Binomial Difference Ideals

Xiao-Shan Gao, Zhang Huang, Chun-Ming Yuan
KLMM, Academy of Mathematics and Systems Science
The Chinese Academy of Sciences, Beijing 100190, China

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 over \(\mathbb{Z}[x]\)-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 difference binomial ideals. Finally, algorithms are given to check whether a given Laurent binomial difference ideal \(I\) is reflexive, prime, well-mixed, or perfect, and in the negative case, to compute the reflexive, well-mixed, and perfect closures of \(I\). An algorithm is given to decompose a finitely generated perfect binomial difference ideal as the intersection of reflexive prime binomial difference ideals.

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.

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 [7], which were further studied in [1, 6, 19, 16, 23] and were applied in algebraic statistics [22], chemical reactions [20], and error-correcting codes [25].

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 [24] and Cohn [4], who aimed to study algebraic difference equations in the way polynomial equations were studied in commutative algebra and algebraic geometry [4, 13, 17, 26].

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 \(\sigma\). For instance, \(a^2\sigma(a)^2\) 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 [7]. 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 [9] is used for similar purposes. It is shown that any Laurent binomial difference ideal can be written as $[A]$, where $A$ is a regular and coherent difference ascending chain consisting of binomial difference polynomials.

Let $I$ be a proper Laurent binomial difference ideal and $L = \{ f \in \mathbb{Z}[x]^n \mid \forall f - cf \in I \}$ the support lattice of $I$, which is a $\mathbb{Z}[x]$-lattice. In Section 5 we give criteria for a Laurent binomial difference ideal to be prime, reflexive, well-mixed, and perfect in terms of its support lattice. 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 $I$ 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 $I$ 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 $I$.

In Section 6 binomial difference ideals are studied. It is shown that a large portion of the properties for binomial ideals proved in [7] 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.

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 $I$ 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 $I$. 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 [9].

A distinctive feature of the algorithms presented in this paper is that problems about difference binomial polynomial 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 [4, 9, 13, 17, 26].

2.1 Difference polynomial and Laurent difference polynomial

An ordinary difference field, or simply a $\sigma$-field, is a field $\mathcal{F}$ with a third unitary operation $\sigma$ 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 $\sigma$ 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 $\sigma$-field has an inversive closure [4]. A typical example of inversive $\sigma$-field is $\mathbb{Q}(\lambda)$ with $\sigma(f(\lambda)) = f(\lambda + 1)$.

In this paper, $\mathcal{F}$ is assumed to be inversive and of characteristic zero. Furthermore, we use $\sigma$- 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 $\sigma$-over field of $\mathcal{F}$, denote

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

For instance, $a^{x^2-1} = a^{(2)}/a$. It is easy to check that for $p, q \in \mathbb{Z}[x]$, we have

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

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 $\sigma$-field $\mathcal{G}$ which contains $\mathcal{F}$. We will denote respectively by $\mathcal{F}[S]$, $\mathcal{F}(S)$, $\mathcal{F}\{S\}$, and $\mathcal{F}(S)$ the smallest subring, the smallest subfield, the smallest $\sigma$-subring, and the smallest $\sigma$-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 $\mathcal{F}\{S\} = \mathcal{F}(\Theta(S))$.

