ such that $m_i\mathbf{g}_i \in L$ for $m_i \in \mathbb{N}$. Then $(x - o_{m_i})\mathbf{g}_i \in L$.*

Proof. We need only to show $(x - o_{m_i})\mathbf{g}_i \in L$ implies (27). For any $m\mathbf{f} \in L$, we have $\mathbf{f} \in L_1$ and hence $\mathbf{f} = \sum_{i=1}^s q_i\mathbf{g}_i$, where $q_i \in \mathbb{Z}[x]$. Let $t = \mathrm{lcm}(m, m_1, \ldots, m_s)$. By Corollary 51, we have $o_t = o_{m_i} + c_i m_i$, where $c_i \in \mathbb{Z}$. Then $(x - o_t)\mathbf{f} = \sum_{i=1}^s q_i(x - o_t)\mathbf{g}_i = \sum_{i=1}^s q_i(x - o_{m_i})\mathbf{g}_i - \sum_{i=1}^s q_i c_i m_i \mathbf{g}_i \in L$. By Corollary 51, $o_t = o_m + cm$, where $c \in \mathbb{Z}$. Then $(x - o_m)\mathbf{f} = (x - o_t)\mathbf{f} + cm\mathbf{f} \in L$. □

We now give a criterion for a Laurent binomial σ-ideal to be well-mixed.

Theorem 56. *Let ρ be a partial character and $\mathcal{F}$ an algebraically closed σ-field. If $\mathcal{I}(\rho)$ is well-mixed, then L_ρ is* M*-saturated. Conversely, if L_ρ is* M*-saturated, then either $\langle \mathcal{I}(\rho)\rangle = [1]$ or $\mathcal{I}(\rho)$ is well-mixed and in this case $\mathcal{I}(\rho)$ can be written as the intersection of Laurent prime binomial σ-ideals with support lattice $\mathrm{sat}_{\mathbb{Z}}(L_\rho)$.*

Proof. Suppose that $\mathcal{I}(\rho)$ is well-mixed. If there exists an $m \in \mathbb{N}$ such that $m\mathbf{f} \in L_\rho$, then by Lemma 32, there exists a $c \in \mathcal{F}^*$ such that $\mathbb{Y}^{m\mathbf{f}} - c \in \mathcal{I}(\rho)$. Since $\mathcal{F}$ is algebraically closed, there exists an $a \in \mathcal{F}^*$ such that $c = a^m$. Then, $\mathbb{Y}^{m\mathbf{f}} - a^m \in \mathcal{I}(\rho)$. Since $\mathcal{I}(\rho)$ is well-mixed, by Corollary 53, $\mathbb{Y}^{(x-o_m)\mathbf{f}} - a^{x-o_m} \in \mathcal{I}(\rho)$, and by Lemma 32 again, $(x - o_m)\mathbf{f} \in L_\rho$ follows and L_ρ is M-saturated.

Conversely, let L_ρ be M-saturated. If L_ρ is $\mathbb{Z}$-saturated, then by Theorem 37, $\mathcal{I}(\rho)$ is prime and hence well-mixed. Otherwise, there exists an $m_1 \in \mathbb{N}$, and $\mathbf{f} \in \mathbb{Z}[x]^n$ such that $\mathbf{f} \notin L_\rho$ and $m_1\mathbf{f} \in L_\rho$. By Lemma 32, there exists an $a \in \mathcal{F}^*$ such that $\mathbb{Y}^{m_1\mathbf{f}} - a^{m_1} \in \mathcal{I}(\rho)$. We claim that either $\langle \mathcal{I}(\rho)\rangle = [1]$ or

$$\mathcal{I}(\rho) = \cap_{l_1=0}^{m_1-1}\mathcal{I}_{l_1} \tag{28}$$

where $\mathcal{I}_{l_1} = [\mathcal{I}(\rho), \mathbb{Y}^{\mathbf{f}} - a\zeta_{m_1}^{l_1}]$ and $\zeta_{m_1} = e^{\frac{2\pi \mathrm{i}}{m_1}}$. By (27), $(x - o_{m_1})\mathbf{f} \in L_\rho$. By Lemma 32, there exists a $b \in \mathcal{F}^*$ such that $\mathbb{Y}^{(x-o_{m_1})\mathbf{f}} - b \in \mathcal{I}(\rho)$. Since $\mathbb{Y}^{m_1\mathbf{f}} - a^{m_1} \in \mathcal{I}(\rho)$, by Corollary 50, we have $\mathbb{Y}^{(x-o_{m_1})\mathbf{f}} - a^{x-o_{m_1}} \in [\mathbb{Y}^{\mathbf{f}} - a\zeta_{m_1}^{l_1}]$ for any $l_1 \in [0, m_1 - 1]$. Then $b - a^{x-o_{m_1}} = \mathbb{Y}^{(x-o_{m_1})\mathbf{f}} - a^{x-o_{m_1}} - (\mathbb{Y}^{(x-o_{m_1})\mathbf{f}} - b) \in \mathcal{I}_{l_1}$ for any l_1. If $b \ne a^{x-o_{m_1}}$, $\mathcal{I}_{l_1} = [1]$ for all l_1, and hence $1 \in \cap_{l_1=0}^{m_1-1}\mathcal{I}_{l_1} \subset \langle \mathcal{I}(\rho)\rangle$ by Lemma 52 and $\langle \mathcal{I}(\rho)\rangle = [1]$ follows. Now suppose $b = a^{x-o_{m_1}}$ or $a^x = ba^{o_{m_1}}$. To prove (28), it suffices to show $\cap_{l_1=0}^{m_1-1}\mathcal{I}_{l_1} \subset \mathcal{I}(\rho)$. Let $f \in \cap_{l_1=0}^{m_1-1}\mathcal{I}_{l_1}$. From $f \in \mathcal{I}_{l_1}$, we have $f = f_{l_1} + \sum_{j=0}^s p_j\sigma^j(\mathbb{Y}^{\mathbf{f}} - a\zeta_{m_1}^{l_1})$, where $f_{l_1} \in \mathcal{I}(\rho)$, $p_j \in \mathcal{F}\{\mathbb{Y}^{\pm}\}$. By Lemma 48, $\sigma(\zeta_{m_1}) = \zeta_{m_1}^{o_{m_1}}$. We thus have

$$\sigma(\mathbb{Y}^{\mathbf{f}} - a\zeta_{m_1}^{l_1}) = \mathbb{Y}^{x\mathbf{f}} - b\mathbb{Y}^{o_{m_1}\mathbf{f}} + b\mathbb{Y}^{o_{m_1}\mathbf{f}} - \sigma(a\zeta_{m_1}^{l_1})$$
$$= \mathbb{Y}^{o_{m_1}\mathbf{f}}(\mathbb{Y}^{(x-o_{m_1})\mathbf{f}} - b) + b(\mathbb{Y}^{o_{m_1}\mathbf{f}} - a^{o_{m_1}}\zeta_{m_1}^{l_1 o_{m_1}}) + (ba^{o_{m_1}} - \sigma(a))\zeta_{m_1}^{l_1 o_{m_1}}.$$

Since $\mathbb{Y}^{(x-o_{m_1})\mathbf{f}} - b \in \mathcal{I}(\rho)$ and $ba^{o_{m_1}} - \sigma(a) = ba^{o_{m_1}} - a^x = 0$, we have $\sigma(\mathbb{Y}^{\mathbf{f}} - a\zeta_{m_1}^{l_1}) = g_{l_1} + q_{l_1}(\mathbb{Y}^{\mathbf{f}} - a\zeta_{m_1}^{l_1})$, where $g_{l_1} \in \mathcal{I}(\rho), q_{l_1} \in \mathcal{F}\{\mathbb{Y}^{\pm}\}$. Using the above equation repeatedly, we have $f = h_{l_1} + p_{l_1}(\mathbb{Y}^{\mathbf{f}} - a\zeta_{m_1}^{l_1})$, where $h_{l_1} \in \mathcal{I}(\rho)$. Then, $f^{m_1} = \prod_{l_1=0}^{m_1-1}(h_{l_1} + p_{l_1}(\mathbb{Y}^{\mathbf{f}} - a\zeta_{m_1}^{l_1})) = s_1 + \prod_{l_1=0}^{m_1-1} p_{l_1}(\mathbb{Y}^{\mathbf{f}} - a\zeta_{m_1}^{l_1}) = s_1 + (\mathbb{Y}^{m_1\mathbf{f}} - a^{m_1})\prod_{l_1=0}^{m_1-1} p_{l_1} \in \mathcal{I}(\rho)$, where s_1 is in $\mathcal{I}(\rho)$. By Corollary 25, we have $f \in \mathcal{I}(\rho)$. The claim is proved.

The support lattice for any of $[\mathcal{I}_{l_1}]$ is $L_1 = (L_\rho, \mathbf{f})$. Similar to the proof of Theorem 40, we can show that $\mathcal{I}(\rho) \subsetneq \mathcal{I}_{l_1}$ and $L_\rho \subsetneq L_1$. If L_1 is not $\mathbb{Z}$-saturated, there exists a $k > 1$ and $\mathbf{g} \in \mathbb{Z}[x]^n$ such that $\mathbf{g} \notin L_1$ and $k\mathbf{g} \in L_1$. Let $m_2 = km_1$. We have $m_2\mathbf{g} = km_1\mathbf{g} \in L_\rho$ and there exists a $c \in \mathcal{F}^*$ such that $\mathbb{Y}^{m_2\mathbf{g}} - c^{m_2} \in \mathcal{I}(\rho)$. Hence, $(x - o_{m_2})\mathbf{g} \in L_\rho \subset L_1$ and there exists a $d \in \mathcal{F}^*$, such that $\mathbb{Y}^{(x-o_{m_2})\mathbf{g}} - d \in \mathcal{I}(\rho)$. Let $L_2 = (L_1, \mathbf{g})$ and $\mathcal{I}_{l_1,l_2} = [\mathcal{I}_{l_1}, \mathbb{Y}^{\mathbf{g}} - c\zeta_{m_2}^{l_2}]$, $l_2 = 0, \ldots, m_2 - 1$. Then $L_1 \subsetneq L_2$ and L_2 is the support lattice for all $\mathcal{I}_{l_1,l_2}$ provided $\mathcal{I}_{l_1,l_2} \neq [1]$. Similar to the above, it can be shown that $d - c^{x-o_{m_2}} \in \mathcal{I}_{l_1,l_2}$ for any l_1, l_2. If $d - c^{x-o_{m_2}} \neq 0$, then $\mathcal{I}_{l_1,l_2} = [1]$ for any l_1, l_2 and $\langle\mathcal{I}_{l_1}\rangle = [1]$ by Lemma 52. Since Laurent binomial σ-ideals are radical, $\langle\mathcal{I}(\rho)\rangle = \cap_{l_1=0}^{m_1-1}\langle\mathcal{I}_{l_1}\rangle = [1]$ by Lemma 47 and (28). If $d - c^{x-o_{m_2}} = 0$, it can be similarly proved that $\mathcal{I}_{l_1} = \cap_{l_2=0}^{m_2-1}\mathcal{I}_{l_1,l_2}$ for any l_1. As a consequence, we have either $\langle\mathcal{I}(\rho)\rangle = [1]$ or $\mathcal{I}(\rho) = \cap_{l_1=0}^{m_1-1}\mathcal{I}_{l_1} = \cap_{l_1=0}^{m_1-1}\cap_{l_2=0}^{m_2-1}\mathcal{I}_{l_1,l_2}$.

Repeating the process, we have either $\langle\mathcal{I}(\rho)\rangle = [1]$ or

$$\mathcal{I}(\rho) = \cap_{l_1=0}^{m_1-1}\mathcal{I}_{l_1} = \cdots = \cap_{l_1=0}^{m_1-1}\cdots\cap_{l_t=0}^{m_t-1}\mathcal{I}_{l_1,\ldots,l_t} \tag{29}$$

where $L_\rho \subsetneq L_1 \subsetneq \cdots \subsetneq L_t \subset \mathrm{sat}_{\mathbb{Z}}(L_\rho)$. Since $\mathbb{Z}[x]^n$ is Noetherian, the procedure will end and L_t is $\mathbb{Z}$-saturated for some t. Since each $\mathcal{I}_{l_1,\ldots,l_t}$ is either $[1]$ or a prime σ-ideal, and hence either $\langle\mathcal{I}(\rho)\rangle = [1]$ or $\mathcal{I}(\rho)$ is well-mixed. If $\mathcal{I}(\rho)$ is proper, from (29), $\mathcal{I}(\rho)$ is the intersection of Laurent prime binomial σ-ideals with support lattice $\mathrm{sat}_{\mathbb{Z}}(L_\rho)$. □

Example 57. We use this example to show that $\langle\mathcal{I}(\rho)\rangle = [1]$ can indeed happen in Theorem 56. Let $\mathcal{I} = [\mathcal{A}_1]$, where $\mathcal{A}_1$ is from (12). The support lattice of $\mathcal{I}$ is M-saturated. We have $(y_1^{-1}y_2)^2 - 1 = y_1^{-2}(y_2^2+1) - y_1^{-2}(y_1^2+1) \in \mathcal{I}$. Then by Corollary 53, $(y_1^{-1}y_2)^{x-1} - 1 \in \langle\mathcal{I}\rangle$. Since $y_1^{x-1} - 1$ and $y_2^{x-1} + 1$ are in $\mathcal{I}$, we have $1 \in \langle\mathcal{I}\rangle$.

Theorem 58. *Let $\mathcal{F}$ be an algebraically closed σ-field and $\mathcal{I} = \mathcal{I}(\rho)$ a Laurent binomial σ-ideal. Then $\langle\mathcal{I}\rangle$ is either* [1] *or a Laurent binomial σ-ideal whose support lattice is $\mathrm{sat}_M(L_\rho)$. If $\langle\mathcal{I}\rangle \neq [1]$, then $\langle\mathcal{I}\rangle$ can be written as the intersection of Laurent prime binomial σ-ideals with support lattice $\mathrm{sat}_{\mathbb{Z}}(L_\rho)$.*

Proof. Suppose that $\langle\mathcal{I}(\rho)\rangle \neq [1]$. If L is not M-saturated, then there exists an $m \in \mathbb{N}$ and $\mathbf{f} \in \mathbb{Z}[x]^n$ such that $\mathbf{f} \notin L$, $m\mathbf{f} \in L$, and $(x - o_m)\mathbf{f} \notin L$. By Lemma 32, there exists a $c \in \mathcal{F}^*$ such that $\mathbb{Y}^{m\mathbf{f}} - c^m \in \mathcal{I}(\rho)$. Let $\mathcal{I}_1 = [\mathcal{I}, \mathbb{Y}^{(x-o_m)\mathbf{f}} - c^{x-o_m}]$ and $L_1 = (L, (x - o_m)\mathbf{f})$. By Corollary 53, $\mathbb{Y}^{(x-o_m)\mathbf{f}} - c^{x-o_m} \in \langle\mathcal{I}(\rho)\rangle$. Let $L_M = \mathrm{sat}_M(L)$. Then $\mathcal{I} \subsetneq \mathcal{I}_1 \subset \langle\mathcal{I}\rangle$ and $L \subsetneq L_1 \subset L_M$. Repeat the procedure to construct I_i and L_i for $i = 2, \ldots, t$ such that $\mathcal{I} \subsetneq \mathcal{I}_1 \subsetneq \cdots \subsetneq \mathcal{I}_t \subset \{\mathcal{I}\}$ and $L \subsetneq L_1 \subsetneq \cdots \subsetneq L_t \subset L_M$. Since $\mathbb{Z}[x]^n$ is Noetherian, the procedure will terminate at, say t. Then $L_t = L_M$ is M-saturated for some t. By Lemma 62, L_t is also x-saturated. By Theorem 56, $\mathcal{I}_t \subset \langle\mathcal{I}\rangle$ is well-mixed and hence $\mathcal{I}_t = \langle\mathcal{I}\rangle$.

If $\langle\mathcal{I}\rangle \neq [1]$, by Theorem 56, $\langle\mathcal{I}\rangle$ can be written as the intersection of Laurent prime binomial σ-ideals with support lattice $\mathrm{sat}_{\mathbb{Z}}(\mathrm{sat}_M(L_\rho))$. It is easy to show that $\mathrm{sat}_{\mathbb{Z}}(\mathrm{sat}_M(L_\rho)) = \mathrm{sat}_{\mathbb{Z}}(L_\rho)$. □

By the proof of Theorem 58, we have

Corollary 59. *A $\mathbb{Z}[x]$-lattice and its M-saturation have the same rank.*

Example 60. Let $p = y_2^2 - y_1^2$. Following the proof of Theorem 58, it can be shown that $\langle p\rangle = \{p\} = [y_1^{-2}y_2^2 - 1, y_1^{1-x}y_2^{x-1} - 1] = [y_2^2 - y_1^2, y_1y_2^x - y_1^x y_2]$ in $\mathbb{K}\{\mathbb{Y}^{\pm}\}$.

In the rest of this section, we prove similar results for the perfect Laurent binomial σ-ideals. We first give a definition.

Definition 61. If a $\mathbb{Z}[x]$-lattice is both x-saturated and M-saturated, then it is called P-*saturated*. For any $\mathbb{Z}[x]$-lattice L, the smallest P-saturated $\mathbb{Z}[x]$-lattice containing L is called the P-saturation of L and is denoted by $\mathrm{sat}_P(L)$.

Lemma 62. *For any $\mathbb{Z}[x]$-lattice L, $\mathrm{sat}_P(L) = \mathrm{sat}_x(\mathrm{sat}_M(L)) = \mathrm{sat}_M(\mathrm{sat}_x(L))$.*

Proof. Let $L_1 = \mathrm{sat}_x(\mathrm{sat}_M(L))$ and $L_2 = \mathrm{sat}_M(\mathrm{sat}_x(L))$. It suffices to show $L_1 = L_2$. We claim that L_1 is P-saturated. Let $m\mathbf{f} \in L_1$ for $m \in \mathbb{N}$. Then $mx^a\mathbf{f} \in \mathrm{sat}_M(L)$ for some $a \in \mathbb{N}$, which implies $(x - o_m)x^a\mathbf{f} \in L \subset \mathrm{sat}_x(\mathrm{sat}_M(L)) = L_1$. Since L_1 is x-saturated, $(x - o_m)\mathbf{f} \in L_1$ and the claim is proved. Since $L \subset \mathrm{sat}_M(L)$, $\mathrm{sat}_x(L) \subset \mathrm{sat}_x(\mathrm{sat}_M(L)) = L_1$. From the claim, L_1 is P-saturated and hence $L_2 \subset \mathrm{sat}_M(L_1) = L_1$.

For the other direction, we claim that L_2 is x-saturated. Let $x\mathbf{f} \in \mathrm{sat}_M(\mathrm{sat}_x(L)) \subset \mathrm{sat}_{\mathbb{Z}}(\mathrm{sat}_x(L))$. Then there exists an $m \in \mathbb{N}$, such that $m\mathbf{f} \in \mathrm{sat}_x(L)$ which implies $(x - o_m)\mathbf{f} \in \mathrm{sat}_M(\mathrm{sat}_x(L))$ and hence $o_m\mathbf{f} = x\mathbf{f} - (x - o_m)\mathbf{f} \in \mathrm{sat}_M(\mathrm{sat}_x(L))$ follows. By Lemma 48, $\gcd(o_m, m) = 1$. Then $\mathbf{f} \in \mathrm{sat}_M(\mathrm{sat}_x(L))$, and the claim is true. Since $\mathrm{sat}_M(L) \subset \mathrm{sat}_M(\mathrm{sat}_x(L)) = L_2 = \mathrm{sat}_x(\mathrm{sat}_M(\mathrm{sat}_x(L)))$, we have $L_1 \subset L_2$. □

It is easy to check that a σ-ideal $\mathcal{I}$ is perfect if and only if $\mathcal{I}$ is reflexive, radical, and well-mixed. Since a Laurent binomial σ-ideal $\mathcal{I}$ is always radical, $\mathcal{I}$ is perfect if and only if $\mathcal{I}$ is reflexive and well-mixed. From this observation, we can deduce the following result about perfect Laurent binomial σ-ideals.

Theorem 63. *Let ρ be a partial character and $\mathcal{F}$ an algebraically closed and inversive σ-field. If $\mathcal{I}(\rho)$ is perfect, then L_ρ is* P*-saturated; conversely, if L_ρ is* P*-saturated, then either $\{\mathcal{I}(\rho)\} = [1]$ or $\mathcal{I}(\rho)$ is perfect. Furthermore, for any ρ, $\{\mathcal{I}(\rho)\}$ is either* [1] *or a Laurent binomial σ-ideal whose support lattice is $\mathrm{sat}_P(L_\rho)$.*

Proof. If $\mathcal{I}(\rho)$ is perfect, then it is well-mixed and reflexive. By Theorems 56 and Theorem 37, L_ρ is M-saturated and x-saturated, and hence P-saturated. Conversely, if L_ρ is P-saturated, it is M-saturated and x-saturated. By Theorem 56, either $\langle\mathcal{I}(\rho)\rangle = [1]$ or $\mathcal{I}(\rho)$ is well-mixed. If $\langle\mathcal{I}(\rho)\rangle = [1]$, $\{\mathcal{I}(\rho)\} = [1]$. Otherwise, by Theorem 37, $\mathcal{I}(\rho)$ is reflexive. By Corollary 25, $\mathcal{I}(\rho)$ is radical. Then $\mathcal{I}(\rho)$ is perfect and the first statement of the theorem is proved.