Now suppose $\mathcal{Y} = \{y_1, \ldots, y_n\}$ is a set of $\sigma$-indeterminates over $\mathcal{F}$. The elements of $\mathcal{F}\{\mathcal{Y}\} = \mathcal{F}\{y_j^{(k)} : j = 1, \ldots, n; k \in \mathbb{N}\}$ are called $\sigma$-polynomials over $\mathcal{F}$ in $\mathcal{Y}$, and $\mathcal{F}\{\mathcal{Y}\}$ itself is called the $\sigma$-polynomial ring over $\mathcal{F}$ in $\mathcal{Y}$. A $\sigma$-polynomial ideal, or simply a $\sigma$-ideal, $\mathcal{I}$ in $\mathcal{F}\{\mathcal{Y}\}$ 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 $\sigma$-ideal. A prime $\sigma$-ideal is a $\sigma$-ideal which is prime as an ordinary algebraic polynomial ideal. For convenience, a prime $\sigma$-ideal is assumed not to be the unit ideal in this paper. A $\sigma$-ideal $\mathcal{I}$ is called well-mixed if $fg \in \mathcal{I}$ implies $fg^\sigma \in \mathcal{I}$ for $f, g \in \mathcal{F}\{\mathcal{Y}\}$. A $\sigma$-ideal $\mathcal{I}$ is called perfect if for any $a \in \mathbb{N}[x] \setminus \{0\}$ and $p \in \mathcal{F}\{\mathcal{Y}\}$, $a^p \in \mathcal{I}$ implies $p \in \mathcal{I}$. If $S$ is a subset of $\mathcal{F}\{\mathcal{Y}\}$, we use $(S)$, $[S]$, $(S)$ and $\{S\}$ to denote the algebraic ideal, the $\sigma$-ideal, the well-mixed $\sigma$-ideal, and the perfect $\sigma$-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 $\eta_i$ are selected from a $\sigma$-overfield of $\mathcal{F}$. For a $\sigma$-polynomial $f \in \mathcal{F}\{\mathcal{Y}\}$, $\eta$ is called a $\sigma$-zero of $f$ if when substituting $y_j^{(j)}$ by $\eta_j^{(j)}$ in $f$, the result is 0.
For \( f = (f_1, \ldots, f_n)^\tau \in \mathbb{Z}[x]^n \), we define \( \mathcal{Y}^f = \prod_{i=1}^n y_i^{f_i} \). \( \mathcal{Y}^f \) is called a Laurent \( \sigma \)-monomial in \( \mathcal{Y} \) and \( f \) is called its support. A nonzero vector \( f = (f_1, \ldots, f_n)^\tau \in \mathbb{Z}[x]^n \) 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 \( \sigma \)-polynomial over \( \mathcal{F} \) in \( \mathcal{Y} \) is an \( \mathcal{F} \)-linear combination of Laurent \( \sigma \)-monomials in \( \mathcal{Y} \). Clearly, the set of all Laurent \( \sigma \)-polynomials form a commutative \( \sigma \)-ring under the obvious sum, product, and the usual transforming operator \( \sigma \), where all Laurent \( \sigma \)-monomials are invertible. We denote the \( \sigma \)-ring of Laurent \( \sigma \)-polynomials with coefficients in \( \mathcal{F} \) by \( \mathcal{F}\{\mathcal{Y}^\pm\} \). Let \( p \) be a Laurent \( \sigma \)-polynomial in \( \mathcal{F}\{\mathcal{Y}^\pm\} \). An \( n \)-tuple \((a_1, \ldots, a_n)\) over \( \mathcal{F} \) with each \( a_i \neq 0 \) is called a nonzero \( \sigma \)-solution of \( p \) if \( p(a_1, \ldots, a_n) = 0 \).

### 2.2 Characteristic set for a difference polynomial system

Let \( f \) be a \( \sigma \)-polynomial in \( \mathcal{F}\{\mathcal{Y}\} \). 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 \( \text{ord}(f, y_i) \). If \( y_i \) does not appear in \( f \), then we set \( \text{ord}(f, y_i) = -\infty \). The order of \( f \) is defined to be \( \max_i \text{ord}(f, y_i) \), that is, \( \text{ord}(f) = \max_i \text{ord}(f, y_i) \).

The elimination ranking \( \mathcal{R} \) on \( \Theta(\mathcal{Y}) = \{\sigma^k y_i | 1 \leq i \leq n, k \geq 0\} \) 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 \( \Theta(\mathcal{Y}) \). By convention, \( 1 < \theta y_j \) for all \( \theta y_j \in \Theta(\mathcal{Y}) \).

Let \( f \) be a \( \sigma \)-polynomial in \( \mathcal{F}\{\mathcal{Y}\} \). The greatest \( y_j^{(k)} \) w.r.t. \( \mathcal{R} \) which appears effectively in \( f \) is called the leader of \( f \), denoted by \( \text{ld}(f) \) and correspondingly \( y_j \) is called the leading variable of \( f \), denoted by \( \text{lvar}(f) = y_j \). The leading coefficient of \( f \) as a univariate polynomial in \( \text{ld}(f) \) is called the initial of \( f \) and is denoted by \( \text{I}_f \).

Let \( p \) and \( q \) be two \( \sigma \)-polynomials in \( \mathcal{F}\{\mathcal{Y}\} \). \( q \) is said to be of higher rank than \( p \) if \( \text{ld}(q) > \text{ld}(p) \) or \( \text{ld}(q) = \text{ld}(p) = y_j^{(k)} \) and \( \text{deg}(q, y_j^{(k)}) > \text{deg}(p, y_j^{(k)}) \).

Suppose \( \text{ld}(p) = y_j^{(k)} \). \( q \) is said to be reduced w.r.t. \( p \) if \( \text{deg}(q, y_j^{(k+l)}) < \text{deg}(p, y_j^{(k)}) \) for all \( l \in \mathbb{N} \).