Let $\mathcal{I}_x$ be the reflexive closure of $\mathcal{I}(\rho)$. By Theorem 40, $\mathbb{L}(\mathcal{I}_x) = \mathrm{sat}_x(L_\rho)$. Let $\mathcal{I}_P = \langle\mathcal{I}_x\rangle$. By Theorem 58, $\mathcal{I}_P$ is either [1] or a Laurent binomial σ-ideal with support lattice $\mathrm{sat}_M(\mathrm{sat}_x(L_\rho))$ which is $\mathrm{sat}_P(L_\rho)$ by Lemma 62. Then $\mathcal{I}_P = \{\mathcal{I}(\rho)\}$, since $\mathcal{I}_P$ is both reflexive and well-mixed. The last statement of the theorem is proved. □

6. Binomial σ-ideal

6.1. Basic properties of binomial σ-ideal

In this section, it is shown that certain results from Eisenbud and Sturmfels (1996) can be extended to the difference case using the theory of infinite Gröbner bases.

A σ-*binomial* in $\mathbb{Y}$ is a σ-polynomial with at most two terms, that is, $a\mathbb{Y}^{\mathbf{a}} + b\mathbb{Y}^{\mathbf{b}}$ where $a, b \in \mathcal{F}$ and $\mathbf{a}, \mathbf{b} \in \mathbb{N}[x]^n$. For $\mathbf{f} \in \mathbb{Z}[x]^n$, let $\mathbf{f}^+, \mathbf{f}^- \in \mathbb{N}^n[x]$ denote the positive part and the negative part of $\mathbf{f}$ such that $\mathbf{f} = \mathbf{f}^+ - \mathbf{f}^-$. Consider a σ-binomial $f = a\mathbb{Y}^{\mathbf{a}} + b\mathbb{Y}^{\mathbf{b}}$, where $a, b \in \mathcal{F}^*$. Without loss of generality, assume $\mathbf{a} > \mathbf{b}$ according to the order defined in Section 3. Then f has the following canonical representation

$$f = a\mathbb{Y}^{\mathbf{a}} + b\mathbb{Y}^{\mathbf{b}} = a\mathbb{Y}^{\mathbf{g}}(\mathbb{Y}^{\mathbf{f}+} - c\mathbb{Y}^{\mathbf{f}^-}) \tag{30}$$

where $c = \frac{-b}{a}$, $\mathbf{f} = \mathbf{a} - \mathbf{b} \in \mathbb{Z}[x]^n$ is a normal vector, and $\mathbf{g} = \mathbf{a} - \mathbf{f}^+ \in \mathbb{N}[x]$. The normal vector $\mathbf{f}$ is called the *support* of f. Note that $\gcd(\mathbb{Y}^{\mathbf{f}^+}, \mathbb{Y}^{\mathbf{f}^-}) = 1$.

A σ-ideal in $\mathcal{F}\{\mathbb{Y}\}$ is called *binomial* if it is generated by, possibly infinitely many, σ-binomials.

In this section, $\mathcal{F}\{\mathbb{Y}\}$ is considered as a polynomial ring in infinitely many algebraic variables $\Theta(\mathbb{Y}) = \{y_i^{x^j}, i = 1, \ldots, n; j \geq 0\}$ and denoted by $S = \mathcal{F}[\Theta(\mathbb{Y})]$. A theory of Gröbner bases in the case of infinitely many variables is developed in Iima and Yoshino (2009) and will be used in this section. For any $m \in \mathbb{N}$, denote $\Theta^{\langle m \rangle}(\mathbb{Y}) = \{y_i^{x^j}, i = 1, \ldots, n; j = 0, 1, \ldots, m\}$ and $S^{\langle m \rangle} = \mathcal{F}[\Theta^{\langle m \rangle}(\mathbb{Y})]$ is a polynomial ring in finitely many variables.

A monomial order in S is called *compatible* with the difference structure, if $y_i^{x^{k_1}} < y_i^{x^{k_2}}$ for $k_1 < k_2$. Only compatible monomial orders are considered in this section.

Let $\mathcal{I}$ be a σ-ideal in $\mathcal{F}\{\mathbb{Y}\}$. Then $\mathcal{I}$ is an algebraic ideal in S. By Iima and Yoshino (2009), we have

Lemma 64. *Let $\mathcal{I}$ be a binomial σ-ideal in $\mathcal{F}\{\mathbb{Y}\}$. Then for a compatible monomial order, the reduced Gröbner basis $\mathbb{G}$ of $\mathcal{I}$ exists and satisfies*

$$\mathbb{G} = \cup_{m=0}^{\infty} \mathbb{G}^{\langle m \rangle} \tag{31}$$

where $\mathbb{G}^{\langle m \rangle} = \mathbb{G} \cap S^{\langle m \rangle}$ is the reduced Gröbner basis of $\mathcal{I}^{\langle m \rangle} = \mathcal{I} \cap S^{\langle m \rangle}$ in $S^{\langle m \rangle}$.

Contrary to the Laurent case, a binomial σ-ideal may be infinitely generated, as shown by the following example.

Example 65. Let $\mathcal{I} = [y_1^{x^i} y_2^{x^j} - y_1^{x^j} y_2^{x^i} : 0 \leq i < j \in \mathbb{N}]$. It is clear that $\mathcal{I}$ does not have a finite set of generators and hence a finite Gröbner basis. The reduced Gröbner basis of

$$\mathcal{I}^{\langle m \rangle} = \mathcal{I} \cap \mathbb{Q}[y_1, y_2; y_1^x, y_2^x; \ldots; y_1^{x^m}, y_2^{x^m}]$$

is $\{y_1^{x^i} y_2^{x^j} - y_1^{x^j} y_2^{x^i} : 0 \leq i < j \leq m\}$ with a monomial order satisfying $y_1 < y_2 < y_1^x < y_2^x < \cdots < y_1^{x^j} < y_2^{x^m}$. Then $\{y_1^{x^i} y_2^{x^j} - y_1^{x^j} y_2^{x^i} : 0 \leq i < j \in \mathbb{N}\}$ is an infinite reduced Gröbner basis for $\mathcal{I}$ in the sense of Iima and Yoshino (2009) when $y_1^{x^m}$ and $y_2^{x^m}$ are treated as independent algebraic variables.

Remark 66. The above concept of Gröbner basis does not consider the difference structure. The concept may be refined by introducing the reduced *σ-Gröbner basis* (Gerdt and Robertz, 2012). A σ-monomial M_1 is called *reduced* w.r.t. another σ-monomial M_2 if there do not exist a σ-monomial M_0 and a $k \in \mathbb{N}$ such that $M_1 = M_0 M_2^{x^k}$. Then the reduced σ-Gröbner basis of $\mathcal{I}$ in Example 65 is $\{y_1 y_2^{x^i} - y_1^{x^i} y_2 : i \in \mathbb{Z}_{\geq 1}\}$ which is still infinite. Since the purpose of Gröbner bases in this paper is theoretic and not computational, we will use the version of infinite Gröbner bases in the sense of Iima and Yoshino (2009).

With Lemma 64, a large portion of the properties for algebraic binomial ideals proved by Eisenbud and Sturmfels (1996) can be extended to the difference case. The proofs follow the same pattern: to prove a property for $\mathcal{I}$, we first show that the property is valid for $\mathcal{I}$ if and only if it is valid for all $\mathcal{I}^{\langle m \rangle}$, and then the corresponding statement from Eisenbud and Sturmfels (1996) will be used to show that the property is indeed valid for $\mathcal{I}^{\langle m \rangle}$. We will illustrate the procedure in the following corollary. For other results, we omit the proofs. By a *σ-term*, we mean the multiplication of an element from $\mathcal{F}^*$ and a σ-monomial.

Corollary 67. *Let $\mathcal{I} \subset \mathcal{F}\{\mathbb{Y}\}$ be a binomial σ-ideal. Then the reduced Gröbner basis $\mathbb{G}$ of $\mathcal{I}$ consists of σ-binomials and the normal form of any σ-term modulo $\mathbb{G}$ is again a σ-term.*

Proof. By (31), it suffices to show that corollary is valid for all $\mathbb{G}^{\langle m \rangle}$, that is, the reduced Gröbner basis $\mathbb{G}^{\langle m \rangle}$ of $\mathcal{I}^{\langle m \rangle}$ consists of binomials and the normal form of any term modulo $\mathbb{G}^{\langle m \rangle}$ is again a

term. Since $\mathbb{G}^{\langle m\rangle}$ is the Gröbner basis of $\mathcal{I}^{\langle m\rangle} = \mathcal{I} \cap S^{\langle m\rangle}$ and $\mathcal{I}^{\langle m\rangle}$ is a binomial ideal in a polynomial ring with finitely many variables, the corollary follows from Proposition 1.1 in Eisenbud and Sturmfels (1996). □

Corollary 68. *A σ-ideal $\mathcal{I}$ is binomial if and only if the reduced Gröbner basis for $\mathcal{I}$ consists of σ-binomials.*

Corollary 69. *If $\mathcal{I}$ is a binomial σ-ideal, then the elimination ideal $\mathcal{I} \cap \mathcal{F}\{y_1, y_2, \ldots, y_r\}$ is binomial for every $r \leq n$.*

The following lemma can be proved similar to its algebraic counterpart.

Lemma 70. *If $\mathcal{I}$ and $\mathcal{J}$ are binomial σ-ideals in $\mathcal{F}\{\mathbb{Y}\}$ then we have $\mathcal{I} \cap \mathcal{J} = [t\mathcal{I} + (1-t)\mathcal{J}] \cap \mathcal{F}\{\mathbb{Y}\}$ where t is a new σ-indeterminate.*

The intersection of binomial σ-ideals is not binomial in general, but from Lemma 70 and Eisenbud and Sturmfels (1996) we have

Corollary 71. *If $\mathcal{I}$ and $\mathcal{I}'$ are binomial σ-ideals and $\mathcal{J}_1, \ldots, \mathcal{J}_s$ are σ-ideals generated by σ-monomials, then $[\mathcal{I} + \mathcal{I}'] \cap [\mathcal{I} + \mathcal{J}_1] \cap \ldots \cap [\mathcal{I} + \mathcal{J}_s]$ is binomial.*

Corollary 72. *Let $\mathcal{I}$ be a binomial σ-ideal and let $\mathcal{J}_1, \ldots, \mathcal{J}_s$ be monomial σ-ideals.*
(a) The intersection $[\mathcal{I} + \mathcal{J}_1] \cap \cdots \cap [\mathcal{I} + \mathcal{J}_s]$ is generated by σ-monomials modulo $\mathcal{I}$.
(b) Any σ-monomial in the sum $\mathcal{I} + \mathcal{J}_1 + \cdots + \mathcal{J}_s$ lies in one of the σ-ideals $\mathcal{I} + \mathcal{J}_i$.

Corollary 73. *If $\mathcal{I}$ is a binomial σ-ideal, then for any σ-monomial M, the σ-ideal quotients $[\mathcal{I} : M]$ and $[\mathcal{I} : M^\infty]$ are binomial.*

Corollary 74. *Let $\mathcal{I}$ be a binomial σ-ideal and $\mathcal{J}$ a monomial σ-ideal. If $f \in \mathcal{I} + \mathcal{J}$ and g is the sum of those terms of f that are not individually contained in $\mathcal{I} + \mathcal{J}$, then $g \in \mathcal{J}$.*

From Eisenbud and Sturmfels (1996, Theorem 3.1), we have

Theorem 75. *If $\mathcal{I}$ is a binomial σ-ideal, then the radical of $\mathcal{I}$ is binomial.*

Finally, we consider the reflexive closure of binomial σ-ideals.

Lemma 76. *A binomial σ-ideal $\mathcal{I}$ is reflexive if and only if $b^x \in \mathcal{I} \Rightarrow b \in \mathcal{I}$ for any σ-binomial $b \in \mathcal{F}\{\mathbb{Y}\}$.*

Proof. It suffices to prove one side of the statement, that is, if $b^x \in \mathcal{I} \Rightarrow b \in \mathcal{I}$ for any σ-binomial b then $\mathcal{I}$ is reflexive. Let p be a σ-polynomial such that $p^x \in \mathcal{I}$. Let $\mathbb{G}$ be the infinite reduced Gröbner basis of $\mathcal{I}$ in S under any variable order satisfying $y_i^{x^j} < y_k$ for any $i, k, j > 0$. It is easy to see that $\mathbb{G}$ consists of binomials. p^x can be reduced to zero by $\mathbb{G}$. Due to the chosen variable order, we have $p^x = \sum_i e_i^x g_i^x$, where $e_i^x \in S$ and g_i^x is a binomial in S. Since g_i^x are σ-binomials in $\mathcal{I}$, we have $g_i \in \mathcal{I}$. Then, $p = \sum_i e_i g_i \in \mathcal{I}$ and $\mathcal{I}$ is reflexive. □

Theorem 77. *If $\mathcal{I}$ is a binomial σ-ideal, then the reflexive closure of $\mathcal{I}$ is binomial.*

Proof. Let $\mathcal{I}_1$ be the σ-ideal generated by the σ-binomials $p \in \mathcal{F}\{\mathbb{Y}\}$ such that $p^{x^k} \in \mathcal{I}$ for a $k \in \mathbb{N}$. We claim that $\mathcal{I}_1$ is the reflexive closure of $\mathcal{I}$ and it suffices to show that $\mathcal{I}_1$ is reflexive. Let p be a σ-binomial such that $p^x \in \mathcal{I}_1$. Then for some $s \in \mathbb{N}$, $(p^x)^{x^s} = p^{x^{s+1}} \in \mathcal{I}$. Thus $p \in \mathcal{I}_1$ and $\mathcal{I}_1$ is reflexive by Lemma 76. □

6.2. Normal binomial σ-ideal

In this section, most of the results about Laurent binomial σ-ideals proved in Sections 4 and 5 will be extended to normal binomial σ-ideals.

Let $\mathbb{m}$ be the multiplicative set generated by $y_i^{x^j}$ for $i = 1, \ldots, n$, $j \in \mathbb{N}$.

Definition 78. A σ-ideal $\mathcal{I}$ is called *normal* if for $M \in \mathbb{m}$ and $p \in \mathcal{F}\{\mathbb{Y}\}$, $Mp \in \mathcal{I}$ implies $p \in \mathcal{I}$.

For any σ-ideal $\mathcal{I}$,

$$\mathcal{I} : \mathbb{m} = \{f \in \mathcal{F}\{\mathbb{Y}\} \mid \exists M \in \mathbb{m} \text{ s.t. } Mf \in \mathcal{I}\}$$

is a normal σ-ideal. For any σ-ideal $\mathcal{I}$ in $\mathcal{F}\{\mathbb{Y}\}$, it is easy to check that

$$\mathcal{F}\{\mathbb{Y}^{\pm}\}\mathcal{I} \cap \mathcal{F}\{\mathbb{Y}\} = \mathcal{I} : \mathbb{m}. \tag{32}$$

We first prove a property for general normal σ-ideals.

Lemma 79. *A normal σ-ideal $\mathcal{I}$ in $\mathcal{F}\{\mathbb{Y}\}$ is reflexive (radical, well-mixed, perfect, prime) if and only if $\mathcal{F}\{\mathbb{Y}^{\pm}\}\mathcal{I}$ is reflexive (radical, well-mixed, perfect, prime) in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$.*

Proof. Let $\overline{\mathcal{I}} = \mathcal{F}\{\mathbb{Y}^{\pm}\}\mathcal{I}$ be a Laurent σ-ideal. Since $\mathcal{I}$ is normal, from (32) we have $\overline{\mathcal{I}} \cap \mathcal{F}\{\mathbb{Y}\} = \mathcal{I}$. If $\overline{\mathcal{I}}$ is reflexive, it is clear that $\mathcal{I}$ is reflexive. For the other direction, if $f^x \in \overline{\mathcal{I}}$, then by clearing denominators of f^x, there exists a σ-monomial M^x in $\mathbb{Y}$ such that $M^x f^x \in \overline{\mathcal{I}} \cap \mathcal{F}\{\mathbb{Y}\} = \mathcal{I}$. Since $\mathcal{I}$ is reflexive, $Mf \in \mathcal{I}$ and hence $f \in \overline{\mathcal{I}}$, that is, $\overline{\mathcal{I}}$ is reflexive. The results about radical and perfect σ-ideals can be proved similarly.

We now show that $\mathcal{I}$ is prime if and only if $\overline{\mathcal{I}}$ is prime. If $\overline{\mathcal{I}}$ is prime, it is clear that $\mathcal{I}$ is also prime. For the other side, let $fg \in \overline{\mathcal{I}}$. Then there exist σ-monomials N_1, N_2 such that $N_1 f \in \mathcal{F}\{\mathbb{Y}\}$, $N_2 g \in \mathcal{F}\{\mathbb{Y}\}$, and hence $N_1 f N_2 g \in \mathcal{I}$. Since $\mathcal{I}$ is prime, $N_1 f$ or $N_2 g$ is in $\mathcal{I}$ that is f or g is in $\overline{\mathcal{I}}$. The result about well-mixed σ-ideals can be proved similarly. □

Given a partial character ρ on $\mathbb{Z}[x]^n$, we define the following binomial σ-ideal in $\mathcal{F}\{\mathbb{Y}\}$

$$\mathcal{I}^+(\rho) = [\mathbb{Y}^{\mathbf{f}^+} - \rho(\mathbf{f})\mathbb{Y}^{\mathbf{f}^-} \mid \mathbf{f} \in L_\rho]. \tag{33}$$

We will show that any normal binomial σ-ideal can be written as the form (33).

Lemma 80. *Let ρ be a partial character on $\mathbb{Z}[x]^n$ and $\mathcal{I}(\rho)$ defined in (20). Then $\mathcal{I}^+(\rho) = \mathcal{I}(\rho) \cap \mathcal{F}\{\mathbb{Y}\}$. As a consequence, $\mathcal{I}^+(\rho)$ is proper and normal.*

Proof. It is clear that $\mathcal{I}^+(\rho) \subset \mathcal{I}(\rho) \cap \mathcal{F}\{\mathbb{Y}\}$. If $f \in \mathcal{I}(\rho) \cap \mathcal{F}\{\mathbb{Y}\}$, then $f = \sum_{i=1}^{s} f_i M_i (\mathbb{Y}^{\mathbf{f}_i} - \rho(\mathbf{f}_i))$ where $f_i \in \mathcal{F}$, $\mathbf{f}_i \in L_\rho$, and M_i are Laurent σ-monomials in $\mathbb{Y}$. There exists a σ-monomial M in $\mathbb{Y}$ such that

$$Mf = \sum_{i=1}^{s} f_i N_i (\mathbb{Y}^{\mathbf{f}_i^+} - \rho(\mathbf{f}_i)\mathbb{Y}^{\mathbf{f}_i^-}) \in \mathcal{I}^+(\rho), \tag{34}$$

where N_i is a σ-monomial in $\mathbb{Y}$. We will prove $f \in \mathcal{I}^+(\rho)$ from the above equation. Without loss of generality, we may assume that $M = y_c^{x^o}$ for some c and $o \in \mathbb{N}$. Note that (34) is an algebraic identity in $y_i^{x^k}, i = 1, \ldots, n, k \in \mathbb{N}$. If N_i contains $y_c^{x^o}$ as a factor, we move $F_i = f_i N_i (\mathbb{Y}^{\mathbf{f}_i^+} - \rho(\mathbf{f}_i)\mathbb{Y}^{\mathbf{f}_i^-})$ to the left hand side of (34) and let $f_1 = f - F_i / y_c^{x^o}$. Then $f \in \mathcal{I}^+(\rho)$ if and only if $f_1 \in \mathcal{I}^+(\rho)$. Repeat the above procedure until no N_i contains $y_c^{x^o}$ as a factor.