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

A \( \sigma \)-chain \( \mathcal{A} \) can be written as the following form

\[
\mathcal{A} : A_{11}, \ldots, A_{1k_1}, \ldots, A_{p_1}, \ldots, A_{p_k_p}
\]  

(1)

where \( \text{lvar}(A_{ij}) = y_{c_j} \) for \( j = 1, \ldots, k_i \) and \( \text{ord}(A_{ij}, y_{c_j}) < \text{ord}(A_{il}, y_{c_l}) \) for \( j < l \). The following are two \( \sigma \)-chains

\[
\begin{align*}
\mathcal{A}_1 &= y_1^1 - 1, \quad y_2^2 y_2^1 - 1, \quad y_2^2 - 1 \\
\mathcal{A}_2 &= y_1^2 - 1, \quad y_2^2 - y_1, \quad y_2^2 - 1, \quad y_2^2 + y_2
\end{align*}
\]  

(2)

Let \( \mathcal{A} = A_1, A_2, \ldots, A_t \) be a \( \sigma \)-chain with \( I_1 \) as the initial of \( A_1 \), and \( f \) any \( \sigma \)-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

\[
\prod_{i=1}^{t} I_i^{e_i} \cdot f \equiv r, \quad \text{mod} \ [\mathcal{A}],
\]

(3)

where the \( e_i \in \mathbb{N}[x] \) and \( r = \text{prem}(f, \mathcal{A}) \) is called the \( \sigma \)-remainder of \( f \) w.r.t. \( \mathcal{A} \) \[9\].

A \( \sigma \)-chain \( \mathcal{C} \) contained in a \( \sigma \)-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 \( \sigma \)-polynomial set has a characteristic set. A characteristic set \( \mathcal{C} \) of a \( \sigma \)-ideal \( \mathcal{J} \) reduces to zero all elements of \( \mathcal{J} \).

Let \( \mathcal{A} : A_1, \ldots, A_t \) be a \( \sigma \)-chain, \( I_i = I(A_i), y_i^{(a_i)} = \text{ld}(A_i) \). \( \mathcal{A} \) is called regular if for any \( j \in \mathbb{N} \), \( I_i^{x_j} \) is invertible w.r.t. \( \mathcal{A} \) \[10\] in the sense that \( [A_1, \ldots, A_{i-1}, I_i^{x_j}] \) contains a nonzero \( \sigma \)-polynomial involving no \( y_i^{(a_i+k)}, k = 0, 1, \ldots \). To introduce the concept of coherent \( \sigma \)-chain, we need to define the \( \Delta \)-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 \( y_i \), then \( o_i = \text{ord}(A_i, y_i) < o_j = \text{ord}(A_j, y_j) \). Define

\[
\Delta(A_i, A_j) = \text{prem}((A_i)x_j^{o_j-o_i}, A_j).
\]

(4)

Then \( \mathcal{A} \) is called coherent if \( \text{prem}(\Delta(A_i, A_j), \mathcal{A}) = 0 \) for all \( i < j \) \[9\].

Let \( \mathcal{A} \) be a \( \sigma \)-chain. Denote \( \mathbb{I}_A \) 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

\[
\text{sat}(\mathcal{A}) = [\mathcal{A}] : \mathbb{I}_A = \{ p \in \mathcal{F}(\mathbb{Y}) : \exists h \in \mathbb{I}_A, \text{s.t.} \ hp \in [\mathcal{A}] \}.
\]

The following result is needed in this paper.

**Theorem 2.1** [9, Theorem 3.3] A \( \sigma \)-chain \( \mathcal{A} \) is a characteristic set of \( \text{sat}(\mathcal{A}) \) 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 \( \mathbf{f} = \{f_1, \ldots, f_s\} \subset \mathbb{Z}[x]^n \):

\[
L = \text{Span}_{\mathbb{Z}[x]}(f_1, \ldots, f_s) \cong (f_1, \ldots, f_s).
\]

A matrix representation of \( \mathbf{f} \) or \( L \) is

\[
M = [f_1, \ldots, f_s]_{n \times s},
\]

with \( f_i \) 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 [5].

Denote $e_i$ to be the $i$-th standard basis vector $(0, \ldots, 0, 1, 0, \ldots, 0)^T \in \mathbb{Z}^n$, where 1 lies in the $i$-th row of $e_i$. A monomial $m$ in $\mathbb{Z}[x]^n$ is an element of the form $ax^k e_i \in \mathbb{Z}[x]^n$, where $a \in \mathbb{Z}$ and $k \in \mathbb{N}$. The following monomial order $\triangleright$ of $\mathbb{Z}[x]^n$ will be used in this paper: $ax^\alpha e_i > bx^\beta e_j$ if $i > j$, or $i = j$ and $\alpha > \beta$, or $i = j$, $\alpha = \beta$, and $|\alpha| > |\beta|$.

With the above order, any $f \in \mathbb{Z}[x]^n$ can be written in a unique way as a linear combination of monomials, $f = \sum_{i=1}^l \mathbf{h}_i$, where $\mathbf{h}_i \neq 0$ and $\mathbf{h}_1 \triangleright \mathbf{h}_2 \triangleright \cdots \triangleright \mathbf{h}_l$. The leading term of $f$ is defined to be $\text{LT}(f) = \mathbf{h}_1$. For any $G \subset \mathbb{Z}[x]^n$, we denote by $\text{LT}(G)$ the set of leading terms of $G$.

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

Let $G \subset \mathbb{Z}[x]^n$ and $f \in \mathbb{Z}[x]^n$. We say that $f$ is $G$-reduced with respect to $G$ if any monomial of $f$ is not a multiple of $\text{LT}(g)$ by an element in $\mathbb{Z}[x]$ for any $g \in G$.

**Definition 3.1** A finite set $\mathcal{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Z}[x]^n$ is called a Gröbner basis for the $\mathbb{Z}[x]$-lattice $L$ generated by $\mathcal{F}$ if for any $g \in L$, there exists an $i$, such that $\text{LT}(g) \triangleright \text{LT}(f_i)$. A Gröbner basis $\mathcal{F}$ is called reduced if for any $f \in \mathcal{F}$, $f$ is $G$-reduced with respect to $\mathcal{F} \setminus \{f\}$. In this paper, it is always assumed that $f_1 < f_2 < \cdots < f_s$.

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

**Definition 3.2** Let $f, g \in \mathbb{Z}[x]^n$, $\text{LT}(f) = ax^k e_i$, $\text{LT}(g) = bx^s e_j$, $s \leq k$. Then the $S$-polynomial of $f$ and $g$ is defined as follows: if $i \neq j$ then $S(f, g) = 0$; otherwise $S(f, g) = \begin{cases} f - \frac{a}{b} x^k s g, & \text{if } b \mid a; \\ \frac{k}{a} f - x^k s g, & \text{if } a \mid b; \\ uf + vx^k s g, & \text{if } a \not\mid b \text{ and } b \not\mid a, \end{cases}$ where $\text{gcd}(a, b) = u a + v b$.

The following basic property for Gröbner basis is obviously true for $\mathbb{Z}[x]$-lattices and a polynomial-time algorithm to compute Gőbner bases for $\mathbb{Z}[x]$-lattices is given in [15].

**Theorem 3.3 (Buchberger’s Criterion)** The following statements are equivalent.

1) $\mathcal{F} = \{f_1, \ldots, f_s\} \subset \mathbb{Z}[x]^n$ is a Gröbner basis.

2) $\text{grem}(S(f_i, f_j), G) = 0$ for all $i, j$.

3) $f \in (\mathcal{F})$ if and only if $\text{grem}(f, \mathcal{F}) = 0$.

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 3.4** 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 $\text{LT}(b_i) = c_i x^{d_i} \in \mathbb{N}[x]$. Then