If $s = 0$ in (34), then $f = 0$ and the lemma is proved. Since $\gcd(\mathbb{Y}^{\mathbf{f}_i^+}, \mathbb{Y}^{\mathbf{f}_i^-}) = 1$, $y_c^{x^o}$ cannot be a factor of both $\mathbb{Y}^{\mathbf{f}_i^+}$ and $\mathbb{Y}^{\mathbf{f}_i^-}$. Let $\mathbb{Y}^{\mathbf{f}_i^+}$ be the largest σ-monomial in (34) not divisible by $y_c^{x^o}$ under

a given σ-monomial total order . If $\mathbb{Y}^{\mathbf{f}_i^-}$ is the largest σ-monomial in (34) not divisible by $y_c^{x^o}$, the proving process is similar. There must exists another σ-binomial $f_j N_j(\mathbb{Y}^{\mathbf{f}_j^+} - \rho(\mathbf{f}_j)\mathbb{Y}^{\mathbf{f}_j^-})$ such that $N_i\mathbb{Y}^{\mathbf{f}_i^+} = N_j\mathbb{Y}^{\mathbf{f}_j^-}$. Let $N_i = \mathbb{Y}^{\mathfrak{p}_i}$, $N_j = \mathbb{Y}^{\mathfrak{p}_j}$. Then $\mathbb{Y}^{\mathbf{f}_i^+ + \mathfrak{p}_i} = \mathbb{Y}^{\mathbf{f}_j^- + \mathfrak{p}_j}$ and $\mathbf{f}_i^+ + \mathfrak{p}_i = \mathbf{f}_j^- + \mathfrak{p}_j$. We have

$$p = f_i N_i(\mathbb{Y}^{\mathbf{f}_i^+} - \rho(\mathbf{f}_i)\mathbb{Y}^{\mathbf{f}_i^-}) + f_j N_j(\mathbb{Y}^{\mathbf{f}_j^+} - \rho(\mathbf{f}_j)\mathbb{Y}^{\mathbf{f}_j^-})$$

$$= \frac{f_i}{\rho(\mathbf{f}_j)}(\mathbb{Y}^{\mathbf{f}_j^+ + \mathfrak{p}_j} - \rho(\mathbf{f}_i)\rho(\mathbf{f}_j)\mathbb{Y}^{\mathbf{f}_i^- + \mathfrak{p}_i}) + (f_j - \frac{f_i}{\rho(\mathbf{f}_j)})N_j(\mathbb{Y}^{\mathbf{f}_j^+} - \rho(\mathbf{f}_j)\mathbb{Y}^{\mathbf{f}_j^-}).$$

Since $\mathbf{f} = \mathbf{f}_j^+ + \mathfrak{p}_j - (\mathbf{f}_i^- + \mathfrak{p}_i) = \mathbf{f}_i^+ - \mathbf{f}_i^- + \mathbf{f}_j^+ - \mathbf{f}_j^- = \mathbf{f}_i + \mathbf{f}_j \in L_\rho$, we have $\mathbb{Y}^{\mathbf{f}_j^+ + \mathfrak{p}_j} - \rho(\mathbf{f}_i)\rho(\mathbf{f}_j)\mathbb{Y}^{\mathbf{f}_i^- + \mathfrak{p}_i} = N(\mathbb{Y}^{\mathbf{f}^+} - \rho(\mathbf{f})\mathbb{Y}^{\mathbf{f}^-}) \in \mathcal{I}^+(\rho)$, where N is a σ-monomial. As a consequence, $p \in \mathcal{I}^+(\rho)$. If N contains $y_c^{x^o}$, move the term $\frac{f_i}{\rho(\mathbf{f}_j)}N(\mathbb{Y}^{\mathbf{f}^+} - \rho(\mathbf{f})\mathbb{Y}^{\mathbf{f}^-})$ to the left hand side of (34) as we did in the first phase of the proof. After the above procedure, equation (34) is still valid. Furthermore, the number of σ-binomials in (34) does not increase, no N_i contains $y_c^{x^o}$, and the largest σ-monomial $\mathbb{Y}^{\mathbf{f}_i^+}$ or $\mathbb{Y}^{\mathbf{f}_i^-}$ not containing $y_c^{x^o}$ becomes smaller. The above procedure will stop after a finite number of steps, which means $s = 0$ in (34) and hence $y_c^{x^o} f = 0$ which means the original f is in $\mathcal{I}^+(\rho)$. Then $\mathcal{I}^+(\rho) = \mathcal{I}(\rho) \cap \mathcal{F}\{\mathbb{Y}\}$.

$\mathcal{I}^+(\rho) = \mathcal{I}(\rho) \cap \mathcal{F}\{\mathbb{Y}\}$ is proper. For otherwise $\mathcal{I}(\rho) = [1]$, contradicting to Lemma 31. Note that $\mathcal{I}^+(\rho)\mathcal{F}\{\mathbb{Y}^\pm\} = \mathcal{I}(\rho)$. Then $\mathcal{I}^+(\rho) = \mathcal{I}(\rho) \cap \mathcal{F}\{\mathbb{Y}\} = \mathcal{I}^+(\rho)\mathcal{F}\{\mathbb{Y}^\pm\} \cap \mathcal{F}\{\mathbb{Y}\} = \mathcal{I}^+(\rho) : \mathbb{m}$, and $\mathcal{I}^+(\rho)$ is normal. □

Lemma 81. *Let ρ be a partial character on $\mathbb{Z}[x]^n$. Then $\mathbb{Y}^{\mathbf{f}^+} - c\mathbb{Y}^{\mathbf{f}^-} \in \mathcal{I}^+(\rho)$ if and only if $\mathbf{f} \in L_\rho$ and $c = \rho(\mathbf{f})$.*

Proof. By Lemma 80, $\mathbb{Y}^{\mathbf{f}^+} - c\mathbb{Y}^{\mathbf{f}^-} \in \mathcal{I}^+(\rho)$ if and only if $\mathbb{Y}^{\mathbf{f}} - c \in \mathcal{I}(\rho)$ which is equivalent to $\mathbf{f} \in L_\rho$ and $c = \rho(\mathbf{f})$ by Lemma 32. □

Lemma 82. *If $\mathcal{I}$ is a normal binomial σ-ideal, then there exists a unique partial character ρ on $\mathbb{Z}[x]^n$ such that $\mathcal{I} = \mathcal{I}^+(\rho)$ and $L_\rho = \{\mathbf{f} \in \mathbb{Z}[x]^n \mid \mathbb{Y}^{\mathbf{f}^+} - \rho(\mathbf{f})\mathbb{Y}^{\mathbf{f}^-} \in \mathcal{I}\}$ which is called the* support lattice *of $\mathcal{I}$.*

Proof. We have $\mathcal{I} \cdot \mathcal{F}\{\mathbb{Y}^\pm\} \cap \mathcal{F}\{\mathbb{Y}\} = \mathcal{I} : \mathbb{m}$. By Theorem 33, there exists a partial character ρ such that $\mathcal{I} \cdot \mathcal{F}\{\mathbb{Y}^\pm\} = \mathcal{I}(\rho)$. Then by Lemma 80, $\mathcal{I} = (\mathcal{I} : \mathbb{m}) = \mathcal{I} \cdot \mathcal{F}\{\mathbb{Y}^\pm\} \cap \mathcal{F}\{\mathbb{Y}\} = \mathcal{I}(\rho) \cap \mathcal{F}\{\mathbb{Y}\} = \mathcal{I}^+(\rho)$. By Lemma 81, we have $L_\rho = \{\mathbf{f} \in \mathbb{Z}[x]^n \mid \mathbb{Y}^{\mathbf{f}^+} - \rho(\mathbf{f})\mathbb{Y}^{\mathbf{f}^-} \in \mathcal{I} = \mathcal{I}^+(\rho)\}$. The uniqueness of ρ comes from the fact that L_ρ is uniquely determined by $\mathcal{I}$. □

By Lemmas 80 and 82, we have

Theorem 83. *The map $\mathcal{I}(\rho) \Rightarrow \mathcal{I}^+(\rho)$ gives a one to one correspondence between Laurent binomial σ-ideals in $\mathcal{F}\{\mathbb{Y}^\pm\}$ and normal binomial σ-ideals in $\mathcal{F}\{\mathbb{Y}\}$.*

Due to Lemma 80 and Theorem 83, most properties of Laurent binomial σ-ideals can be extended to normal binomial σ-ideals. As a consequence of Corollary 25, Lemma 79, and Lemma 80, we have

Corollary 84. *A normal binomial σ-ideal is radical.*

As a directly consequence of Theorem 40, Lemma 79, and Theorem 83, we obtain

Corollary 85. *If $\mathcal{F}$ is inversive, then the reflexive closure of $\mathcal{I}^+(\rho)$ is also a normal binomial σ-ideal whose support lattice is the x-saturation of L_ρ.*

Corollary 86. *If $\mathcal{F}$ is algebraically closed and inversive, then*

(a) *L_ρ is $\mathbb{Z}$-saturated if and only if $\mathcal{I}^+(\rho)$ is prime;*
(b) *L_ρ is x-saturated if and only if $\mathcal{I}^+(\rho)$ is reflexive;*
(c) *L_ρ is saturated if and only if $\mathcal{I}^+(\rho)$ is reflexive prime.*

Proof. It is easy to show that $\mathcal{I}(\rho) = \mathcal{I}^+(\rho)\mathcal{F}\{\mathbb{Y}^{\pm}\}$. Then the corollary is a consequence of Theorem 37, Lemma 79, and Lemma 80. □

For properties related with perfect σ-ideals, it becomes more complicated. Direct extension of Theorems 42, and 63 to the normal binomial case is not correct as shown by the following example.

Example 87. Let $\mathcal{I} = [y_1^x - y_1, y_2^2 - y_1^2, y_2^x + y_2]$ which is a normal binomial σ-ideal whose representation matrix is $L = \begin{bmatrix} x-1 & -2 & 0 \\ 0 & 2 & x-1 \end{bmatrix}$. Since $o_2 = 1$, L is P-saturated. Also, $L_s = \mathrm{sat}(L) = \begin{bmatrix} x-1 & -1 \\ 0 & 1 \end{bmatrix}$. We have $\{\mathcal{I}\} = \{\mathcal{I}, y_2 - y_1\} \cap \{\mathcal{I}, y_2 + y_1\} = [y_1, y_2]$. Then $\{\mathcal{I}\} \neq [1]$ and $\mathcal{I}$ is not perfect and hence Theorems 63 are not correct. Theorem 42 is also not correct, since the supporting lattice of the prime component of $\mathcal{I}$ is not L_s. This example also shows that the perfect closure of a normal binomial σ-ideal is not necessarily normal.

It can be seen that the problem is due to the occurrence of σ-monomials. For any partial character ρ, it can be shown that

$$\{\mathcal{I}^+(\rho)\} : \mathbb{m} = \{\mathcal{I}(\rho)\} \cap \mathcal{F}\{\mathbb{Y}\}. \tag{35}$$

We thus have the following modifications for Theorems 63 and 42.

Corollary 88. *Let $\mathcal{F}$ be an inversive and algebraically closed σ-field. If $\mathcal{I}^+(\rho)$ is perfect, then L_ρ is P-saturated. Conversely, if L_ρ is P-saturated, then either $\{\mathcal{I}\} : \mathbb{m} = [1]$ or $\mathcal{I}$ is perfect. For any ρ, either $\{\mathcal{I}^+(\rho)\} : \mathbb{m} = [1]$ or $\{\mathcal{I}^+(\rho)\} : \mathbb{m}$ is a binomial σ-ideal whose support lattice is the P-saturation of L_ρ.*

Proof. If $\mathcal{I}$ is perfect, by Lemma 79, $\mathcal{I}(\rho) = \mathcal{I}\mathcal{F}\{\mathbb{Y}^{\pm}\}$ is also perfect. By Theorem 63, L_ρ is P-saturated. If L_ρ is P-saturated and x-saturated, by Theorem 63, either $\mathcal{I}(\rho) = [1]$ or $\mathcal{I}(\rho)$ is perfect. If $\mathcal{I}(\rho) = [1]$, by (35), $\{\mathcal{I}\} : \mathbb{m} = [1]$. If $\mathcal{I}(\rho)$ is perfect, by Lemma 79, $\mathcal{I} = \mathcal{I}^+(\rho)$ is also perfect. □

Similar results hold for normal well-mixed σ-ideals.

In the rest of this section, we give decomposition theorems for perfect binomial σ-ideals. We first consider normal binomial σ-ideals. By Corollary 84 and Example 57, a normal binomial σ-ideal is radical but may not be perfect.

Theorem 89. *Let $\mathcal{I} = \mathcal{I}^+(\rho)$ be a normal binomial σ-ideal and $\mathcal{F}$ an inversive and algebraically closed σ-field. Then $\{\mathcal{I}\} : \mathbb{m}$ is either $[1]$ or can be written as the intersection of reflexive prime binomial σ-ideals whose support lattice is the saturation lattice of L_ρ.*

Proof. By Theorem 42, either $\{\mathcal{I}(\rho)\} = [1]$ or $\{\mathcal{I}(\rho)\} = \bigcap_{i=1}^s \mathcal{I}(\rho_i)$, where $\mathcal{I}(\rho_i)$ are reflexive prime Laurent binomial σ-ideals whose support lattices are $\mathrm{sat}(L_\rho)$. By (35) and Lemma 80, either $\{\mathcal{I}^+(\rho)\} : \mathbb{m} = [1]$ or $\{\mathcal{I}^+(\rho)\} : \mathbb{m} = \{\mathcal{I}(\rho)\} \cap \mathcal{F}\{\mathbb{Y}\} = (\bigcap_{i=1}^s \mathcal{I}(\rho_i)) \cap \mathcal{F}\{\mathbb{Y}\} = \bigcap_{i=1}^s (\mathcal{I}(\rho_i) \cap \mathcal{F}\{\mathbb{Y}\}) = \bigcap_{i=1}^s \mathcal{I}^+(\rho_i)$. By Corollary 86, $\mathcal{I}^+(\rho_i)$ is reflexive and prime whose support lattices are the saturation of L_ρ. □

Now, consider general binomial σ-ideals.

Lemma 90. *$\mathcal{I} \subset \mathcal{F}\{\mathbb{Y}\}$ is a reflexive prime binomial σ-ideal if and only if $\mathcal{I} = [y_{i_1}, \ldots, y_{i_s}] + \mathcal{I}_1$, where $\{y_{i_1}, \ldots, y_{i_s}\} = \mathbb{Y} \cap \mathcal{I}$, $\{z_1, \ldots, z_t\} = \mathbb{Y} \backslash \mathcal{I}$, and $\mathcal{I}_1$ is a normal binomial reflexive prime σ-ideal in $\mathcal{F}\{z_1, \ldots, z_t\}$.*

Proof. If $\mathcal{I}$ is reflexive and prime, then $(y_i^{x^j})^d \in \mathcal{I}$ if and only if $y_i \in \mathcal{I}$. Let $\mathcal{I}_1 = \mathcal{I} \cap \mathcal{F}\{z_1, \ldots, z_t\}$. Then $\mathcal{I} = [y_{i_1}, \ldots, y_{i_s}] + \mathcal{I}_1$. $\mathcal{I}_1$ is clearly reflexive and prime. We still need to show that $\mathcal{I}_1$ is normal. Let $Nf \in \mathcal{I}_1$ for a σ-monomial N in $\{z_1, \ldots, z_t\}$ and $f \in \mathcal{F}\{z_1, \ldots, z_t\}$. N cannot be in $\mathcal{I}_1$. Otherwise, some z_i is in $\mathcal{I}_1$ since $\mathcal{I}_1$ is reflexive and prime, which contradicts to $\{z_1, \ldots, z_t\} = \mathbb{Y} \backslash \mathcal{I}$. Therefore, $f \in \mathcal{I}_1$ and $\mathcal{I}_1$ is normal. The other direction is trivial. □

The σ-ideal $\mathcal{I}$ in Lemma 90 is said to be *quasi-normal*. The following result can be proved similarly to Theorem 42.

Theorem 91. *Let $\mathcal{I}$ be a binomial σ-ideal. If $\mathcal{F}$ is algebraically closed and inversive, then the perfect σ-ideal $\{\mathcal{I}\}$ is either* [1] *or the intersection of quasi-normal reflexive prime binomial σ-ideals.*

Proof. We prove the theorem by induction on n. Let $\mathcal{I}_1 = \{\mathcal{I}\} : \mathbb{m}$. Then $\{\mathcal{I}\} = \mathcal{I}_1 \cap \cap_{i=1}^n \{\mathcal{I}, y_i\}$. It is easy to check $\mathcal{I}_1 = \{\mathcal{I} : \mathbb{m}\} : \mathbb{m}$. Since $\mathcal{I} : \mathbb{m}$ is normal, by Theorem 89, $\mathcal{I}_1$ is either [1] or intersection of normal reflexive prime σ-ideals. If $n = 1$, then $\{\mathcal{I}, y_i\}$ must be either $[y_1]$ or [1]. Then the theorem is proved for $n = 1$. Suppose the theorem is valid for $n = 1, \ldots, k-1$. Still use $\{\mathcal{I}\} = \mathcal{I}_1 \cap \cap_{i=1}^n \{\mathcal{I}, y_i\}$. Let $\mathcal{I}_i$ be the σ-ideal obtained by setting y_i to 0 in $\mathcal{I}$. By the induction hypothesis, $\mathcal{I}_i$ can be written as intersection of quasi-normal reflexive prime σ-ideals in $\mathcal{F}\{\mathbb{Y} \setminus \{y_i\}\}$. So the theorem is also valid for $\{\mathcal{I}, y_i\} = \{\mathcal{I}_i, y_i\}$. The theorem is proved. □

6.3. Characteristic set for normal binomial σ-ideal

The theory of characteristic set given in Section 4.2 will be extended to the normal σ-binomial case.

Let ρ be a partial character on $\mathbb{Z}[x]^n$, $L_\rho = (\mathbf{f}_1, \ldots, \mathbf{f}_s)$ where $\mathbb{f} = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$ is a reduced Gröbner basis, and

$$\mathcal{A}^+(\rho) : \mathbb{Y}^{\mathbf{f}_1^+} - \rho(\mathbf{f}_1)\mathbb{Y}^{\mathbf{f}_1^-}, \ldots, \mathbb{Y}^{\mathbf{f}_s^+} - \rho(\mathbf{f}_s)\mathbb{Y}^{\mathbf{f}_s^-}. \tag{36}$$

We have the following canonical representation for normal binomial σ-ideals.

Theorem 92. *Use the notations in (36). Then $\mathcal{I}^+(\rho) = \mathrm{sat}(\mathcal{A}^+(\rho))$, where $\mathrm{sat}(\mathcal{A}^+(\rho))$ is defined in (5). Furthermore, $\mathcal{A}^+(\rho)$ is a regular and coherent σ-chain and hence is a characteristic set of $\mathcal{I}^+(\rho)$.*

Proof. Assume that $\mathcal{A}^+(\rho)$ is not trivial, that is, $\mathcal{A}^+(\rho) \neq 1$. Let $\mathcal{I}_1 = [\mathcal{A}^+(\rho)] : \mathbb{m}$. We claim $\mathcal{I}_1 = \mathrm{sat}(\mathcal{A}^+(\rho))$. It is clear that $\mathrm{sat}(\mathcal{A}^+(\rho)) \subset [\mathcal{A}^+(\rho)] : \mathbb{m} = \mathcal{I}_1$. For the other direction, let $p \in \mathcal{I}_1$ and $p_1 = \mathrm{prem}(p, \mathcal{A}^+(\rho))$ which is reduced w.r.t. $\mathcal{A}^+(\rho)$. By (3), $p_1 \in \mathcal{I}_1$. As a consequence, $p_1 \in [\mathcal{A}(\rho)]$ as Laurent σ-polynomials in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$. By Lemma 31, $\mathcal{A}(\rho)$ is a characteristic set of $[\mathcal{A}(\rho)]$. Since p_1 is reduced w.r.t. $\mathcal{A}^+(\rho)$, it is also reduced w.r.t. $\mathcal{A}(\rho)$. Then $p_1 = 0$ and hence the claim is proved.

We now prove $\mathcal{I}^+(\rho) = \mathrm{sat}(\mathcal{A}^+(\rho))$. By the above claim, Lemma 31, and Lemma 80, $\mathrm{sat}(\mathcal{A}^+(\rho)) = [\mathcal{A}^+(\rho)] : \mathbb{m} = [\mathcal{A}^+(\rho)]\mathcal{F}\{\mathbb{Y}^{\pm}\} \cap \mathcal{F}\{\mathbb{Y}\} = [\mathcal{A}(\rho)] \cap \mathcal{F}\{\mathbb{Y}\} = \mathcal{I}(\rho) \cap \mathcal{F}\{\mathbb{Y}\} = \mathcal{I}^+(\rho)$.

It remains to prove that $\mathcal{A}^+(\rho)$ is a characteristic set of $\mathcal{I}_1 = [\mathcal{A}^+(\rho)] : \mathbb{m}$. By definition, it suffices to show that if $p \in \mathcal{I}_1$ is reduced w.r.t. $\mathcal{A}^+(\rho)$ then $p = 0$. Let $A_i = \mathbb{Y}^{\mathbf{f}_i} - \rho(\mathbf{f}_i)$ and $A_i^+ = \mathbb{Y}^{\mathbf{f}_i^+} - \rho(\mathbf{f}_i)\mathbb{Y}^{\mathbf{f}_i^-}$. Since $p \in \mathcal{I}_1$, there exist a σ-monomial M and $f_{i,j} \in \mathcal{F}\{\mathbb{Y}\}$ such that $Mp = \sum_{i,j} f_{i,j}(A_i^+)^{x^j}$. Then in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$, we have $p = \sum_{i,j} g_{i,j} A_i^{x^j} \in [\mathcal{A}(\rho)]$, where $g_{i,j} \in \mathcal{F}\{\mathbb{Y}^{\pm}\}$. Since p is reduced w.r.t. $\mathcal{A}^+(\rho)$, it is also reduced w.r.t. $\mathcal{A}(\rho)$. By Lemma 31, $\mathcal{A}(\rho)$ is a characteristic set of $[\mathcal{A}(\rho)]$ and hence $p = 0$. The claim is proved.

Since $\mathcal{I}_1 = \mathrm{sat}(\mathcal{A}^+(\rho))$, $\mathcal{A}^+(\rho)$ is also a characteristic set of $\mathrm{sat}(\mathcal{A}^+(\rho))$. By Theorem 1, $\mathcal{A}^+(\rho)$ is regular and coherent. □

Example 93. Let $L = ([1 - x, x - 1]^\tau)$ be a $\mathbb{Z}[x]$-module and ρ the trivial partial character on L, that is, $\rho(\mathbf{f}) = 1$ for $\mathbf{f} \in$L. By Theorem 92, $\mathcal{I}^+(\rho) = \mathrm{sat}[y_1 y_2^x - y_1^x y_2] \subseteq \mathbb{Q}\{y_1, y_2\}$. By Corollary 86, $\mathcal{I}^+(\rho)$

is a reflexive prime σ-ideal. We can show that $\mathcal{I}^+(\rho) = [y_1^{x^i} y_2^{x^j} - y_1^{x^j} y_2^{x^i} \mid 0 \le i < j \le m]$, which is an infinitely generated σ-ideal.

As a consequence of Theorem 83, Theorem 92, and Lemma 31, we have

Corollary 94. *Let $\mathcal{A}(\rho)$ and $\mathcal{A}^+(\rho)$ be defined in (21) and (36), respectively. Then $([\mathcal{A}(\rho)]\mathcal{F}\{\mathbb{Y}^{\pm}\}) \cap \mathcal{F}\{\mathbb{Y}\} = \mathrm{sat}(\mathcal{A}^+(\rho))$.*

As a consequence of Theorem 37, Corollary 86, and Theorem 92, we have

Corollary 95. *$[\mathcal{A}(\rho)]$ is a reflexive (prime) σ-ideal in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$ if and only if $\mathrm{sat}(\mathcal{A}^+(\rho))$ is a reflexive (prime) σ-ideal in $\mathcal{F}\{\mathbb{Y}\}$.*

We now prove the converse of Theorem 92. Let $\mathbf{f}_i \in \mathbb{Z}[x]^n$ and $c_i \in \mathcal{F}^*$, $i = 1, \ldots, s$. Consider the following σ-chains

$$\begin{aligned} &\mathcal{A} : \mathbb{Y}^{\mathbf{f}_1} - c_1, \ldots, \mathbb{Y}^{\mathbf{f}_s} - c_s \\ &\mathcal{A}^+ : \mathbb{Y}^{\mathbf{f}_1^+} - c_1 \mathbb{Y}^{\mathbf{f}_1^-}, \ldots, \mathbb{Y}^{\mathbb{Y}^{\mathbf{f}_s^+}} - c_s \mathbb{Y}^{\mathbf{f}_s^-} \end{aligned} \tag{37}$$

in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$ and $\mathcal{F}\{\mathbb{Y}\}$, respectively. Notice that, when talking about $\mathcal{A}^+$ (or $\mathcal{A}$), all operations are performed in $\mathcal{F}\{\mathbb{Y}\}$ (or $\mathcal{F}\{\mathbb{Y}^{\pm}\}$). Since $\mathbf{f}_i$ are assumed to be normal, $\mathcal{A}^+$ is a σ-chain if and only if $\mathcal{A}$ is a Laurent σ-chain (defined in Section 4.2).

Lemma 96. *Use the notations in (37). Let $p = a\mathbb{Y}^{\mathbf{a}} + b\mathbb{Y}^{\mathbf{b}} = aN(\mathbb{Y}^{\mathbf{f}} - c) \in \mathcal{F}\{\mathbb{Y}\}$, where $\mathbf{a}, \mathbf{b} \in \mathbb{N}[x]^n$, $\mathbf{f} \in \mathbb{Z}[x]^n$, N is a σ-monomial, $a, b, c \in \mathcal{F}^*$. If $\mathcal{A}^+$ is coherent and regular, then $\mathrm{prem}(p, \mathcal{A}^+) = 0$ implies $\mathrm{prem}(\mathbb{Y}^{\mathbf{f}} - c, \mathcal{A}) = 0$.*

Proof. Since $\mathrm{prem}(p, \mathcal{A}^+) = 0$, there exists a σ-monomial M_1 such that $M_1 p \in [\mathcal{A}^+]$. Let $p_1 = \mathbb{Y}^{\mathbf{f}} - c$. Since $r_1 = \mathrm{prem}(p_1, \mathcal{A}) = \mathbb{Y}^{\mathbf{g}} - c_{\mathbf{g}}$, by Lemma 20, there exists a $c_1 \in \mathcal{F}^*$ such that $r_1 - c_1 p_1 \in [\mathcal{A}]$. Then, there exists a σ-monomial M_2 such that $M_2 N r_1, M_2 N p_1 \in \mathcal{F}\{\mathbb{Y}\}$ and $M_2 N(r_1 - c_1 p_1) \in [\mathcal{A}^+]$ and hence $M_2 M_1 N(r_1 - c_1 p_1) = M_2 M_1 N r_1 - \frac{c_1}{a} M_2 M_1 p \in [\mathcal{A}^+]$. Let $M = M_1 M_2 N$. From $M_1 p \in [\mathcal{A}^+]$, we have $M r_1 \in [\mathcal{A}^+] \subset \mathrm{sat}(\mathcal{A}^+)$.

Suppose $A_i = \mathbb{Y}^{\mathbf{f}_i^+} - c\mathbb{Y}^{\mathbf{f}_i^-} = I_i^+ y_{c_i}^{d_i x^{o_i}} - c I_i^-$, where y_{c_i} is the leading variable of A_i. A variable like $y_{c_i}^{x^{o_i+k}}$ for $k \in \mathbb{N}$ is called a *main variable* of $\mathcal{A}^+$. A variable $y_i^{x^j}$ is called a *parameter* of $\mathcal{A}^+$ if it is not a main variable. If M contains a main variable of $\mathcal{A}^+$ as a factor. Then let $z = y_{c_i}^{x^{o_i+k}}$ be the largest one appearing in M under the variable ordering induced by the lexicographical of the index $(c_i, o_i + k)$. Let $s = \deg(M, z)$ and $M_1 = M/(z^s)$. We may assume that d_i is a factor of s. Otherwise, let $s_1 = \lfloor \frac{s}{d_i} \rfloor$, $s_0 = s - s_1 d_i$, and consider $M z^{d_i - s_0} = M_1 z^{d_i(s_1+1)}$ as the new M. We still have $M r_1 \in \mathrm{sat}(\mathcal{A}^+)$. We may use $A_i = 0$ to eliminate z from M as follows: $M_1 z^{s-d_i}(c I_i^-)^{x^k} r_1 = M_1 z^{s-d_i}(I_i^+ y_{c_i}^{d_i x^{o_i}} - A_i)^{x^k} r_1 = M(I_i^+)^{x^k} r_1 - M_1 z^{s-d_i}(A_i)^{x^k} r_1 \in \mathrm{sat}(\mathcal{A}^+)$. Note that $\deg(M_1 z^{s-d_i}(c I_i^-)^{x^k}, z) = s - d_i$. Repeating the above procedure, we may find a σ-monomial N such that $N r_1 \in \mathrm{sat}(\mathcal{A}^+)$, N does not contain z as a factor, and any variable $y_i^{x^j}$ in M is smaller than z in the given variable ordering. Repeat the procedure, we may finally obtain a σ-monomial L such that L does not contain main variables of $\mathcal{A}^+$ as factors and $L r_1 \in \mathrm{sat}(\mathcal{A}^+)$. Since L contains only parameters of $\mathcal{A}^+$ and r_1 is reduced w.r.t. $\mathcal{A}^+$, $L r_1$ is also reduced w.r.t. $\mathcal{A}^+$. Since $\mathcal{A}^+$ is regular and coherent, by Lemma 5, it is the characteristic set of $\mathrm{sat}(\mathcal{A}^+)$. Therefore, $L r_1 = 0$, and $r_1 = 0$. □

The following example shows that if $\mathrm{prem}(p, \mathcal{A}^+) \neq 0$ then the relation between $\mathrm{prem}(p, \mathcal{A}^+)$ and $\mathrm{prem}(\mathbb{Y}^{\mathbf{f}} - c, \mathcal{A})$ may be complicated, where $p = a\mathbb{Y}^{\mathbf{a}} + b\mathbb{Y}^{\mathbf{b}} = aN(\mathbb{Y}^{\mathbf{f}} - c)$.

Example 97. Let $p = y_2(y_2 - 1)$, $A_1 = y_1^{-1}y_2^2 - 1$, and $A_1^+ = y_2^2 - y_1$. Then $\mathrm{prem}(p, A_1^+) = y_1 - y_2$ in $\mathcal{F}\{y_1, y_2\}$. But in the Laurent case, p is represented as $\widetilde{p} = y_2 - 1$ and $\mathrm{prem}(\widetilde{p}, A_1) = y_2 - 1$.

Lemma 98. *Use the notations in (37). $\mathcal{A}$ is a Laurent regular and coherent σ-chain in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$ if and only if $\mathcal{A}^+$ is a regular and coherent σ-chain in $\mathcal{F}\{\mathbb{Y}\}$.*

Proof. If $\mathcal{A}$ is regular and coherent, by Theorem 33 and Theorem 34, there exists a partial character ρ on $\mathbb{Z}[x]^n$ such that $L_\rho = (\mathbf{f}_1, \ldots, \mathbf{f}_s)$, $\rho(\mathbf{f}_i) = c_i$, and $\mathcal{I}(\rho) = [\mathcal{A}]$. By Theorem 92, $\mathcal{A}^+ = \mathcal{A}^+(\rho)$ is regular and coherent.

Assume that $\mathcal{A}^+$ is regular and coherent. We first show that $[\mathcal{A}] \neq [1]$ in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$. It suffices to show that $\mathrm{sat}(\mathcal{A}^+)$ does not contain a σ-monomial. Suppose the contrary, there is a σ-monomial $M \in \mathrm{sat}(\mathcal{A}^+)$. Since $\mathcal{A}^+$ is a regular and coherent σ-chain, we have $\mathrm{prem}(M, \mathcal{A}^+) = 0$. Now consider the procedure of prem, it can be shown that the pseudo-remainder of a nonzero σ-monomial w.r.t. a binomial σ-chain is still a nonzero σ-monomial, a contradiction.

Note that $\mathcal{A}$ is always regular since σ-monomials are invertible in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$. Then, it suffices to prove that $\mathcal{A}$ is coherent.

Let $A_i = \mathbb{Y}^{\mathbf{f}_i} - c_i$ and $A_i^+ = \mathbb{Y}^{\mathbf{f}_i^+} - c_i\mathbb{Y}^{\mathbf{f}_i^-}$. Assume A_i^+ and A_j^+ $(i < j)$ have the same leading variable y_l, and $A_i^+ = I_i^+ y_l^{d_i x^{o_i}} - c_i I_i^-$, $A_j^+ = I_j^+ y_l^{d_j x^{o_j}} - c_j I_j^-$, where $I_i^- = \mathbb{Y}^{\mathbf{f}_i^-}$. From Definition 7, we have $o_i < o_j$ and $d_i | d_j$. Let $d_i = t d_j$ where $t \in \mathbb{N}$. From (4),

$$\Delta(A_i^+, A_j^+) = \mathrm{prem}((A_i^+)^{x^{o_j - o_i}}, A_j^+) = c_j^t (I_j^-)^t (I_i^-)^{x^{o_j - o_i}} - (I_j^+)^t (c_i I_i^+)^{x^{o_j - o_i}}.$$

Comparing to (19), if $\Delta(A_i, A_j) = \mathbb{Y}^{\mathbf{h}} - c_f$, then $\Delta(A_i^+, A_j^+) = c_j^t M(\mathbb{Y}^{\mathbf{h}^+} - c_f \mathbb{Y}^{\mathbf{h}^-})$, where M is a σ-monomial. Since $\mathcal{A}^+$ is coherent, $\mathrm{prem}(\Delta(A_i^+, A_j^+), \mathcal{A}^+) = 0$. By Lemma 96, $\mathrm{prem}(\Delta(A_i, A_j), \mathcal{A}) = 0$ which implies that $\mathcal{A}$ is coherent. □

We now prove the converse of Theorem 92.

Theorem 99. *Use the notations in (37). If $\mathcal{A}^+$ is a regular and coherent σ-chain, then there is a partial character ρ on $\mathbb{Z}[x]^n$ such that $L_\rho = (\mathbf{f}_1, \ldots, \mathbf{f}_s)$, $\rho(\mathbf{f}_i) = c_i$, $\mathcal{I}(\rho) = [\mathcal{A}]$, and $\mathcal{I}^+(\rho) = \mathrm{sat}(\mathcal{A}^+)$*

Proof. By Lemma 98, $\mathcal{A}$ is regular and coherent. By Theorem 29, $\mathbf{f}$ is a reduced Gröbner basis for a $\mathbb{Z}[x]$-lattice and $[\mathcal{A}] \subset \mathcal{F}\{\mathbb{Y}^{\pm}\}$ is proper. By Theorem 33 and Theorem 34, there exists a partial character ρ such that $L_\rho = (\mathbf{f}_1, \ldots, \mathbf{f}_s)$, $\rho(\mathbf{f}_i) = c_i$, and $\mathcal{I}(\rho) = [\mathcal{A}]$. By Theorem 92, $\mathcal{I}^+(\rho) = \mathrm{sat}(\mathcal{A}^+(\rho)) = \mathrm{sat}(\mathcal{A}^+)$. □

As a consequence of Theorem 99 and Lemma 80, we have the following canonical representation for a normal binomial σ-ideal.

Corollary 100. *$\mathcal{I}$ is a normal binomial σ-ideal if and only if $\mathcal{I} = \mathrm{sat}(\mathcal{A}^+)$, where $\mathcal{A}^+$ is a regular and coherent σ-chain given in (37).*

6.4. Perfect closure of binomial σ-ideal and binomial σ-variety

In this section, we will show that the perfect closure of a binomial σ-ideal is also binomial. We will also give a geometric description of the zero set of a binomial σ-ideal. For the perfect closure of a binomial σ-ideal, we have

Theorem 101. *Let $\mathcal{F}$ be an algebraically closed and inversive σ-field. The perfect closure of a binomial σ-ideal $\mathcal{I}$ is binomial.*

We remark that it is not known whether the well-mixed closure of a binomial σ-ideal is still binomial. Before proving Theorem 101, we first prove several lemmas. In the rest of this section, we assume that $\mathcal{I} \subseteq S = \mathcal{F}\{\mathbb{Y}\}$ and $\mathbb{m}$ the set of σ-monomials in S.

Lemma 102. *If $\mathcal{I}$ is a binomial σ-ideal, then $\{\mathcal{I}\} : \mathbb{m}$ is either $[1]$ or a binomial σ-ideal.*

Proof. It is easy to check $\{\mathcal{I}\}\mathcal{F}\{\mathbb{Y}^{\pm}\} = \{\mathcal{I}\mathcal{F}\{\mathbb{Y}^{\pm}\}\}$. By (32), $\{\mathcal{I}\} : \mathbb{m} = \{\mathcal{I}\}\mathcal{F}\{\mathbb{Y}^{\pm}\} \cap \mathcal{F}\{\mathbb{Y}\} = \{\mathcal{I}\mathcal{F}\{\mathbb{Y}^{\pm}\}\} \cap \mathcal{F}\{\mathbb{Y}\}$. Now the lemma follows from Theorem 63. □

Lemma 103. *If $\mathcal{I}$ is a σ-ideal in $\mathcal{F}\{\mathbb{Y}\}$, then*

$$\{\mathcal{I}\} = \{\mathcal{I}\} : \mathbb{m} \cap \{\mathcal{I} + y_1\} \cap \cdots \cap \{\mathcal{I} + y_n\} \tag{38}$$

Proof. The right hand side of (38) clearly contains $\{\mathcal{I}\}$. It suffices to show that every reflexive prime P containing $\mathcal{I}$ contains one of the σ-ideals on the right-hand side of (38). If $\{\mathcal{I}\} : \mathbb{m} \subseteq P$, we are done. Otherwise, there exists an element $f \in (\{\mathcal{I}\} : \mathbb{m}) \setminus P$ which implies that there exists a σ-monomial M such that $Mf \in \{\mathcal{I}\} \subseteq P$. This implies $y_i \in P$ for some i. Thus, P contains $\{\mathcal{I} + y_i\}$ as required. □

Lemma 104. *Let $\mathcal{I}$ be a binomial σ-ideal in $S = \mathcal{F}\{\mathbb{Y}\}$ and $S' = \mathcal{F}\{y_1, \ldots, y_{n-1}\}$. If $\mathcal{I}' = \mathcal{I} \cap S'$, then $[\mathcal{I} + y_n]$ is the sum of $[\mathcal{I}'S + y_n]$ and a monomial σ-ideal in S'.*

Proof. Every σ-binomial involving $y_n^{x^k}$ is either contained in $[y_n]$ or is congruent modulo $[y_n]$ to a σ-monomial in S'. Thus, all generators of $\mathcal{I}$ which are not in $\mathcal{I}'$ may be replaced by σ-monomials in S' when forming a generating set for $[\mathcal{I} + y_n]$. □

Lemma 105. *Let $\mathcal{I}$ be a perfect binomial σ-ideal in $S = \mathcal{F}\{\mathbb{Y}\}$. If $\mathcal{M}$ is a monomial σ-ideal, then $\{\mathcal{I} + \mathcal{M}\} = [\mathcal{I} + \mathcal{M}_1]$ for some monomial σ-ideal $\mathcal{M}_1$.*

Proof. If $1 \in \mathcal{M}$, then the lemma is obviously valid. Otherwise, $[\mathcal{I} + \mathcal{M}] : \mathbb{m} = [1]$. Lemma 103 yields $\{\mathcal{I} + \mathcal{M}\} = \bigcap_{i=1}^{i=n} \{\mathcal{I} + \mathcal{M} + y_i\}$. By Corollary 72, we need only to show that $\{\mathcal{I} + \mathcal{M} + y_i\}$ is the sum of $\mathcal{I}$ and a monomial σ-ideal. For simplicity, let $i = n$ and write $S' = \mathcal{F}\{y_1, y_2, \ldots, y_{n-1}\}$. Since $\mathcal{I}$ is perfect, the σ-ideal $\mathcal{I}' = \mathcal{I} \cap S'$ is perfect as well. By Lemma 104, $[\mathcal{I} + \mathcal{M} + y_n] = [\mathcal{I}'S + \mathcal{M}'S + y_n]$ where $\mathcal{M}'$ is a monomial σ-ideal in S'. By induction on n, the perfect closure of $\mathcal{I}' + \mathcal{M}'$ in S' has the form $\mathcal{I}' + \mathcal{M}'_1$, where $\mathcal{M}'_1$ is a monomial σ-ideal of S'. Putting this together, we have

$$\begin{aligned} \{\mathcal{I} + \mathcal{M} + y_n\} &= \{\mathcal{I}'S + \mathcal{M}'S + y_n\} = [\mathcal{I}'S + \mathcal{M}'_1 S + y_n] \\ &\subseteq [\mathcal{I} + \mathcal{M}'_1 S + y_n] \subseteq \{\mathcal{I} + \mathcal{M} + y_n\}. \end{aligned}$$

So $\{\mathcal{I} + \mathcal{M} + y_n\} = [\mathcal{I} + \mathcal{M}'_1 S + y_n]$ is $\mathcal{I}$ plus a monomial σ-ideal, as required. □

Proof of Theorem 101. We will prove the theorem by induction on n. By Lemma 102, $\mathcal{I}_1 = \{\mathcal{I}\} : \mathbb{m}$ is binomial. For $n = 1$, by Lemma 103, $\{\mathcal{I}\} = \mathcal{I}_1 \cap \{\mathcal{I} + y_1\}$. If $\{\mathcal{I} + y_1\} = [1]$ then $\{\mathcal{I}\} = \mathcal{I}_1$ is binomial. Otherwise $\{\mathcal{I} + y_1\} = [y_1]$ and hence $\mathcal{I} \subset [y_1]$. Since $\mathcal{I} \subset \mathcal{I}_1$, $\{\mathcal{I}\} = \mathcal{I}_1 \cap [y_1] = [\mathcal{I} + \mathcal{I}_1] \cap [\mathcal{I} + y_1]$ is binomial by Lemma 71. Suppose the lemma is valid for $n - 1$ variables and let $\mathcal{I}$ be a binomial σ-ideal in $S = \mathcal{F}\{\mathbb{Y}\}$. Let $\mathcal{I}_j := \mathcal{I} \cap S_j$, where $S_j = \mathcal{F}\{y_1, \ldots, y_{j-1}, y_{j+1}, \ldots, y_n\}$. By the induction hypothesis, we may assume that the perfect closure of each $\mathcal{I}_j$ is binomial. Adding these binomial σ-ideals to $\mathcal{I}$, we may assume that each $\mathcal{I}_j$ is perfect begin with. By Lemma 102, $\mathcal{I}_1 = \{\mathcal{I}\} : \mathbb{m}$ is binomial. Then there exists a binomial σ-ideal $\mathcal{I}'$, say $\mathcal{I}' = \mathcal{I}_1$, such that $\mathcal{I}_1 = [\mathcal{I} + \mathcal{I}']$. By Lemma 104, $[\mathcal{I} + y_j] = [\mathcal{I}_j S + \mathcal{J}_j S + y_j]$, where $\mathcal{J}_j$ is a monomial σ-ideal in S_j. Since $\mathcal{I}_j$ is perfect, the σ-ideal $\mathcal{I}_j S$ is perfect, so we can apply Lemma 105 with $\mathcal{M} = [\mathcal{J}_j S + y_i]$ to see that there exists a monomial σ-ideal $\mathcal{M}_j$ in S such that $\{\mathcal{I} + y_j\} = \{\mathcal{I}_j S + \mathcal{J}_j S + y_j\} = [\mathcal{I}_j S + \mathcal{M}_j] = [\mathcal{I} + \mathcal{M}_j]$. By Lemma 103 and Corollary 71, $\{\mathcal{I}\} = [\mathcal{I} + \mathcal{I}'] \cap \bigcap_{j=1}^{n} [\mathcal{I} + \mathcal{M}_j]$ is binomial. □

Example 106. Let $p = y_2^2 - y_1^2$. Following the proof of Theorem 101, $\{p\} = (\{p\} : \mathbb{m}) \cap [y_1, y_2]$. By Example 60 and Corollary 94, $\mathcal{I}_1 = \{p\} : \mathbb{m} = \text{sat}[y_2^2 - y_1^2, y_1 y_2^x - y_1^x y_2] = [y_1 y_2^{x^i} - y_1^{x^i} y_2, y_2^{1+x^j} - y_1^{1+x^j} \mid i, j \in \mathbb{N}]$. Thus, $\{p\} = \mathcal{I}_1 \cap [y_1, y_2] = \mathcal{I}_1$.