\[...\]
1) \( 0 \leq d_1 < d_2 < \cdots < d_k \).
2) \( c_k | \cdots | c_2 | c_1 \) and \( c_i \neq c_{i+1} \) for \( 1 \leq i \leq k-1 \).
3) \( \frac{c_i}{c_k} | b_i \) for \( 1 \leq i < k \). If \( b_1 \) is the primitive part of \( b_1 \), then \( \tilde{b}_1 | b_i \) for \( 1 < i \leq k \).
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 3.3. To prove 2), assume that there exists an \( l \) such that \( c_{l-1} | \cdots | c_2 | c_1 \) but \( c_l \nmid c_{l-1} \). 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 \( \text{LT}(g) = r x^{d_l} \) 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 \( b_1 = c_1 x^{d_1} + s_1 x^{d_1-1} + \cdots + s_{1d_1} \) and \( b_2 = c_2 x^{d_2} + s_2 x^{d_2-1} + \cdots + s_{2d_2} \). 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 \( \mathbb{Z}[x] \). The claim is true. Assume that for \( k = l-1 \), the claim is true, then \( \tilde{b}_1 b_l \) for \( 1 \leq i \leq l-1 \). We will prove the claim for \( k = l \). Since \( S(b_1, b_l) = \frac{c_l}{c_l} b_l - x^{d_l-d_1} b_1 \) can be reduced to zero by \( B \). We have \( \frac{c_l}{c_l} b_l - x^{d_l-d_1} b_1 = \sum_{i=1}^{l-1} f_i b_i \) with \( f_i \in \mathbb{Z}[x] \) and \( \deg(f_i b_i) \leq d_i - 1 \). Then, \( \frac{c_l}{c_l} b_l = x^{d_l-d_1} b_1 + \sum_{i=1}^{l-1} f_i b_i \). By induction, \( b_l \) is a factor of the right hand side of the above equation. Thus \( \tilde{b}_1 | b_l \). Let \( b_i = s_i b'_i \) for \( 1 \leq i \leq l \), we have \( \frac{c_l}{c_l} s_l = x^{d_l-d_1} s_l + \sum_{i=1}^{l-1} f_i s_i \) where \( \deg(s_i) = d_i - d_1 \) and \( s_1 \in \mathbb{Z} \). Since \( \deg(f_i s_i) \leq d_i - d_1 - 1 \), we have \( \frac{c_l}{c_l} | s_l \) and \( \frac{c_l}{c_l} | b_l \). For any \( 1 \leq i < j < l \), assume \( \frac{c_l}{c_l} | b_i \). We will show that \( \frac{c_l}{c_l} | b_j \). Since \( S(b_j-1, b_j) = \frac{c_l}{c_l} b_j - x^{d_j-d_{j-1}} b_{j-1} = \sum_{i=1}^{j-1} f_i b_i \), we have \( \frac{c_l}{c_l} \) is a factor of the right hand side of the above equation, for \( c_{j-1} | c_{j-2} | \cdots | c_1 \). Then, \( \frac{c_l}{c_l} \) divides \( b_i \). The claim is proved.

**Example 3.5** 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\}.

To give the structure of a reduced Gröbner basis similar to that in Example 3.5, we introduce the concept of generalized Hermite normal form. Let

\[
C = \begin{bmatrix}
c_{1,1} & \ldots & c_{1,1} & 0 & \ldots & \ldots & \ldots & \ldots & \ldots \\
c_{r_1,1} & \ldots & c_{r_1,1} & 0 & \ldots & \ldots & \ldots & \ldots & \ldots \\
o & \ldots & 0 & c_{r_1+1,1} & \ldots & \ldots & \ldots & \ldots & \ldots \\
o & \ldots & 0 & c_{r_2,1} & \ldots & \ldots & \ldots & \ldots & \ldots \\
\vdots & \vdots & \vdots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
o & \ldots & 0 & 0 & \ldots & 0 & \ldots & \ldots & \ldots \\
o & \ldots & 0 & 0 & \ldots & 0 & \ldots & \ldots & \ldots \\
0 & \ldots & 0 & 0 & \ldots & 0 & \ldots & \ldots & \ldots \\
0 & \ldots & 0 & 0 & \ldots & 0 & \ldots & \ldots & \ldots \\
\end{bmatrix}_{m \times s}
\]  

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 \( c_{r_i,j} \) to be the column of the matrix \( C \) whose last nonzero element is

\[
c_{r_i,j} = c_{r_i,j,0} x^{d_{r_i,j}} + \cdots + c_{r_i,j,d_{r_i,j}}.
\]

(7) Then the leading monomial of \( c_{r_i,j} \) is \( c_{r_i,j,0} x^{d_{r_i,j}} \). It is clear that \( \text{rk}(L) = t \).
Definition 3.6 The matrix $C$ in (6) is called a generalized Hermite normal form if it satisfies the following conditions:

1) $0 \leq d_{r_i,1} < d_{r_i,2} < \cdots < d_{r_i,i}$ for any $i$.

2) $c_{r_i,l,0} \cdots |c_{r_i,2,0}|c_{r_i,1,0}$.

3) $S(c_{r_i,j_1}, c_{r_i,j_2}) = x^{d_{r_i,j_2} - d_{r_i,j_1}} c_{r_i,j_1} - \frac{c_{r_i,j_2}}{c_{r_i,j_1}} c_{r_i,j_2}$ can be reduced to zero by the column vectors of the matrix for any $1 \leq i \leq t, 1 \leq j_1 < j_2 \leq l_i$.

4) $c_{r_i,j}$ is $G$-reduced w.r.t. the column vectors of the matrix other than $c_{r_i,j}$, for any $1 \leq i \leq t, 1 \leq j \leq l_i$.