In the rest of this section, we give a geometric description of the zero set of a binomial σ-ideal, which is a generalization of Theorem 4.1 in Eisenbud and Sturmfels (1996) to the difference case. The basic idea of the proof also follows Eisenbud and Sturmfels (1996), except we need to consider the distinction between the perfect σ-ideals and radical ideals.

We decompose the affine n-space $\mathbb{A}^n$ into the union of 2^n σ-coordinate flats:

$$(\mathbb{A}^*)^\Omega := \{(a_1, a_2, \ldots, a_n) \mid a_i \neq 0, i \in \Omega; a_i = 0, i \notin \Omega\}$$

where Ω runs over all subsets of $\{1, 2, \ldots, n\}$. The Cohn closure of $(\mathbb{A}^*)^\Omega$ in $\mathbb{A}^n$ is defined by the σ-ideal

$$M(\Omega) := [y_i | i \notin \Omega] \subset \mathcal{F}\{\mathbb{Y}\}.$$

The σ-coordinate ring of $(\mathbb{A}^*)^\Omega$ is the Laurent polynomial σ-ring $\mathcal{F}\{\Omega^\pm\} := \mathcal{F}\{y_i, y_i^{-1}, i \in \Omega\}$. We can define a coordinate projection $(\mathbb{A}^*)^{\Omega'} \longrightarrow (\mathbb{A}^*)^\Omega$ whenever $\Omega \subseteq \Omega' \subseteq \{1, 2, \ldots, n\}$ by setting all those coordinates not in Ω to zero.

If X is any σ-variety of $\mathbb{A}^n$ and $\mathcal{I} = \mathbb{I}(X) \subseteq \mathcal{F}\{\mathbb{Y}\}$, then the Cohn closure of the intersection of X with $(\mathbb{A}^*)^\Omega$ corresponds to the σ-ideal

$$\mathcal{I}_\Omega := [\mathcal{I} + M(\Omega)] : \mathbb{m}_\Omega \subset \mathcal{F}\{\mathbb{Y}\}$$

where $\mathbb{m}_\Omega = \{\prod_{i \in \Omega} y_i^{m_i(x)} | m_i(x) \in \mathbb{N}[x]\}$. Since $\mathcal{I}$ is perfect, by the difference Nullstellsatz,

$$\mathcal{I} = \bigcap_\Omega \{\mathcal{I}_\Omega\}.$$

If $\mathcal{I}$ is binomial, then by Corollary 73, the σ-ideal $\mathcal{I}_\Omega$ is also binomial.

Lemma 107. *Let $R := \mathcal{F}\{z_1, z_1^{-1}, \ldots, z_t, z_t^{-1}\} \subset R' := \mathcal{F}\{z_1, z_1^{-1}, \ldots, z_t, z_t^{-1}, y_1, \ldots, y_s\}$ be a Laurent polynomial σ-ring and a polynomial σ-ring over it. If $B \subset R'$ is a binomial σ-ideal and $M \subset R'$ is a monomial σ-ideal such that $[B + M]$ is a proper σ-ideal in R', then $[B + M] \cap R = B \cap R$.*

Proof. This is a σ-version of Eisenbud and Sturmfels (1996, Lemma 4.3), which can be proved similarly. □

We can make a classification of all binomial σ-varieties X by intersecting X with $(\mathbb{A}^*)^\Omega$, since by Theorem 101, the perfect closure of a binomial σ-ideal is still binomial.

Theorem 108. *Let $\mathcal{F}$ be any algebraically closed and inversive σ-field. A σ-variety $X \subset \mathbb{A}^n$ is generated by σ-binomials if and only if the following three conditions hold.*

(1) *For each $(\mathbb{A}^*)^\Omega$, the σ-variety $X \cap (\mathbb{A}^*)^\Omega$ is generated by σ-binomials.*
(2) *The family of sets $U = \{\Omega \subseteq \{1, 2, \ldots, n\} | X \cap (\mathbb{A}^*)^\Omega \neq \emptyset\}$ is closed under taking intersections.*
(3) *If $\Omega_1, \Omega_2 \in U$ and $\Omega_1 \subset \Omega_2$, then the coordinate projection $(\mathbb{A}^*)^{\Omega_2} \longrightarrow (\mathbb{A}^*)^{\Omega_1}$ maps $X \cap (\mathbb{A}^*)^{\Omega_2}$ onto a subset of $X \cap (\mathbb{A}^*)^{\Omega_1}$.*

The above theorem can be reduced to the following algebraic version.

Theorem 109. *Let $\mathcal{F}$ be any algebraically closed and inversive σ-field. A perfect σ-ideal $\mathcal{I} \subset \mathcal{F}\{\mathbb{Y}\}$ is binomial if and only if the following three conditions hold.*

(1) *For each* $\Omega \subseteq \{1, \ldots, n\}$, $\mathcal{I}_\Omega$ *is binomial.*
(2) $U = \{\Omega \subseteq \{1, 2, \ldots, n\} \mid \{\mathcal{I}_\Omega\} \neq [1]\}$ *is closed under taking intersections.*
(3) *If* $\Omega_1, \Omega_2 \in U$ *and* $\Omega_1 \subset \Omega_2$, *then* $\mathcal{I}_{\Omega_1} \cap \mathcal{F}\{\Omega_1\} \subset \mathcal{I}_{\Omega_2}$, *where* $\mathcal{F}\{\Omega_1\} = \mathcal{F}\{y_i \mid y_i \in \Omega_1\}$.

Proof. Suppose $\mathcal{I}$ is a perfect σ-ideal in $\mathcal{F}\{\mathbb{Y}\}$. Since $\mathcal{I}$ is binomial, by Lemma 73 $\mathcal{I}_\Omega$ is also binomial and (1) is proved. To prove (2) by contradiction, assume that for $\Omega_1, \Omega_2 \in U$, $\{\mathcal{I}_{\Omega_1}\} \neq [1], \{\mathcal{I}_{\Omega_2}\} \neq [1], \{\mathcal{I}_{\Omega_1 \cap \Omega_2}\} = [1]$. We consider two cases. If $\mathcal{I}_{\Omega_1 \cap \Omega_2} = [1]$, then for some $m(x) \in \mathbb{N}[x]$ we have $(\prod_{i \in \Omega_1 \cap \Omega_2} y_i)^{m(x)} \in [\mathcal{I} + M(\Omega_1) + M(\Omega_2)]$. By Corollary 72, $(\prod_{i \in \Omega_1 \cap \Omega_2} y_i)^{m(x)}$ is either in $[\mathcal{I} + M(\Omega_1)]$ or $[\mathcal{I} + M(\Omega_2)]$, so $\mathcal{I}_{\Omega_1}$ or $\mathcal{I}_{\Omega_2}$ is [1]. For the second case, we have $\mathcal{I}_{\Omega_1 \cap \Omega_2} \neq [1]$ and $\{\mathcal{I}_{\Omega_1 \cap \Omega_2}\} = [1]$. Then there exist a finite number of proper σ-binomials $B_1, \ldots, B_s$ and σ-monomials $m_1, \ldots, m_s$ in $\mathcal{F}\{\Omega_1 \cap \Omega_2\}$ such that $m_i B_i \in \mathcal{I}$ and $\{B_1, \ldots, B_s, y_i | i \notin \Omega_1 \cap \Omega_2\} = [1]$. We thus have $\{B_1, \ldots, B_s\} = [1]$. Since $m_i B_i \in \mathcal{I} \cap \mathcal{F}\{\Omega_1 \cap \Omega_2\}$, we have $B_i \in \mathcal{I}_{\Omega_1}$ and $B_i \in \mathcal{I}_{\Omega_2}$ and thus $\{\mathcal{I}_{\Omega_1}\} = \{\mathcal{I}_{\Omega_2}\} = [1]$. To prove (3), given $\Omega_1, \Omega_2 \in U$ and $\Omega_1 \subset \Omega_2$, we have $\mathcal{I}_{\Omega_2} = [\mathcal{I}_{\Omega_2} : \mathbb{m}_{\Omega_1}]$. Set $R' = \mathcal{F}\{\Omega_1^{\pm}\}\{\{y_i\}_{i \notin \Omega_1}\}$, then

$$[\mathcal{I} + M(\Omega_1)]R' \cap \mathcal{F}\{\Omega_1^{\pm}\} \subseteq \mathcal{I}_{\Omega_2} R'.$$

Since $\Omega_1 \in U$, the σ-ideal $[\mathcal{I} + M(\Omega_1)]R'$ is proper. By Lemma 107, we have $[\mathcal{I} + M(\Omega_1)]R' \cap \mathcal{F}\{\Omega_1^{\pm}\} = \mathcal{I}R' \cap \mathcal{F}\{\Omega_1^{\pm}\} \subset \mathcal{I}_{\Omega_2} R' \cap \mathcal{F}\{\Omega_1^{\pm}\}$. So $\mathcal{I}_{\Omega_1} \cap \mathcal{F}\{\Omega_1\} \subset \mathcal{I}_{\Omega_2}$.

To prove the other direction, let $\mathcal{I}$ be a perfect σ-ideal satisfying the three conditions. By the difference Nullstellensatz, $\mathcal{I} = \cap_{\Omega \in U}\{\mathcal{I}_\Omega\}$. By condition (2), U is a partially ordered set under the inclusion for subsets of $\{1, \ldots, n\}$. For each $\Omega \in U$, we set $\mathcal{J}(\Omega) = [\mathcal{I}_\Omega \cap \mathcal{F}\{\Omega\}]\mathcal{F}\{\mathbb{Y}\}$ with the properties that if $\Omega_1 \subset \Omega_2$, $\{\mathcal{J}(\Omega_1)\} \subset \{\mathcal{J}(\Omega_2)\}$. Note that $[M_{\Omega_1 \cap \Omega_2}] \subset [M_{\Omega_1} + M_{\Omega_2}]$. Then we have

$$\mathcal{I} = \cap_{\Omega \in U}\{\mathcal{I}_\Omega\} = \cap_{\Omega \in U}\{\mathcal{J}(\Omega) + M(\Omega)\}.$$

Now we will prove that

$$\cap_{\Omega \in U}\{\mathcal{J}(\Omega) + M(\Omega)\} = \{\cap_{\Omega \in U} M(\Omega) + \sum_{\Omega \in U}\{\mathcal{J}(\Omega) \cap (\cap_{\Omega_\eta \not\supseteq \Omega} M(\Omega_\eta))\}\}. \tag{39}$$

If $\Omega_2 \supseteq \Omega_1$, then $\{\mathcal{J}(\Omega_2) + M(\Omega_2)\} \supseteq \{\mathcal{J}(\Omega_2)\} \supseteq \{\mathcal{J}(\Omega_1)\} \supseteq \{\mathcal{J}(\Omega_1) \cap \cap_{\Omega_\eta \not\supseteq \Omega_1} M(\Omega_\eta)\}$. If $\Omega_2 \not\supseteq \Omega_1$, we have $\{\mathcal{J}(\Omega_2) + M(\Omega_2)\} \supseteq M\{\Omega_2\} \supseteq \{\mathcal{J}(\Omega_1) \cap \cap_{\Omega_\eta \not\supseteq \Omega_1} M(\Omega_\eta)\}$. So the left hand side contains the right hand side of (39). For the other direction, consider a reflexive prime σ-ideal $P \supseteq [\cap_{\Omega \in U} M(\Omega) + \sum_{\Omega \in U}\{\mathcal{J}(\Omega) \cap \cap_{\Omega_\eta \not\supseteq \Omega} M(\Omega_\eta)\}]$ and set $V = \{\Omega \in U | M(\Omega) \subset P\}$. Then V is a finite partially ordered set and nonempty since $P \supseteq \cap_{\Omega \in U} M(\Omega)$ and $\{M_{\Omega_1 \cap \Omega_2}\} \subset \{M_{\Omega_1} + M_{\Omega_2}\}$. Let Ω_0 be the smallest element of V such that $P \supseteq M_{\Omega_0}$. At the same time, $P \supset \mathcal{J}(\Omega_0) \cap \cap_{\Omega_\eta \not\supseteq \Omega_0} M(\Omega_\eta)$, then $P \supseteq \mathcal{J}(\Omega_0)$. Therefore, $P \supseteq \mathcal{J}(\Omega_0) + M(\Omega_0)$ and P contains the left hand side of (39) and (39) is proved. Since $\cap_{\Omega \in U} M(\Omega) + \sum_{\Omega \in U}\{\mathcal{J}(\Omega) \cap \cap_{\Omega_\eta \not\supseteq \Omega} M(\Omega_\eta)\}$ is binomial, the theorem follows from (39). □

7. Algorithms

In this section, we give algorithms for most of the results in the previous sections. In particular, we give an algorithm to decompose a finitely generated perfect binomial σ-ideal as the intersection of reflexive and prime binomial σ-ideals. The following basic algorithms will be used.

- **Algorithm GHNF**. Let $\mathbb{f}$ be a finite set of $\mathbb{Z}[x]^n$. The algorithm computes the generalized Hermite normal form of $[\mathbb{f}]$, or equivalently, the reduced Gröbner basis of the $\mathbb{Z}[x]$-module $(\mathbb{f})$ Cox et al. (1998, p. 197). A polynomial-time algorithm is given in Jing et al. (2016).

- **Algorithm GKER**. For a matrix $M \in \mathbb{Z}[x]^{n\times s}$, compute a set of generators of the $\mathbb{Z}[x]$-lattice: $\ker_{\mathbb{Z}[x]}(M) = \{X \in \mathbb{Z}[x]^s \mid MX = 0\}$. This can be done by combining Algorithm **GHNF** and Theorem 10.

Let $\mathbb{D}$ be $\mathbb{Z}$, $\mathbb{Q}[x]$, $\mathbb{Z}_p[x]$, or $\mathbb{Q}[x]/(q(x))$, where $q(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$. Then $\mathbb{D}$ is either a PID or a field. The following algorithms will be used.

- **Algorithm HNF**. For $M \in \mathbb{D}^{n\times s}$, compute the Hermite normal form of M (Cohen, 1993, p. 68).
- **Algorithm KER**. For a matrix $M \in \mathbb{D}^{n\times s}$, compute a basis for the $\mathbb{D}$-module: $\ker_{\mathbb{D}}(M) = \{X \in \mathbb{D}^s \mid MX = 0\}$ (Cohen, 1993, p. 74).

7.1. x-saturation of $\mathbb{Z}[x]$-lattice

In this section, we give algorithms to check whether a $\mathbb{Z}[x]$-lattice L is x-saturated and in the negative case to compute the x-saturation of L.

Let $\mathbf{f}_1, \ldots, \mathbf{f}_s \in \mathbb{Z}[x]^n$ and $L = (\mathbf{f}_1, \ldots, \mathbf{f}_s)$. If L is not x-saturated, then there exist $g_i \in \mathbb{Z}[x]$ such that $\sum_{i=1}^s g_i\mathbf{f}_i = x\mathbf{h}$ and $\mathbf{h} \notin L$. Setting $g_i(x) = g_i(0) + x\widetilde{g}_i(x)$ and $\widetilde{\mathbf{h}} = \mathbf{h} - \sum_{i=1}^s \widetilde{g}_i(x)\mathbf{f}_i$, we have

$$\sum_{i=1}^{s} g_i(0)\mathbf{f}_i = x\widetilde{\mathbf{h}} \tag{40}$$

where $\widetilde{\mathbf{h}} \notin L$. Setting $x = 0$ in the above equation, we have

$$\sum_{i=1}^{s} g_i(0)\mathbf{f}_i(0) = 0,$$

that is, $G = (g_1(0), \ldots, g_s(0))^\tau$ is in the kernel of the matrix $F = [\mathbf{f}_1(0), \ldots, \mathbf{f}_s(0)] \in \mathbb{Z}^{n\times s}$, which can be computed efficiently with Algorithm **KER**. From G and (40), we may compute $\widetilde{\mathbf{h}}$. This observation leads to the following algorithm.

Algorithm 1 — XFactor$([\mathbf{f}_1, \ldots, \mathbf{f}_s])$.

Input: A generalized Hermite normal form $[\mathbf{f}_1, \ldots, \mathbf{f}_s] \in \mathbb{Z}[x]^{n\times s}$.
Output: $\emptyset$, if the $\mathbb{Z}[x]$-lattice $L = (\mathbf{f}_1, \ldots, \mathbf{f}_s)$ is x-saturated; otherwise, a finite set $\{(\mathbf{h}_i, \mathbf{e}_i) \mid i = 1, \ldots, r\}$ such that $\mathbf{e}_i = (e_{i1}, \ldots, e_{is})^\tau \in \mathbb{Z}^s$, $\mathbf{h}_i \notin L$, and $x\mathbf{h}_i = \sum_{l=1}^s e_{il}\mathbf{f}_l \in L$, $i = 1, \ldots, r$.

1. Set $F = [\mathbf{f}_1(0), \ldots, \mathbf{f}_s(0)] \in \mathbb{Z}^{n\times s}$.
2. Compute a basis $E \subset \mathbb{Z}^s$ of the $\mathbb{Z}$-module $\ker_{\mathbb{Z}}(F)$ with Algorithm **KER**.
3. Set $H = \emptyset$.
4. While $E \neq \emptyset$
   4.1. Let $\mathbf{e} = (e_1, \ldots, e_s)^\tau \in E$ and $E = E \setminus \{\mathbf{e}\}$.
   4.2. Let $\mathbf{h} = (e_1\mathbf{f}_1 + \cdots + e_s\mathbf{f}_s)/x$.
   4.3. If $\mathrm{grem}(\mathbf{h}, \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}) \neq 0$, then add $(\mathbf{h}, \mathbf{e})$ to H.
5. Return H.

We now give the algorithm to compute the x-saturation of a $\mathbb{Z}[x]$-lattice.

Algorithm 2 — SatX$(\mathbf{f}_1, \ldots, \mathbf{f}_s)$.

Input: A finite set $\mathbb{f} = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\} \subset \mathbb{Z}[x]^n$.
Output: A set of generators of $\mathrm{sat}_x(\mathbf{f}_1, \ldots, \mathbf{f}_s)$.

1. Compute the generalized Hermite normal form $\mathbb{g}$ of $\mathbb{f}$ with Algorithm **GHNF**.
2. Set $H =$ **XFactor**$(\mathbb{g})$.
3. If $H = \emptyset$, then output $\mathbb{g}$; otherwise set $\mathbb{f} = \mathrm{Col}(\mathbb{g}) \cup \{\mathbf{h} \mid (\mathbf{h}, \mathbf{f}) \in H\}$ and goto step 1.

Note. $\mathrm{Col}(\mathbb{g})$ is the set of columns of $\mathbb{g}$.