It is clear that $\{c_{r_i,1}, \ldots, c_{r_i,l_i}\}$ is a reduced Gröbner basis in $\mathbb{Z}[x]$. Then, as a consequence of Theorem 3.3 and Lemma 3.4 we have

Theorem 3.7 $f = \{f_1, \ldots, f_s\} \subset \mathbb{Z}[x]^n$ is a reduced Gröbner basis such that $f_1 < f_2 < \cdots < f_s$ if and only if $\{f_1, \ldots, f_s\}$ is a generalized Hermite normal form.

Example 3.8 The following matrices are generalized Hermite normal forms

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

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

Let $f = \{f_1, \ldots, f_s\}$ be a reduced Gröbner basis. Let $S(f_i, f_j) = m_{ij}f_i - m_{jj}f_j$ be the S-polynomial of $f_i, f_j$ and $\text{grem}(S(f_i, f_j), f) = \sum_k c_k f_k$ be the normal representation of $f$ in terms of the Gröbner basis $f$. Then the syzygy polynomial $\tilde{S}(f_i, f_j)$

$$\tilde{S}(f_i, f_j) = m_{ij}e_i - m_{jj}e_j - \sum_k c_k e_k,$$

is an element in $\mathbb{Z}[x]^s$, where $e_k$ is the $k$-th standard basis vector of $\mathbb{Z}[x]^s$. Define an order in $\mathbb{Z}[x]^s$ as follows: $ax^\alpha e_i < bx^\beta e_j$ if $\text{LT}(ax^\alpha f_i) > \text{LT}(bx^\beta f_j)$ in $\mathbb{Z}[x]^n$. By Schreyer’s Theorem [5, p. 212], we have

Theorem 3.9 Let $F = [f_1, \ldots, f_s]_{n \times s} \in \mathbb{Z}[x]^{n \times s}$ be a generalized Hermite normal form. Then the syzygy polynomials $\tilde{S}(f_i, f_j)$ form a Gröbner basis of the $\mathbb{Z}[x]$-lattice $\ker(F) = \{X \in \mathbb{Z}[x]^n | FX = 0\}$ under the newly defined order $\prec$.

Let $C$ be defined in (6) and $k \in \mathbb{N}$. Introduce the following notations:

$$C_- = \bigcup_{i=1}^t \bigcup_{k=0}^{l_i-1} \{x^{\deg(c_{r_i,k+1})-\deg(c_{r_i,k})-1}c_{r_i,k}\},$$

$$C^+ = \bigcup_{i=1}^t \bigcup_{k=0}^\infty \{x^k c_{r_i,k}\}.$$

$$C^\infty = C_- \cup C^+$$

(8)
Example 3.10 Let $C = \begin{bmatrix} 6 & 3x & 0 & 3 & 2x \\ 0 & 0 & 6 & 3x & x^3 + x \end{bmatrix}$. Then $C_- = \begin{bmatrix} 6 & 0 & 3 & 3x \\ 0 & 6 & 3x & 3x^2 \end{bmatrix}$ and $C_\infty = \begin{bmatrix} 6 & 3x & 3x^2 & 3x^3 & \ldots & 0 & 3 & 3x & 2x & 2x^2 & \ldots \\ 0 & 0 & 0 & 0 & \ldots & 6 & 3x & 3x^2 & x^3 + x & x^4 + x^2 & \ldots \end{bmatrix}$.

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

Lemma 3.11 The columns of $C_\infty$ in (8) are linear independent over $\mathbb{Z}$.

Proof: Suppose $C$ is given in (6). The leading term of $c \in C_\infty$ is $\text{LT}(c) = ax^l \epsilon_i$ for $i = 1, \ldots, t$ and $l \in \mathbb{N}$. Furthermore, for two different $c_1$ and $c_2$ in $C_\infty$ such that $\text{LT}(c_1) = ax^{l_1} \epsilon_i$ and $\text{LT}(c_2) = bx^{l_2} \epsilon_i$, we have $l_1 \neq l_2$. Then $\text{LT}(C_\infty) = \{a_d x^{l_i} \epsilon_i | i = 1, \ldots, t; l_i = d_{i1}, d_{i1} + 1, \ldots; a_d \in \mathbb{Z}\}$ are linear independent over $\mathbb{Z}$, where $d_{i1}$ is from (7). Then $C_\infty$ are also linear independent over $\mathbb{Z}$. □

Lemma 3.12 Let $C$ be a generalized Hermite normal form. Then any $g \in (C)$ can be written uniquely as a linear combination of finitely many elements of $C_\infty$ over $\mathbb{Z}$.