Example 110. Let $\mathcal{C}$ be the following generalized Hermite normal form.

$$\mathcal{C} = [\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3] = \begin{bmatrix} -x+2 & 1 & 1 \\ 3x+2 & 1 & 2x+1 \\ 0 & 2x & x^2 \end{bmatrix}.$$

In **XFactor**$(\mathcal{C})$, the kernel of the following matrix $[\mathbf{f}_1(0), \mathbf{f}_2(0), \mathbf{f}_3(0)] = \begin{bmatrix} 2 & 1 & 1 \\ 2 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$ is generated by $\mathbf{e}_1 = (0, -1, 1)^\tau$ and $\mathbf{e}_2 = (1, -2, 0)^\tau$. In step 4.2 of **XFactor**, we have $\mathbf{h} = (-\mathbf{f}_2 + \mathbf{f}_3)/x = (0, 2, x-2)^\tau$. One can check that $(0, 2, x-2)^\tau \notin (\mathcal{C})$. In **SatX**, computing the generalized Hermite normal form of $\mathcal{C} \cup \{(0, 2, x-2)^\tau\}$, we have

$$\mathcal{C}_1 = \begin{bmatrix} 1 & 0 \\ -3 & 2 \\ 4 & x-2 \end{bmatrix}.$$

XFactor$(\mathcal{C}_1)$ returns $\emptyset$. So, $(\mathcal{C}_1)$ is the x-saturation of $(\mathcal{C})$.

Proposition 111. *Algorithms* **SatX** *and* **XFactor** *are correct.*

Proof. From the output of Algorithm **XFactor**, in step 3 of **SatX**, we have $(\mathfrak{g}) \subsetneq (\mathfrak{g} \cup \{\mathbf{h} \mid (\mathbf{h}, \mathbf{f}) \in H\}) \subseteq \mathrm{sat}_x(\mathbb{f})$. Since $\mathbb{Z}[x]^n$ is a Noetherian $\mathbb{Z}[x]$-module, **SatX** will terminate and return the x-saturation of $(\mathbb{f})$. So, it suffices to show the correctness of Algorithm **XFactor**.

We first explain step 4.2 of Algorithm **XFactor**. Since $\mathbf{e} \in \ker_{\mathbb{Z}}(F)$, $\mathbf{h}(0) = [\mathbf{f}_1(0), \ldots, \mathbf{f}_s(0)]\mathbf{e} = [0, \ldots, 0]^\tau$. Therefore, x is a factor of $e_1\mathbf{f}_1 + \cdots + e_s\mathbf{f}_s$ and thus $\mathbf{h} = (e_1\mathbf{f}_1 + \cdots + e_s\mathbf{f}_s)/x \in \mathbb{Z}[x]^n$.

To prove the correctness of Algorithm **XFactor**, it suffices to show that $L = \mathrm{sat}_x(L)$ if and only if for each $\mathbf{e} \in E$, $e_1\mathbf{f}_1 + \cdots + e_s\mathbf{f}_s = x\mathbf{h}$ implies $\mathbf{h} \in L$.

Let $E = \{\mathbf{e}_1, \ldots, \mathbf{e}_k\}$ where $\mathbf{e}_i \in \mathbb{Z}^s$. If $L = \mathrm{sat}_x(L)$, then it is clear that $(\mathbf{f}_1, \ldots, \mathbf{f}_s)\mathbf{e}_i = x\mathbf{h}_i$ implies $\mathbf{h}_i \in L$. To prove the other direction, let $[\mathbf{f}_1, \ldots, \mathbf{f}_s]\mathbf{e}_i = x\mathbf{h}_i$ for $1 \le i \le k$, where $\mathbf{h}_i \in L$. Let $x\mathbf{f} \in L$. Then $x\mathbf{f} = \sum_{i=1}^s c_i(x)\mathbf{f}_i$, where $c_i(x) \in \mathbb{Z}[x]$. If for each i, $x | c_i(x)$, then we have $\mathbf{f} = \sum_{i=1}^s (c_i(x)/x)\mathbf{f}_i \in L$, and the lemma is proved. Otherwise, set $x = 0$ in $x\mathbf{f} = \sum_{i=1}^s c_i(x)\mathbf{f}_i$, we obtain $\sum_{i=1}^s c_i(0)\mathbf{f}_i(0) = 0$. Hence $Q = [c_1(0), \ldots, c_s(0)]^\tau \in \ker_{\mathbb{Z}}(F)$ and hence there exist $a_i \in \mathbb{Z}, i = 1, \ldots, k$ such that $Q = \sum_{i=1}^k a_i\mathbf{e}_i$. Then, $[\mathbf{f}_1, \ldots, \mathbf{f}_s]Q = \sum_{i=1}^k a_i[\mathbf{f}_1, \ldots, \mathbf{f}_s]\mathbf{e}_i = \sum_{i=1}^k a_i x\mathbf{h}_i = x\widetilde{\mathbf{h}}$, where $\widetilde{\mathbf{h}} = \sum_{i=1}^k a_i\mathbf{h}_i \in L$. Then,

$$\begin{aligned} x\mathbf{f} &= \textstyle\sum_{i=1}^s c_i(x)\mathbf{f}_i = \sum_{i=1}^s c_i(0)\mathbf{f}_i + \sum_{i=1}^s x\overline{c}_i(x)\mathbf{f}_i \\ &= [\mathbf{f}_1, \ldots, \mathbf{f}_s]Q + x\textstyle\sum_{i=1}^s \overline{c}_i(x)\mathbf{f}_i = x\widetilde{\mathbf{h}} + x\sum_{i=1}^s \overline{c}_i(x)\mathbf{f}_i, \end{aligned}$$

where $\overline{c}_i(x) = (c_i(x) - c_i(0))/x \in \mathbb{Z}[x]$. Hence, $\mathbf{f} = \widetilde{\mathbf{h}} + \sum_{i=1}^s \overline{c}_i(x)\mathbf{f}_i \in L$ and the lemma is proved. □

7.2. $\mathbb{Z}$-saturation of $\mathbb{Z}[x]$-lattice

The key idea to compute $\mathrm{sat}_{\mathbb{Z}}(L)$ for a $\mathbb{Z}[x]$-lattice $L \in \mathbb{Z}[x]^n$ is as follows. Let $\mathbb{f} = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$. Then $(\mathbb{f})$ is not $\mathbb{Z}$-saturated if and only if a linear combination of $\mathbf{f}_i$ contains a nontrivial prime factor in $\mathbb{Z}$, that is, $\sum_i g_i\mathbf{f}_i = p\mathbf{f}$, where p is a prime number and $\mathbf{f} \notin (\mathbb{f})$. Furthermore, $\sum_i g_i\mathbf{f}_i = p\mathbf{f}$ with $g_i \neq 0 \bmod p$ for some $i \in \{1, 2, \ldots, s\}$ is valid if and only if $\mathbf{f}_1, \ldots, \mathbf{f}_s$ are linearly dependent over $\mathbb{Z}_p[x]$. The fact that $\mathbb{Z}_p[x]$ is a PID allows us to compute such linear relations using methods of Hermite normal forms (Cohen, 1993). The following algorithm is based on this observation.

Algorithm 3 — ZFactor.

Input: A generalized Hermite normal form $\mathcal{C} = [\mathbf{c}_1, \ldots, \mathbf{c}_s] \subset \mathbb{Z}[x]^n$ of form (7).

Output: $\emptyset$, if $L = (\mathcal{C})$ is $\mathbb{Z}$-saturated; otherwise, a finite set $\{(\mathbf{h}_i, k_i, \mathbf{e}_i) \mid i = 1, \ldots, r\}$, such that $\mathbf{h}_i \in \mathbb{Z}[x]^n$, $k_i \in \mathbb{N}$, $\mathbf{e}_i = (e_{i1}, \ldots, e_{is})^\tau \in \mathbb{Z}[x]^s$, $\mathbf{h}_i \notin L$ and $k_i \mathbf{h}_i = \sum_{l=1}^s e_{il}\mathbf{c}_l \in L$ for $i = 1, \ldots, r$.

1. Read the numbers $t, r_i, l_i, c_{r_i,1,0}, i = 1, \ldots, t$ from (7).
2. Set $q = \prod_{i=1}^t c_{r_i,1,0} \in \mathbb{N}$.
3. For any prime factor p of q do
   - 3.1. Set $F = [\mathbf{c}_{r_1,l_1}, \mathbf{c}_{r_2,l_2}, \ldots, \mathbf{c}_{r_t,l_t}] \in \mathbb{Z}_p[x]^{n\times t}$.
   - 3.2. With Algorithm **KER**, compute $G \subset \mathbb{Z}[x]^t$ such that the image G in $\mathbb{Z}_p[x]^t$ is a basis of the $\mathbb{Z}_p[x]$-module $\ker_{\mathbb{Z}_p[x]}(F)$.
   - 3.3. If $G \neq \emptyset$, for each $\mathbf{g} = [g_1, \ldots, g_t]^\tau \in G$, let $\sum_{i=1}^t g_i \mathbf{c}_{r_i,l_i} = p\mathbf{h}$ in $\mathbb{Z}[x]^n$. Return the set of $(\mathbf{h}, p, \mathbf{e})$, where $\mathbf{e} = [e_1, \ldots, e_s]^\tau \in \mathbb{Z}[x]^s$ such that $e_{s_k} = g_k$, $s_k = \sum_{i=1}^k l_i, k = 1, \ldots, t$ and $e_j = 0$ for other j.
   - 3.4. With Algorithm **HNF**, compute $B = [\mathbf{b}_1, \ldots, \mathbf{b}_t] \subset \mathbb{Z}[x]^{n\times t}$ such that the image of B in $\mathbb{Z}_p[x]^{n\times t}$ is the Hermite normal form of $[\mathbf{c}_{r_1,l_1}, \ldots, \mathbf{c}_{r_t,l_t}]$ in $\mathbb{Z}_p[x]^{n\times t}$.
   - 3.5. Let $\mathcal{C}_- = \{\mathbf{f}_1, \ldots, \mathbf{f}_l\}$ be given in (9) and $\widetilde{\mathbf{f}}_i = \mathrm{grem}(\mathbf{f}_i, \mathcal{B}) = \mathbf{f}_i + \sum_{k=1}^t a_{i,k}\mathbf{b}_k$, in $\mathbb{Z}_p[x]^n$, where $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_t\}$ and $a_{i,k} \in \mathbb{Z}_p[x]$.
   - 3.6. If $\widetilde{\mathbf{f}}_i = 0$ for some i, then $\mathbf{f}_i + \sum_{k=1}^t a_{i,k}\mathbf{b}_k = p\mathbf{h}_i$ in $\mathbb{Z}[x]^n$. Return the set of $(\mathbf{h}_i, p, \mathbf{e}_i)$ where $\mathbf{e}_i$ is a vector in $\mathbb{Z}[x]^s$ such that $(\mathbf{c}_1, \ldots, \mathbf{c}_s)\mathbf{e}_i = \mathbf{f}_i + \sum_{k=1}^t a_{i,k}\mathbf{b}_k = p\mathbf{h}_i$.
   - 3.7. Set $E = [\widetilde{\mathbf{f}}_1, \ldots, \widetilde{\mathbf{f}}_l] \in \mathbb{Z}_p[x]^{n\times l}$.
   - 3.8. Compute a basis D of $\{X \in \mathbb{Z}_p^l \mid EX = 0\}$ as a vector space over $\mathbb{Z}_p$.
   - 3.9. If $D \neq \emptyset$, for each $\mathbf{b} = [b_1, \ldots, b_l]^\tau \in D$, $\sum_{i=1}^l b_i \widetilde{\mathbf{f}}_i = p\mathbf{h}$ in $\mathbb{Z}[x]^n$. Return the set of $(\mathbf{h}, p, \mathbf{e})$ where $\mathbf{e}$ is a vector in $\mathbb{Z}[x]^s$ such that $(\mathbf{c}_1, \ldots, \mathbf{c}_s)\mathbf{e} = \sum_{i=1}^l b_i \widetilde{\mathbf{f}}_i = p\mathbf{h}$.
4. Return $\emptyset$.

Remark 112. In steps 3.6 and 3.9, we need to compute $\mathbf{e}_i$ or $\mathbf{e}$. Since $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_t\}$ is the Hermite normal form of $\mathbf{c} = \{\mathbf{c}_{r_1,l_1}, \ldots, \mathbf{c}_{r_t,l_t}\}$ in $\mathbb{Z}_p[x]^n$, there exists an invertible matrix $M_{t\times t}$ such that $[\mathbf{b}_1, \ldots, \mathbf{b}_t] = [\mathbf{c}_{r_1,l_1}, \ldots, \mathbf{c}_{r_t,l_t}]M$. In Step 3.6, $\mathbf{e}_i$ can be obtained from the relation $\mathbf{f}_i + \sum_{k=1}^t a_{i,k}\mathbf{b}_k = p\mathbf{h}_i$ and the relation $[\mathbf{b}_1, \ldots, \mathbf{b}_t] = [\mathbf{c}_{r_1,l_1}, \ldots, \mathbf{c}_{r_t,l_t}]M$. Step 3.9 can be treated similarly.

Remark 113. In step 3.8, we need to compute a basis for the vector space $\{X \in \mathbb{Z}_p^l \mid EX = 0\}$ over $\mathbb{Z}_p$. We will show how to do this. A matrix $F \in \mathbb{Z}_p[x]^{m\times s}$ is said to be in standard form if F has the structure in (7) and $\deg(c_{r_i,k_1}, x) < \deg(c_{r_i,k_2}, x)$ for $i = 1, \ldots, t$ and $k_1 < k_2$.

The matrix $E \in \mathbb{Z}_p[x]^{n\times l}$ can be transformed into standard form using the following operations: (1) exchange two columns and (2) add the product of a column by an element from $\mathbb{Z}_p$ to another column. Equivalently, there exists an invertible matrix $U \in \mathbb{Z}_p^{l\times l}$ such that $E \cdot U = S$ is in standard form. Suppose that the first k columns of S are zero vectors. Then the first k columns of U constitute a basis for $\ker(E)$. This can be proved similarly to that of the algorithm to compute a basis for the kernel of a matrix over a PID (Cohen, 1993, page 74).

We now give the algorithm to compute the $\mathbb{Z}$-saturation.

Algorithm 4 — SatZ($\mathbf{f}_0, \ldots, \mathbf{f}_s$).

Input: A set of vectors $\mathbb{f} = \{\mathbf{f}_0, \ldots, \mathbf{f}_s\} \subset \mathbb{Z}[x]^n$.

Output: A reduced Gröbner basis $\mathbb{g}$ such that $(\mathbb{g}) = \mathrm{sat}_{\mathbb{Z}}(\mathbb{f})$.

1. Compute generalized Hermite normal form $\mathbb{g}$ of $\mathbb{f}$.
2. Set $S =$ **ZFactor**($\mathbb{g}$).
3. If $S = \emptyset$, return $\mathbb{g}$; otherwise set $\mathbb{f} = \mathrm{Col}(\mathbb{g}) \cup \{\mathbf{h} \mid (\mathbf{h}, k, \mathbf{f}) \in S\}$ and goto step 1.

Example 114. Let $\mathcal{C}$ be the following generalized Hermite normal form:

$$\mathcal{C} = \begin{bmatrix} x^2 + 2x - 2 & x + 2 & 1 \\ 0 & 4 & 2x \end{bmatrix}.$$

Then, $t=2, r_1=1, l_1=1, r_2=2, l_2=2, q=4$, $\mathbf{c}_{1,1}=[x^2+2x-2,0]^\tau$, $\mathbf{c}_{2,1}=[x+2,4]^\tau$, $\mathbf{c}_{2,2}=[1,2x]^\tau$. Apply algorithm **ZFactor** to $\mathcal{C}$. We have $p=2$. In steps 3.1 and 3.2, $F=\begin{bmatrix} x^2 & 1 \\ 0 & 0 \end{bmatrix}$ and $\ker(F)$ is generated by $G=\{[-1,x^2]^\tau\}$. In step 3.3, $x^2\mathbf{c}_{22}-\mathbf{c}_{11}=2(1-x,x^3)^\tau$ and return $(1-x,x^3)^\tau$.

In Algorithm **SatZ**, $(1-x,x^3)^\tau$ is added into $\mathcal{C}$ and

$$\mathcal{C}_1=\begin{bmatrix} x^2+2x-2 & x+2 & 1 & 1-x \\ 0 & 4 & 2x & x^3 \end{bmatrix},$$

which is also a generalized Hermite normal form.

Applying Algorithm **ZFactor** to $\mathcal{C}_1$. We have $p=2$ and $t=2$. In steps 3.1–3.3, $G=\emptyset$. In step 3.4, $\mathcal{B}=\begin{bmatrix} x^2 & 1-x \\ 0 & x^3 \end{bmatrix}$. In step 3.5, $\mathcal{C}_-=\begin{bmatrix} x+2 & 1 & x \\ 4 & 2x & 2x^2 \end{bmatrix}$ and $\widetilde{\mathbf{f}}_i\neq 0$ for all i. In step 3.7, $E=\begin{bmatrix} x & 1 & x \\ 0 & 0 & 0 \end{bmatrix}$. In Step 3.8, $D=\{\mathbf{b}\}$, where $\mathbf{b}=[1,0,-1]^\tau$. In Step 3.9, $(x+2,4)^\tau-(x,2x^2)^\tau=2(1,2-x^2)^\tau$. Add $(1,2-x^2)^\tau$ into $\mathcal{C}_1$ and compute the generalized Hermite normal form, we have

$$\mathcal{C}_2=\begin{bmatrix} x^2+2x-2 & x+2 & 1 & -1 \\ 0 & 4 & 2x & x^2-2 \end{bmatrix}.$$

Apply Algorithm **ZFactor** again, it is shown that $\mathcal{C}_2$ is $\mathbb{Z}$-saturated.

We will prove the correctness of the algorithm. We denote by $\mathrm{sat}_p(L)$ the set $\{\mathbf{f}\in\mathbb{Z}[x]^n \mid p\mathbf{f}\in L\}$ where $p\in\mathbb{N}$ is a prime number. An infinite set S is said to be *linearly independent* over a ring R if any finite set of S is linearly independent over R, that is $\sum_{i=1}^k a_i\mathbf{g}_i=0$ for $a_i\in R$ and $\mathbf{g}_i\in S$ implies $a_i=0, i=1,\ldots,k$.

Lemma 115. *Let $\mathcal{C}$ be a generalized Hermite normal form and $L=(\mathcal{C})$. Then $\mathrm{sat}_p(L)=L$ if and only if $\mathcal{C}_\infty$ is linearly independent over $\mathbb{Z}_p$, where $\mathcal{C}_\infty$ is defined in (9).*

Proof. "⇒" Assume the contrary, that is, $\mathcal{C}_\infty=\{\mathbf{h}_1,\mathbf{h}_2,\ldots\}$ defined in (9) is linearly dependent over $\mathbb{Z}_p$. Then there exist $a_i\in\mathbb{Z}_p$ not all zero, such that $\sum_{i=1}^r a_i\mathbf{h}_i=0$ in $\mathbb{Z}_p[x]^n$ and hence $\sum_{i=1}^r a_i\mathbf{h}_i=p\mathbf{g}$ in $\mathbb{Z}[x]^n$. By Lemma 12, $\mathbf{h}_i$ are linearly independent over $\mathbb{Z}_p$ and hence $\mathbf{g}\neq\mathbf{0}$. Since $\mathrm{sat}_p(L)=L$, we have $\mathbf{g}\in L$. By Lemma 13, there exist $b_i\in\mathbb{Z}$ such that $\mathbf{g}=\sum_{i=1}^r b_i\mathbf{h}_i$. Hence $\sum_{i=1}^r(a_i-pb_i)\mathbf{h}_i=0$ in $\mathbb{Z}[x]^n$. By Lemma 12, $a_i=pb_i$ and hence $a_i=0$ in $\mathbb{Z}_p[x]$, a contradiction.

"⇐" Assume the contrary, that is, there exists a $\mathbf{g}\in\mathbb{Z}[x]^n$, such that $\mathbf{g}\notin L$ and $p\mathbf{g}\in L$. By Lemma 13, $p\mathbf{g}=\sum_{i=1}^r a_i\mathbf{h}_i$, where $a_i\in\mathbb{Z}$. p cannot be a factor of all a_i. Otherwise, $\mathbf{g}=\sum_{i=1}^r\frac{a_i}{p}\mathbf{h}_i\in L$. Then some of a_i is not zero in $\mathbb{Z}_p$, which means $\sum_{i=1}^r a_i\mathbf{h}_i=0$ is nontrivial linear relation among $\mathcal{C}_i$ over $\mathbb{Z}_p$, a contradiction. □

From the "⇒" part of the above proof, we have

Corollary 116. *Let $\sum_{i=1}^r a_i\mathbf{h}_i=0$ be a nontrivial linear relation among $\mathbf{h}_i$ in $\mathbb{Z}_p[x]^n$, where $a_i\in\mathbb{Z}_p$. Then, in $\mathbb{Z}[x]^n$, $\sum_{i=1}^r a_i\mathbf{h}_i=p\mathbf{h}$ and $\mathbf{h}\notin(\mathcal{C})$.*

Lemma 117. *Let $\mathcal{C}=[\mathbf{c}_1,\ldots,\mathbf{c}_s]$ be a generalized Hermite normal form and $L=(\mathcal{C})$. Then $\mathrm{sat}_p(L)=L$ if and only if $\mathcal{C}_\infty$ is linearly independent over $\mathbb{Z}_p$ for the prime factors of q defined in step 2 of Algorithm* **ZFactor**.

Proof. By Definition 7, the leading monomial of $x^k\mathbf{c}_{r_i,j}\in\mathcal{C}_\infty$ is of the form $c_{r_i,j,0}x^{k+d_{r_i,j}}\boldsymbol{\epsilon}_{r_i}$ and $c_{r_i,l_i,0}|\ldots|c_{r_i,2,0}\ |c_{r_i,1,0}$. If p is coprime with $\prod_{i=1}^t c_{r_i,1,0}$, then $c_{r_i,j,0}\neq 0 \bmod p$ for $1\le j\le l_i$. Therefore, the leading monomials of the elements of $\mathcal{C}_\infty$ are linearly independent over $\mathbb{Z}_p$, and hence $\mathcal{C}_\infty$ is linearly independent over $\mathbb{Z}_p$. Therefore, it suffices to consider prime factors of $\prod_{i=1}^t c_{r_i,1,0}$. □

To check whether $\mathcal{C}_\infty$ is linearly independent over $\mathbb{Z}_p$, we first consider a subset of $\mathcal{C}_\infty$ in the following lemma.

Lemma 118. *Let $\mathcal{C}$ be the generalized Hermite normal form given in (7). Then $\mathcal{C}^+$ defined in (9) is linearly independent over $\mathbb{Z}_p$ if and only if $\{\mathbf{c}_{r_1,l_1}, \mathbf{c}_{r_2,l_2}, \ldots, \mathbf{c}_{r_t,l_t}\}$ are linearly independent over $\mathbb{Z}_p[x]$.*

Proof. This is obvious since $\sum_i \sum_j a_{i,j} x^j \mathbf{c}_{r_i,l_i} = \sum_i p_i \mathbf{c}_{r_i,l_i}$, where $a_{i,j} \in \mathbb{Z}$ and $p_i = \sum_j a_{i,j} x^j$. □

Lemma 119. *Let $\mathcal{B}$ be a Hermite normal form in $\mathbb{Z}_p[x]^n$ and $\mathcal{G} = \{\mathbf{g}_1, \ldots, \mathbf{g}_r\} \subset \mathbb{Z}_p[x]^n$. Then $\mathcal{G} \cup \mathcal{B}_\infty$ is linearly dependent over $\mathbb{Z}_p$ if and only if*

- *either $\widetilde{\mathbf{g}}_i = \mathrm{grem}(\mathbf{g}_i, \mathcal{B}) = 0$ in $\mathbb{Z}_p[x]^n$ for some i, or*
- *the residue set $\{\mathrm{grem}(\mathbf{g}_i, \mathcal{B}) \mid i = 1, \ldots, r\}$ are linearly dependent over $\mathbb{Z}_p$.*

Proof. We may assume that $\mathrm{grem}(\mathbf{g}_i, \mathcal{B}) = 0$ does not happen, since it gives a nontrivial linear relation of $\mathcal{G} \cup \mathcal{B}_\infty$. By Lemma 13, $\widetilde{\mathbf{g}}_i = \mathbf{g}_i \bmod \mathcal{B}_\infty$. $\mathcal{G} \cup \mathcal{B}_\infty$ is linearly dependent over $\mathbb{Z}_p$ if and only if there exist $a_i \in \mathbb{Z}_p$ not all zero such that $\sum_i a_i \mathbf{g}_i = 0 \bmod \mathcal{B}_\infty$ over $\mathbb{Z}_p$, which is valid if and only if $\sum_i a_i \widetilde{\mathbf{g}}_i = 0 \bmod \mathcal{B}_\infty$. Since $\widetilde{\mathbf{g}}_i$ are G-reduced with respect to $\mathcal{B}$, $\sum_i a_i \widetilde{\mathbf{g}}_i = 0 \bmod \mathcal{B}_\infty$ if and only if $\sum_i a_i \widetilde{\mathbf{g}}_i = 0$, that is $\widetilde{\mathbf{g}}_i$ are linearly dependent over $\mathbb{Z}_p$. □

Proposition 120. *Algorithm* **SatZ** *is correct.*

Proof. Since $\mathbb{Z}[x]^n$ is Noetherian, the algorithm terminates and it suffices to show that Algorithm **ZFactor** is correct. Let $\mathcal{C} = [\mathbf{c}_1, \ldots, \mathbf{c}_s]$. By Lemma 115, to check whether $(\mathbf{c}_1, \ldots, \mathbf{c}_s)$ is $\mathbb{Z}$-saturated, it suffices to check for any prime p, $\mathcal{C}_\infty$ is linearly independent on $\mathbb{Z}_p$. Furthermore, by Lemma 117, it suffices to consider prime factors of $\prod_{i=1}^t c_{r_i,1,0}$ in step 3. This explain why only prime factors of q are considered in Step 3.

In steps 3.1 and 3.2, we check whether $\mathcal{C}^+$ in (9) is linearly independent over $\mathbb{Z}_p$. By Lemma 118, we need only to consider whether $\mathcal{C}_1 = \{\mathbf{c}_{r_1,l_1}, \mathbf{c}_{r_2,l_2}, \ldots, \mathbf{c}_{r_t,l_t}\}$ is linearly independent over $\mathbb{Z}_p[x]$. It is clear that $\mathcal{C}_1$ is linearly independent over $\mathbb{Z}_p[x]$ if and only if $G = \emptyset$, where G is given in step 3.2.

In step 3.3, $\mathcal{C}_1$ is linearly dependent over $\mathbb{Z}_p$. If $G \neq \emptyset$ for any $\mathbf{g} = [g_1, \ldots, g_t]^\tau \in G$, $\sum_{i=1}^t g_i \mathbf{c}_{r_i,l_i} = 0$ in $\mathbb{Z}_p[x]$. Hence $\sum_{i=1}^t g_i \mathbf{c}_{r_i,l_i} = p\mathbf{h}$ where $\mathbf{h} \in \mathbb{Z}[x]^n$. By Corollary 116, $\mathbf{h} \notin L$. The correctness of Algorithm **ZFactor** is proved in this case.

In steps 3.4 - 3.10, we handle the case where $\mathcal{C}^+$ is linearly independent over $\mathbb{Z}_p$. In step 3.4, we compute the Hermite normal form of $\mathcal{C}_1$ in $\mathbb{Z}_p[x]^n$, which is possible because $\mathbb{Z}_p[x]^n$ is a PID (Cohen, 1993). Furthermore, we have (Cohen, 1993)

$$[\mathbf{c}_{r_1,l_1}, \ldots, \mathbf{c}_{r_t,l_t}]N = [\mathbf{b}_1, \ldots, \mathbf{b}_t]$$

where $\{\mathbf{b}_1, \ldots, \mathbf{b}_t\}$ is a Hermite normal form and N is an invertible matrix in $\mathbb{Z}_p[x]^{t\times t}$. Then $\mathcal{C}_\infty = \mathcal{C}_- \cup \mathcal{C}^+$ is linearly independent over $\mathbb{Z}_p$ if and only if

$$\widetilde{\mathcal{C}} = \mathcal{C}_- \cup \mathcal{B}_\infty = \mathcal{C}_- \cup \cup_{j=0}^\infty \{x^j \mathbf{b}_1, \ldots, x^j \mathbf{b}_t\} \text{ is linearly independent over } \mathbb{Z}_p. \tag{41}$$

By Lemma 119, property (41) is valid if and only if $\mathrm{grem}(\mathbf{c}, \mathcal{B}) \neq 0$ for all $\mathbf{c} \in \mathcal{C}_-$ and the residue set $\widetilde{\mathcal{C}}_-$ is linearly independent over $\mathbb{Z}_p$, which are considered in step 3.7 and steps 3.8–3.10, respectively. Then we either prove L is $\mathbb{Z}$-saturated or find a nontrivial linear relation for elements in $\mathcal{C}_\infty$ over $\mathbb{Z}_p$. By Corollary 116, such a relation leads to an $\mathbf{h} \in \mathrm{sat}_{\mathbb{Z}}(L) \setminus L$. The correctness of the algorithm is proved. □

As a direct consequence of Lemma 55 and Algorithm **ZFactor**, we have the algorithm to compute the M-saturation.

Algorithm 5 — SatM($\mathbf{f}_0, \ldots, \mathbf{f}_s$).

Input: A set of vectors $\mathbb{f} = \{\mathbf{f}_0, \ldots, \mathbf{f}_s\} \subset \mathbb{Z}[x]^n$.
Output: A generalized Hermite normal form $\mathbb{g}$ such that $\mathrm{sat}_M(\mathbb{f}) = (\mathbb{g})$.

1. Using Algorithm **ZFactor**, we can compute $m_i \in \mathbb{N}$ and $\mathbf{g}_i \in \mathbb{Z}[x]^n$, $i = 1, \ldots, s$ such that $\mathrm{sat}_{\mathbb{Z}}(\mathbb{f}) = (\mathbf{g}_1, \ldots, \mathbf{g}_s)$ and $m_i\mathbf{g}_i \in (\mathbb{f})$.
2. Let $S = \emptyset$ and for $i = 1, \ldots, s$, if $m_i \neq 1$ then $S = S \cup \{(x - o_{m_i})\mathbf{g}_i\}$.
3. Compute the generalized Hermite normal form $\mathbb{g}$ of $\mathbb{f} \cup S$ and return $\mathbb{g}$.

Proposition 121. *Algorithm* **SatM** *is correct.*

Proof. Notice that if $m_i = 1$ then $o_{m_i} = 0$ and $\mathbf{g}_i \in (\mathbb{f})$. Let $L_1 = (\mathbb{f})$ and $L_2 = (\mathbb{f}, (x - o_{m_1})\mathbf{g}_1, \ldots, (x - o_{m_s})\mathbf{g}_s)$. We claimthat $\mathrm{sat}_{\mathbb{Z}}(L_1) = \mathrm{sat}_{\mathbb{Z}}(L_2)$. Since $L_1 \subset L_2$, $\mathrm{sat}_{\mathbb{Z}}(L_1) \subset \mathrm{sat}_{\mathbb{Z}}(L_2)$. Since $\mathrm{sat}_{\mathbb{Z}}(L_1) = (\mathbf{g}_1, \ldots, \mathbf{g}_s)$, we have $L_2 \subset \mathrm{sat}_{\mathbb{Z}}(L_1)$ and hence $\mathrm{sat}_{\mathbb{Z}}(L_2) \subset \mathrm{sat}_{\mathbb{Z}}(L_1)$. The claim is proved. Then $\mathrm{sat}_{\mathbb{Z}}(L_2) = (\mathbf{g}_1, \ldots, \mathbf{g}_s)$ and $m_i\mathbf{g}_i \in L_1 \subset L_2$. Since $(x - o_{m_i})\mathbf{g}_i \in L_2, i = 1, \ldots, s$, L_2 is M-saturated by Lemma 55. □

7.3. Algorithms for Laurent binomial and binomial σ-ideals

In this section, we will present several algorithms for Laurent binomial and binomial σ-ideals, and in particular a decomposition algorithm for binomial σ-ideals. We first give an algorithm to compute the characteristic set for a Laurent binomial σ-ideal.

Algorithm 6 — CharSet.

Input: F: a finite set of Laurent σ-binomials in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$.
Output: $\emptyset$, if $[F] = [1]$; otherwise, a regular and coherent Laurent binomial σ-chain $\mathcal{A}$ such that $[\mathcal{A}] = [F]$ and $\mathcal{A}$ is a characteristic set of the σ-ideal $[F]$.

1. Let $F = \{\mathbb{Y}^{\mathbf{f}_1} - c_1, \ldots, \mathbb{Y}^{\mathbf{f}_r} - c_r\}$ and $\mathbb{f} = \{\mathbf{f}_1, \ldots, \mathbf{f}_r\}$.
2. Compute a set of generators $H \subset \mathbb{Z}[x]^r$ of $\ker_{\mathbb{Z}[x]}([\mathbf{f}_1, \ldots, \mathbf{f}_r])$ with Algorithm **GKER**.
3. If there exists an $\mathbf{h} = (h_1, \ldots, h_r)^{\tau} \in H$ such that $\prod_{i=1}^{r} c_i^{h_i} \neq 1$, then return $\emptyset$.
4. Compute the reduced Gröbner basis $\mathbb{g}$ of $\mathbb{f}$ with Algorithm **GHNF**.
5. Let $\mathbb{g} = \{\mathbf{g}_1, \ldots \mathbf{g}_s\}$ and $\mathbf{g}_i = \sum_{k=1}^{r} a_{i,k}\mathbf{f}_k$, where $a_{i,k} \in \mathbb{Z}[x]$, $i = 1, \ldots, s$.
6. Return $\mathcal{A} = \{g_1, \ldots, g_s\}$, where $g_i = \mathbb{Y}^{\mathbf{g}_i} - d_i$ and $d_i = \prod_{k=1}^{r} c_k^{a_{i,k}}$, $i = 1, \ldots, s$.

Proposition 122. *Algorithm* **CharSet** *is correct.*

Proof. Steps 1–3 uses Proposition 19 to check whether $[F] = [1]$. Note that $(\mathbb{f})$ and $(\mathbb{g})$ are the support lattices of the binomial σ-ideals $[F]$ and $[G]$, respectively. By Corollary 18, $[F] = [G]$. By Theorem 29, $\mathcal{A}$ is a regular and coherent σ-chain and hence a characteristic set of $[\mathcal{A}]$. □

We now show how to compute the reflexive closure for a Laurent binomial σ-ideal.

Algorithm 7 — Reflexive.

Input: P: a finite set of Laurent σ-binomials in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$, where $\mathcal{F}$ is inversive.
Output: $\mathcal{A}$: a regular and coherent Laurent binomial σ-chain such that $[\mathcal{A}]$ is the reflexive closure of $[P]$.

1. Let $G = \mathbf{CharSet}(P)$. If $G = \emptyset$, return 1.
2. Let $G = \{g_1, \ldots, g_s\}$, $g_i = \mathbb{Y}^{\mathbf{g}_i} - d_i$, and $\mathbb{g} = [\mathbf{g}_1, \ldots, \mathbf{g}_s] \in \mathbb{Z}[x]^{n \times s}$.
3. $H = \mathbf{XFactor}(\mathbb{g})$.
4. If $H = \emptyset$, return G.
5. Let $H = \{(\mathbf{h}_i, \mathbf{e}_i) \mid i = 1, \ldots, r\}$ and $\mathbf{e}_i = (e_{i1}, \ldots, e_{is})^{\tau}$.
6. Let $P := G \cup \{\mathbb{Y}^{\mathbf{h}_i} - \sigma^{-1}(\prod_{j=1}^{s} d_j^{e_{i,j}}), i = 1, \ldots, r\}$, and go to step 1.

Proposition 123. *Algorithm* **Reflexive** *is correct.*

Proof. The algorithm basically follows the proof of Theorem 40. In step 1, by **CharSet**, $[P]=[G]$ and G is a regular and coherent σ-chain. In step 4, if $H=\emptyset$, then $(\mathfrak{g})$ is x-saturated, and by Theorem 37, $[G]$ is reflexive and the proposition is proved. Otherwise, we execute steps 5 and 6. Let $\mathcal{I}_1=[P]$, $L_1=(\mathfrak{f})$, $\mathcal{I}_2=[G\cup\{\mathbb{Y}^{\mathbf{h}_i}-\sigma^{-k_i}(\prod_{j=1}^{s}d_j^{e_{i,j}}), i=1,\ldots,r\}]$, and $L_2=\mathbb{L}(\mathcal{I}_2)$. Then, we have $\mathcal{I}_1\subsetneq\mathcal{I}_2\subset\mathcal{I}_x$ and $L_1\subsetneq L_2\subset L_x$, where $L_x=\mathrm{sat}_x(L_1)$ and $\mathcal{I}_x$ is the reflexive closure of $\mathcal{I}_1$. Similar to the proof of Theorem 40, the algorithm will terminate and output the reflexive closure of $[P]$. □

Remark 124. Similar to Algorithm **Reflexive**, we can give algorithms to check whether a Laurent binomial σ-ideal $\mathcal{I}$ is well-mixed, perfect, or prime, and in the negative case to compute the well-mixed or perfect closures of $\mathcal{I}$. The details are omitted.

We give a decomposition algorithm for perfect Laurent binomial σ-ideals.

Algorithm 8 — DecLaurent.

Input: P: a finite set of Laurent σ-binomials in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$, where $\mathcal{F}$ is inversive and algebraically closed.

Output: $\emptyset$, if $\{P\}=[1]$ or regular and coherent binomial σ-chains $\mathcal{C}_1,\ldots,\mathcal{C}_t$ such that $[\mathcal{C}_i]$ are Laurent reflexive prime σ-ideals and $\{P\}=\cap_{i=1}^{t}[\mathcal{C}_i]$ is a minimal decomposition.

1. Let $F=$ **Reflexive**(P). If $F=1$, return $\emptyset$.
2. Set $\mathbb{R}=\emptyset$ and $\mathbb{F}=\{F\}$.
3. While $\mathbb{F}\neq\emptyset$.
   - 3.1. Let $F=\{\mathbb{Y}^{\mathbf{f}_1}-c_1,\ldots,\mathbb{Y}^{\mathbf{f}_r}-c_r\}\in\mathbb{F}$, $\mathbb{F}=\mathbb{F}\setminus\{F\}$.
   - 3.2. Let $G=$ **CharSet**(F). If $G=\emptyset$, goto step 3.
   - 3.3. Let $G=\{g_1,\ldots,g_s\}$, $g_i=\mathbb{Y}^{\mathbf{g}_i}-d_i$, and $\mathfrak{g}=[\mathbf{g}_1,\ldots,\mathbf{g}_s]\in\mathbb{Z}[x]^{n\times s}$.
   - 3.4. $H=$ **ZFACTOR**$(\mathfrak{g})$.
   - 3.5. If $H=\emptyset$, add G to $\mathbb{R}$.
   - 3.6. Let $H=\{(\mathbf{h}_i,k_i,\mathbf{e}_i)\mid i=1,\ldots,r\}$ and $\mathbf{e}_i=(e_{i1},\ldots,e_{is})^{\tau}$.
   - 3.7. For $i=1,\ldots,t$, let $r_{i,1},\ldots,r_{i,k_i}$ be the k_i-th roots of $\prod_{j=1}^{s}d_j^{e_{i,j}}$.
   - 3.8. For $l_1=1,\ldots,k_1,\ldots,l_t=1,\ldots,k_t$, add $G\cup\{\mathbb{Y}^{\mathbf{h}_1}-r_{1,l_1},\ldots,\mathbb{Y}^{\mathbf{h}_t}-r_{t,l_t}\}$ to $\mathbb{F}$.
4. Return $\mathbb{R}$.

Example 125. Let $P=\{g_1,g_2,g_3\}$, where $g_1=y_1^{-2}y_1^{x^k}-1$, $g_2=y_2^{-2}y_2^{x^k}-1$, $g_3=y_1y_2^{-x}y_3^2-1$, and $k\geq 2$. $[P]$ is already reflexive, so step 1 does nothing. P is already a regular and coherent σ-chain, so $G=P$. Let $\mathbf{g}_1=[x^k-2,0,0]^{\tau},\mathbf{g}_2=[0,x^k-2,0]^{\tau},\mathbf{g}_3=[1,-x,2]^{\tau}$ be the supports of g_1, g_2, and g_3, respectively. Then $[\mathbf{g}_1,\mathbf{g}_2,\mathbf{g}_3]$ is already a generalized Hermite normal form.

In Steps 3.4–3.6, $H=\{(\mathbf{h}_1,k_1,\mathbf{e}_1)\}$, where $\mathbf{h}_1=[1,-x,x^k]^{\tau},k_1=2,\mathbf{e}_1=[-1,x,x^k]^{\tau}$. In Step 3.7, $r_{1,1}=1$ and $r_{1,2}=-1$. In Step 3.8, $P_1=y_1y_2^{-x}y_3^{x^k}-1$ and $P_2=y_1y_2^{-x}y_3^{x^k}+1$ are added to G to obtain $\mathcal{C}_1=\{g_1,g_2,g_3,P_1\}$ and $\mathcal{C}_2=\{g_1,g_2,g_3,P_2\}$. Both $[\mathcal{C}_1]$ and $[\mathcal{C}_2]$ are reflexive and prime, and are returned.

To see why the algorithm is correct, from $\mathbf{e}_1=[-1,x,x^k]$, we have $(g_1+1)^{-1}(g_2+1)^{x}(g_3+1)^{x^k}=y_1^2y_2^{-2x}y_3^{2x^k}=1\bmod[P]$. Hence, $P_1P_2=y_1^2y_2^{-2x}y_3^{2x^k}-1\in[P]$.