Proof: $g \in (C)$ can be written as a linear combination of elements of $C_\infty$ over $\mathbb{Z}$ by the procedure to compute $\text{grem}(g, C) = 0$ [5]. The uniqueness is a consequence of Lemma 3.11. □

## 4 Canonical Representations for Laurent binomial $\sigma$-ideal

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

### 4.1 Laurent binomial $\sigma$-ideal

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

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

$$p = \mathbb{Y}^f - c_f$$

where $c_f \in \mathbb{F}^* = \mathbb{F} \setminus \{0\}$ and $f \in \mathbb{Z}[x]^n$ is normal. The vector $f$ is called the support of $p$. For $p = \mathbb{Y}^f - c_f$, we denote $\hat{p} = -c_f^{-1} \mathbb{Y}^{-f} p = \mathbb{Y}^{-f} - c_f^{-1}$ which is called the inverse of $p$. It is clear that any Laurent $\sigma$-binomial $f$ can be written uniquely as $f = a M (\mathbb{Y}^f - c_f)$ where $a \in \mathbb{F}^*$, $M$ is a Laurent $\sigma$-monomial, and $\mathbb{Y}^f - c_f$ is in normal form. Since $a M$ is a unit
A Laurent σ-ideal is called binomial if it is generated by Laurent σ-binomials.

**Lemma 4.1** Let $Y^f_i - c_i, i = 1, \ldots, s$ be contained in a Laurent binomial σ-ideal $\mathcal{I}$ and $f = a_1f_1 + \cdots + a_sf_s$, where $a_i \in \mathbb{Z}[x]$. Then $Y^f - \prod_{i=1}^{s} c_i^{a_i}$ is in $\mathcal{I}$.

**Proof:** It suffices to show that if $p_1 = Y^f_i - c_1 \in \mathcal{I}$ and $p_2 = Y^f_i - c_2 \in \mathcal{I}$, then $Y^{nf_i} - c_1^n \in \mathcal{I}$ for $n \in \mathbb{N}$, $Y^f_i - c_i^{-1} \in \mathcal{I}$, $Y^{xf_i} - \sigma(c_1) \in \mathcal{I}$, and $Y^{f_i + f_j} - c_1c_2 \in \mathcal{I}$, which are indeed true since $Y^{nf_i} - c_1^n = (Y^f_i)^n - c_1^n$ contains $p_1$ as a factor, $Y^{-f_i} - c_1^{-1} = -c_1^{-1}Y^{-f_i}(Y^f_i - c_1) \in \mathcal{I}$, $Y^{xf_i} - \sigma(c_1) = \sigma(Y^f_i - c_1) \in \mathcal{I}$, and $Y^{f_i + f_j} - c_1c_2 = Y^{f_i}(Y^{f_j} - c_2) + c_2(Y^{f_i} - c_1) \in \mathcal{I}$. \hfill $\square$

As a direct consequence, we have

**Proposition 4.2** Let $\mathbb{L}$ be a proper Laurent binomial σ-ideal and

$$\mathbb{L}(\mathcal{I}) := \{f \in \mathbb{Z}[x]^n \mid \exists c \in \mathbb{F}^* \text{ s.t. } Y^f - c_f \in \mathcal{I}\}. \quad (9)$$

Then $\mathbb{L}(\mathcal{I})$ is a $\mathbb{Z}[x]$-lattice, which is called the support lattice of $\mathcal{I}$. Furthermore, Let $\mathbb{L}(\mathcal{I}) = (f_1, \ldots, f_s)$. Then $\mathcal{I} = [Y^f_1 - c_1, \ldots, Y^f_s - c_s]$. That is, a Laurent binomial σ-ideal is finitely generated and $[f_1, \ldots, f_s]$ is called a matrix representation for $\mathcal{I}$.

**Proof:** Let $\mathcal{I}_1 = [Y^f_1 - c_1, \ldots, Y^f_s - c_s]$. 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 $f_h = Y^h - c_h$. Then $h \in \mathbb{L}(\mathcal{I}) = (f_1, \ldots, f_s)$. By Lemma 4.1 there exists a $c_h \in \mathbb{F}$ such that $f_h = Y^h - c_h \in \mathcal{I}_1$. Then $f_h - f_h = \tilde{c}_h - c_h \in \mathcal{I}_1$. Since $\mathcal{I}$ is proper, we have $f_h - f_h = 0$ or $f_h \in \mathcal{I}_1$ and hence $\mathcal{I} \subset \mathcal{I}_1$. \hfill $\square$

Similarly, we can prove

**Corollary 4.3** Let $\mathcal{I} = [Y^f_1 - c_1, \ldots, Y^f_s - c_s]$ be a proper Laurent binomial σ-ideal and let $h_1, \ldots, h_r$ be another set of generators of $(f_1, \ldots, f_s)$, and $h_i = \sum_{k=1}^{s} a_{i,k}f_k$, $i = 1, \ldots, r$, where $a_{i,k} \in \mathbb{Z}[x]$. Then $\mathcal{I} = [Y^{h_1} - \prod_{i=1}^{s} c_i^{a_{1,i}}, \ldots, Y^{h_r} - \prod_{i=1}^{s} c_i^{a_{r,i}}]$.