Proposition 126. *Algorithm* **DecLaurent** *is correct.*

Proof. The algorithm basically follows the proof of Theorem 42. The proof is similar to that of Theorem 123. In the proof of Theorem 42, $\mathcal{I}_{il_1}\not\subset\mathcal{I}_{il_2}$ for any i and $l_1\neq l_2$. Then, we obtain a minimal decomposition. □

In the rest of this section, we give a decomposition algorithm for binomial σ-ideals. Before giving the main algorithm, we give a sub-algorithm **DecMono** which treats the σ-monomials. Basically, it gives the following decomposition

$$\mathbb{V}(\prod_{i=1}^{n}y_i^{f_i})=\mathbb{V}(y_1)\cup\mathbb{V}(y_2/\{y_1\})\cup\cdots\cup\mathbb{V}(y_n/\{y_1,\ldots,y_{n-1}\})$$

where $0 \neq f_i \in \mathbb{N}[x]$ and $\mathbb{V}(y_c/S)$ is the set of zeros of $y_c = 0$ not vanishing any of the variables in S. The correctness of the algorithm comes directly from the above formula.

Algorithm 9 — DecMono.

Input: $(\mathbb{Y}_0, B, \mathbb{Y}_1)$: $\mathbb{Y}_0, \mathbb{Y}_1$ are disjoint subsets of $\mathbb{Y}$ and B a finite set of σ-binomials or σ-monomials in $\mathcal{F}\{\mathbb{Y}\}$.

Output: $(\mathbb{Y}_{0i}, B_i, \mathbb{Y}_{1i})$: $\mathbb{Y}_{0i}, \mathbb{Y}_{1i}$ are disjoint subsets of $\mathbb{Y}$, B_i consists of proper σ-binomials, and $\mathbb{V}(\mathbb{Y}_0 \cup B/\mathbb{Y}_1) = \cup_{i=1}^{r} \mathbb{V}(\mathbb{Y}_{0i} \cup B_i/\mathbb{Y}_{1i})$.

1. Set $\mathbb{R} = \emptyset$ and $\mathbb{F} = \{(\mathbb{Y}_0, B, \mathbb{Y}_1)\}$.
2. While $\mathbb{F} \neq \emptyset$.
   2.1. Let $C = (\mathbb{Y}_0, B, \mathbb{Y}_1) \in \mathbb{F}$, $\mathbb{F} = \mathbb{F} \setminus \{C\}$.
   2.2. For all $y_c \in \mathbb{Y}_0$, let $B_1 = B_{y_c=0}$ (replace y_c^k by 0) and delete 0 from B_1.
   2.3. If B_1 contains no σ-monomials, add $(\mathbb{Y}_0, B_1, \mathbb{Y}_1)$ to $\mathbb{R}$ and goto step 2.
   2.4. Let $M = \prod_{i=1}^{k} y_{c_i}^{f_i} \in B_1$, where $0 \neq f_i \in \mathbb{N}[x]$. $B_1 = B_1 \setminus \{M\}$.
   2.5. Let $\mathbb{Y}_2 := \{y_{c_1}, \ldots, y_{c_k}\} \setminus \mathbb{Y}_1$. If $\mathbb{Y}_2 = \emptyset$, go to step 2; else let $\mathbb{Y}_2 = \{y_{t_1}, \ldots, y_{t_s}\}$.
   2.6. For $i = 1, \ldots, s$, add $(\mathbb{Y}_0 \cup \{y_{t_i}\}, B_1, \mathbb{Y}_1 \cup \{y_{t_1}, \ldots, y_{t_{i-1}}\})$ to $\mathbb{F}$.
3. Return $\mathbb{R}$.

Example 127. Let $\mathbb{Y} = \{y_1, y_2, y_3, y_4\}$, $\mathbb{Y}_0 = \{y_1\}$, $\mathbb{Y}_1 = \{y_2\}$, $B = \{p\}$, where $p = y_1y_3 - y_2y_3y_4$. In step 2.2, we have $y_c = y_1$ and $\mathbb{V}(\{y_1, p\}/\{y_2\}) = \mathbb{V}(\{y_1, y_2y_3y_4\}/\{y_2\})$. In step 2.5, $\mathbb{Y}_2 = \{y_2, y_3, y_4\} \setminus \{y_2\} = \{y_3, y_4\}$, which implies $\mathbb{V}(\{y_1, y_2y_3y_4\}/\{y_2\}) = \mathbb{V}(\{y_1, y_3y_4\}/\{y_2\})$. In step 2.6, we have $\mathbb{V}(\{y_1, y_3y_4\}/\{y_2\}) = \mathbb{V}(\{y_1, y_3\}/\{y_2\}) \cup \mathbb{V}(\{y_1, y_4\}/\{y_2, y_3\})$. The output is $(\{y_1, y_3\}, \emptyset, \{y_2\})$ and $(\{y_1, y_4\}, \emptyset, \{y_2, y_3\})$.

We now give the main algorithm.

Algorithm 10 — DecBinomial.

Input: F: a finite set of σ-binomials in $\mathcal{F}\{\mathbb{Y}\}$.

Output: $\emptyset$, if $\{F\} = [1]$ or $(\mathcal{C}_1, \mathbb{Y}_1), \ldots, (\mathcal{C}_r, \mathbb{Y}_r)$, where $\mathbb{Y}_i \subset \mathbb{Y}$ and $\mathcal{C}_i$ are regular and coherent σ-chains containing σ-binomials or variables in $\mathbb{Y} \setminus \mathbb{Y}_i$ such that $\mathrm{sat}(\mathcal{C}_i)$ are reflexive prime σ-ideals and $\{F\} = \cap_{i=1}^{r} \mathrm{sat}(\mathcal{C}_i)$.

1. Set $\mathbb{R} = \emptyset$ and $\mathbb{F} = \textbf{DecMono}(\emptyset, F, \emptyset)$.
2. While $\mathbb{F} \neq \emptyset$.
   2.1. Let $C = (\mathbb{Z}_0, B, \mathbb{Z}_1) \in \mathbb{F}$, $\mathbb{F} = \mathbb{F} \setminus \{C\}$.
   2.2. If $B = \emptyset$, add $(\mathbb{Z}_0, \mathbb{Z}_1)$ to $\mathbb{R}$.
   2.3. Let $E = \textbf{DecLaurent}(B)$ in $\mathcal{F}\{\mathbb{Z}^{\pm}\}$, where $\mathbb{Z} = \mathbb{Y} \setminus \mathbb{Z}_0$ and $m = |\mathbb{Z}|$.
   2.4. If $E = \emptyset$ goto step 2.
   2.5. Let $E = \{E_1, \ldots, E_l\}$ and $E_l = \{\mathbb{Z}^{\mathbf{f}_{l,1}} - c_{l,1}, \ldots, \mathbb{Z}^{\mathbf{f}_{l,s_l}} - c_{l,s_l}\}$, where $\mathbf{f}_{l,k} \in \mathbb{Z}[x]^m$.
   2.7. Add $(\{\mathbb{Z}_0, \mathbb{Z}^{\mathbf{f}^+_{l,1}} - c_{l,1}\mathbb{Z}^{\mathbf{f}^-_{l,1}}, \ldots, \mathbb{Z}^{\mathbf{f}^+_{l,s_l}} - c_{l,s_l}\mathbb{Z}^{\mathbf{f}^-_{l,s_l}}\}, \mathbb{Z}_1)$ to $\mathbb{R}$, $l = 1, \ldots, k$.
   2.8. Let $\mathbb{Z} = \{y_{c_1}, \ldots, y_{c_s}\}$. For $i = 1, \ldots, s$, do
   $\mathbb{F} = \mathbb{F} \cup \textbf{DecMono}(\mathbb{Z}_0 \cup \{y_{c_i}\}, B, \mathbb{Z}_1 \cup \{y_{c_1}, \ldots, y_{c_{i-1}}\})$.
3. Return $\mathbb{R}$.

The algorithm basically follows the proof of Theorem 91. The main modification is that instead of the perfect σ-ideal decomposition $\{F\} = (\{F\} : \mathfrak{m}) \cap \bigcap_{i=1}^{n} \{F, y_i\}$, we use the following zero decomposition

$$\mathbb{V}(F) = \mathbb{V}(\{F\} : \mathfrak{m}) \cup \bigcup_{i=1}^{n} \mathbb{V}(F \cup \{y_i\}/\{y_1, \ldots, y_{i-1}\}).$$

The purpose of using the later decomposition is that many redundant components can be easily removed by the following criterion $\mathbb{V}(F/D) = \emptyset$ if $F \cap D \neq \emptyset$, which is done in step 2.5 of Algorithm **DecMono**.

Example 128. Let $\mathcal{A} = \{A_1, A_2, A_3\}$, where $A_1 = y_1^k - y_1^2$, $A_2 = y_2^k - y_2^2$, $A_3 = y_1y_3^2 - y_2^x$, and $k \geq 2$. In Step 1, we have $\mathbb{F} = \{(\emptyset, \mathcal{A}, \emptyset)\}$. From Example 125, in Step 2.3, we have $E = \{\mathcal{C}_1, \mathcal{C}_2\}$, where

$\mathcal{C}_1$ and $\mathcal{C}_2$ are given in Example 125. In Step 2.7, $(E_1, \emptyset)$ and $(E_2, \emptyset)$ are added to $\mathbb{R}$, where $E_1 = \{A_1, A_2, A_3, Q_1\}$, $E_2 = \{A_1, A_2, A_3, Q_2\}$, and $Q_1 = y_1 y_3^k - y_2^x$, $Q_2 = y_1 y_3^k + y_2^x$. In Step 2.8, $\mathbb{Z} = \{y_1, y_2, y_3\}$ and $(\{y_1, y_2\}, \emptyset, \emptyset)$, $(\{y_2, y_3\}, \{A_1\}, \{y_1\})$ are added to $\mathbb{F}$. Finally, we have the following decomposition $\{\mathcal{A}\} = [y_1, y_2] \cap [A_1, y_2, y_3] \cap \mathrm{sat}(\mathcal{C}_1) \cap \mathrm{sat}(\mathcal{C}_2)$, where all components are reflexive and prime.

Remark 129. Using the algorithm in Gao et al. (2009a), the following decomposition is obtained: $\{\mathcal{A}\} = [y_1, y_2] \cap \mathrm{sat}(\mathcal{A})$. From Example 125, $\mathrm{sat}(\mathcal{A})$ is not prime. Then, Algorithm **DecBinomial** is stronger than the general decomposition algorithm given in Gao et al. (2009a).

Proposition 130. *Algorithm* **DecBinomial** *is correct.*

Proof. In step 1, σ-monomials in F are treated. In step 2, we will treat the components of $\mathbb{F}$ one by one. In step 2.1, the component $(\mathbb{Z}_0, B, \mathbb{Z}_1)$ is taken from $\mathbb{F}$. In step 2.3, $\{B\}$ is decomposed as $\{B\} = \cap_{l=1}^k [E_l]$ in $\mathcal{F}\{\mathbb{Z}^{\pm}\}$, where E_l are Laurent regular and coherent σ-chains and $[E_l]$ are reflexive prime σ-ideals. By (32) and Corollary 94, we have

$$\{B\} : \mathbb{m} = \{B\} \cap \mathcal{F}\{\mathbb{Z}\} = \cap_{l=1}^k ([E_l]\mathcal{F}\{\mathbb{Z}^{\pm}\}) \cap \mathcal{F}\{\mathbb{Y}\} = \cap_{l=1}^k \mathrm{sat}(E_l^+), \tag{42}$$

where $E_l^+ = \{\mathbb{Z}^{\mathbf{f}_{l,1}^+} - c_{l,1}\mathbb{Z}^{\mathbf{f}_{l,1}^-}, \ldots, \mathbb{Z}^{\mathbf{f}_{l,s_l}^+} - c_{l,s_l}\mathbb{Z}^{\mathbf{f}_{l,s_l}^-}\}$, $l = 1, \ldots, k$. Since E_l is regular and coherent, by Lemma 98, E_l^+ is also regular and coherent. Since $[E_l]$ is reflexive and prime, by Corollary 95, $\mathrm{sat}(E_l^+)$ is also reflexive and prime. Note that $E = \emptyset$ in step 2.4 if and only if $[B]$ contains a σ-monomial.

Since $B \subset \mathcal{F}\{\mathbb{Z}\}$, we have the following decomposition

$$\mathbb{V}(\mathbb{Z}_0 \cup B/\mathbb{Z}_1) = \mathbb{V}(\mathbb{Z}_0 \cup (\{B\} : \mathbb{m})/\mathbb{Z}_1) \cup_{i=1}^s \mathbb{V}(\mathbb{Z}_0 \cup B \cup \{y_{c_i}\}/\{y_{c_1}, \ldots, y_{c_{i-1}}\} \cup \mathbb{Z}_1),$$

where $\mathbb{V}(\mathbb{Z}_0 \cup B \cup \{y_{c_i}\}/\{y_{c_1}, \ldots, y_{c_{i-1}}\} \cup \mathbb{Z}_1)$ is further simplified with Algorithm **DecMono** in step 2.8. From (42),

$$\mathbb{V}(\mathbb{Z}_0 \cup \{B\} : \mathbb{m}/\mathbb{Z}_1) = \cup_{l=1}^k \mathbb{V}(\mathrm{sat}(\mathbb{Z}_0, E_l^+)/\mathbb{Z}_1) = \cup_{l=1}^k \mathbb{V}([\mathbb{Z}_0, \mathrm{sat}(E_l^+)]/\mathbb{Z}_1),$$

where $\{\mathbb{Z}_0, E_l^+\}$ is a regular and coherent σ-chain since E_l^+ does not contain variables in $\mathbb{Z}_0$. The above formula explains why $(\{\mathbb{Z}_0, E_l^+\}, \mathbb{Z}_1)$ is added to $\mathbb{R}$ in steps 2.5–2.7.

Let the algorithm returns $\mathbb{R} = \{(\mathcal{C}_i, \mathbb{Y}_i); i = 1, \ldots, m\}$. From the above proof, we have $\mathbb{V}(F) = \cup_{i=1}^k \mathbb{V}(\mathrm{sat}(\mathcal{C}_i)/\mathbb{Y}_i)$. Since $\mathbb{Y}_i \cap \mathcal{C}_i = \emptyset$ and $\mathrm{sat}(\mathcal{C}_i)$ is a reflexive and prime σ-ideal, the Cohn closure of $\mathbb{V}(\mathrm{sat}(\mathcal{C}_i)/\mathbb{Y}_i)$ is $\mathbb{V}(\mathrm{sat}(\mathcal{C}_i))$ and hence

$$\mathbb{V}(F) = \cup_{i=1}^k \mathbb{V}(\mathrm{sat}(\mathcal{C}_i)/\mathbb{Y}_i) = \cup_{i=1}^k \mathbb{V}(\mathrm{sat}(\mathcal{C}_i)).$$

By the difference Nullstellensatz, $\{F\} = \cap_{i=1}^k \{\mathrm{sat}(\mathcal{C}_i)\} = \cap_{i=1}^k \mathrm{sat}(\mathcal{C}_i)$. The algorithm terminates, since after each execution of step 2, in the new components $(\mathbb{Y}_{0l}, B_l, \mathbb{Y}_{1l})$ added to $\mathbb{F}$ in step 2.8, B_l contains at least one less variables than B. □

8. Conclusion

In this paper, we initiate the study of binomial σ-ideals. Two basic tools used to study binomial σ-ideals are the $\mathbb{Z}[x]$-lattice and the characteristic set instead of the $\mathbb{Z}$-lattice and the Gröbner basis used in the algebraic case (Eisenbud and Sturmfels, 1996).

For Laurent binomial σ-ideals, two main results are proved. Canonical representations for proper Laurent binomial σ-ideals are given in terms of Gröbner bases of $\mathbb{Z}[x]$-lattices, regular and coherent σ-chains in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$, and partial characters on $\mathbb{Z}[x]^n$, respectively. It is also shown that a Laurent binomial σ-ideal is radical and dimensionally un-mixed. We also give criteria for a Laurent binomial σ-ideal to be reflexive, well-mixed, perfect, and prime in terms of its support lattice. It is shown that the reflexive, well-mixed, and perfect closures of a Laurent binomial σ-ideal $\mathcal{I}$ is still binomial whose support lattices are the x-, M-, and P-saturation of the support lattice of $\mathcal{I}$.

For binomial σ-ideals, we show that certain properties of algebraic binomial ideals given in Eisenbud and Sturmfels (1996) can be extended to the difference case using the theory of Gröbner bases in the case of infinitely many variables. It is shown that most properties of Laurent binomial σ-ideals can be extended to the normal binomial σ-ideals. A criterion is given for a difference variety to be defined by a set of difference binomials.

Algorithms are given for the key results of the paper. We give algorithms to check whether a given Laurent binomial difference ideal $\mathcal{I}$ is reflexive, prime, well-mixed, or perfect, and in the negative case, to compute the reflexive, well-mixed, and perfect closures of $\mathcal{I}$. An algorithm is given to decompose a finitely generated perfect binomial difference ideal as the intersection of reflexive prime binomial difference ideals. The efficient implementation and complexity analysis of these algorithms will be our future work. As the first step, an efficient and polynomial-time algorithm for computing the generalized Hermite normal form was given in Jing et al. (2016).

Finally, we make a remark about differential binomial ideals. The study of binomial differential ideals is more difficult, because the differentiation of a binomial is generally not a binomial. Differential toric varieties were defined in Li et al. (2015) and were used to connect the differential Chow form (Gao et al., 2013) and differential sparse resultant (Li et al., 2015). But, contrary to the difference case, the defining ideal for a differential toric variety is generally not binomial.

Acknowledgements

We thank the anonymous referees for their careful reading of the paper and useful comments. We also thank Jie Wang for careful reading of the paper.

References

Barile, M., Morales, M., Thoma, A., 2001. Set-theoretic complete intersections on binomials. Proc. Am. Math. Soc. 130 (7), 1893–1903.
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.
Cohen, H., 1993. A Course in Computational Algebraic Number Theory. Springer-Verlag, Berlin.
Cohn, R.M., 1965. Difference Algebra. Interscience Publishers, New York.
Cox, D., Little, J., O'Shea, D., 1998. Using Algebraic Geometry. Springer-Verlag, New York.
Dickenstein, A., Matusevich, L.F., Miller, E., 2010. Combinatorics of binomial primary decomposition. Math. Z. 264 (4), 745–763.
Eisenbud, D., Sturmfels, B., 1996. Binomial ideals. Duke Math. J. 84 (1), 1–45.
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., 2009a. A characteristic set method for ordinary difference polynomial systems. J. Symb. Comput. 44 (3), 242–260.
Gao, X.S., Van der Hoeven, J., Yuan, C.M., Zhang, G.L., 2009b. Characteristic set method for differential-difference polynomial systems. J. Symb. Comput. 44 (9), 1137–1163.
Geddes, K.O., Czapor, S.R., Labahn, G., 1992. Algorithms for Computer Algebra. Kluwer Academic Publishers, Boston, MA.
Gerdt, V.P., Robertz, D., 2012. Computation of difference Gröbner bases. Comput. Sci. J. Mold. 20 (2), 203–226.
Hrushovski, E., 2012. The elementary theory of the Frobenius automorphisms. Available from http://www.ma.huji.ac.il/~ehud/.
Iima, K.I., Yoshino, Y., 2009. Gröbner bases for the polynomial ring with infinite variables and their applications. Commun. Algebra 37 (10), 3424–3437.
Jing, R.J., Yuan, C.M., Gao, X.S., 2016. A polynomial-time algorithm to compute generalized Hermite normal form of matrices over Z[x]. arXiv:1601.01067.
Koppenhagen, U., Mayr, E.W., 1996. An optimal algorithm for constructing the reduced Gröbner basis of binomial ideals. In: Proc. ISSAC'96. ACM Press, pp. 55–62.
Levin, A., 2008. Difference Algebra. Springer-Verlag, New Work.
Li, W., Yuan, C.M., Gao, X.S., 2015. Sparse differential resultant for Laurent differential polynomials. Found. Comput. Math. 15 (2), 451–517.
Martínez de Castilla, I.O., Sánchez, R.P., 2000. Cellular binomial ideals. Primary decomposition of binomial ideals. J. Symb. Comput. 30 (4), 383–400.
Millán, M.P., Dickenstein, A., Shiu, A., Conradi, C., 2012. Chemical reaction systems with toric steady states. Bull. Math. Biol. 74, 1027–1065.
Pachter, L., Sturmfels, B. (Eds.), 2005. Algebraic Statistics for Computational Biology. Cambridge University Press.
Peeva, I., Sturmfels, B., 1998. Syzygies of codimension 2 lattice ideals. Math. Z. 229 (1), 163–194.
Ritt, J.F., Doob, J.L., 1933. Systems of algebraic difference equations. Am. J. Math. 55 (1), 505–514.
Saleemi, M., Zimmermann, K.H., 2010. Linear codes as binomial ideals. Int. J. Pure Appl. Math. 61 (2), 147–156.
Wibmer, M., 2013. Algebraic difference equations. Preprint.