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

**Proposition 4.4** Let $\mathcal{I} = [Y^f_1 - c_1, \ldots, Y^f_s - c_s]$ be a Laurent binomial σ-ideal and $M = [f_1, \ldots, f_s] \in \mathbb{Z}[x]^{n \times s}$. Let $\ker(M) = \{h \in \mathbb{Z}[x]^s \mid Mh = 0\}$ be generated by $u_1, \ldots, u_t$, where $u_i = (u_{i,1}, \ldots, u_{i,s})$. 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:** \("\Rightarrow\" Suppose $f_i = Y^f_i - c_i$. Suppose $c = \prod_{i=1}^{s} c_i^{u_{l,i}} \neq 1$ for some $l$. Replacing $c_i$ by $Y^f_i - f_i$ in the above equation and noting that $u_i \in \ker(M)$, we have $c = \prod_{i=1}^{s} c_i^{u_{l,i}} = \prod_{i=1}^{s} (g_i^{f_i} - f_i)^{u_{l,i}} = \prod_{i=1}^{s} Y^{M \cdot u_i} + g = 1 + g$ where $g \in \mathcal{I}$. Then $0 \neq c - 1 \in \mathcal{I}$ and $\mathcal{I} = [1]$, a contradiction.

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

$$g_1f_1 + \cdots + g_sf_s = 1. \quad (10)$$
Let $l$ be the maximal $c$ such that $y_i^{(k)}$ occurs in some $f_i$, $0$ the largest $j$ such that $y_i^{(j)}$ occurs in some $f_k$, and $d = \max_{k=1}^{s} \deg(f_k, y_i^{(o)})$. Let $f_k = \nabla f_k - c_k = I_k y_i^{dx_o} - c_k$. Since \(10\) is an identity about the algebraic variables $y_i^{x_o}$, we can set $y_i^{dx_o} = c_k/I_k$ in \(10\) to obtain a new identity. In the new identity, $f_k$ becomes zero and the left hand side of \(10\) 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 \(10\) will eventually becomes zero, and a contradiction is obtained and the lemma is proved.

If $\ord(f_i, y_i) < o$ or $\ord(f_i, y_i) = o$ and $\deg(f_i, y_i^{x_o}) < d$ for some $i$, then $f_i$ is not changed in the above procedure. Let us assume that for some $v$, $\deg(f_v, y_i^{x_o}) = d$ and $f_v = \nabla f_v - c_v = I_v y_i^{dx_o} - c_v$. Then after the substitution, $f_v = c_k I_v/I_k - c_v = c_k \tilde{f}_v$ where $\tilde{f}_v = I_v/I_k - c_v/c_k$. We claim that either $\tilde{f}_v = 0$ 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 $f_v = f_k$, that is $f_v - f_k = 0$ is a syzygy among $f_i$, and let $c_{ve}$ be the corresponding syzygy vector. Then $c_{ve} c_k^{-1} = c_{ve}$ can be written as a product of $c_{ve} = \prod_{i=1}^{r} c_{v_i}^{u_{v_i}} = 1$, and thus $c_{v} c_{k}^{-1} = 1$.

### 4.2 Characteristic set of Laurent binomial $\sigma$-ideal

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

Second, when defining the concepts of rank and $q$ to be reduced w.r.t. $p$, 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 $|\deg(q, y_j^{(k+1)})| < |\deg(p, y_j^{(k)})|$ for all $l \in \mathbb{N}$, where $\lfloor d(p) \rfloor = y_j^{(k)}$. For instance, $y_1^{2x} y_2 - 1$ is not reduced w.r.t. $y_2^2 - 1$. With these changes, the concepts of $\sigma$-chain and characteristic set can be defined in the Laurent $\sigma$-binomial case. For instance, the $\sigma$-chain $A_2$ in \(2\) becomes the following Laurent normal form:

$$A_2 = y_1^2 - 1, \ y_1^{-1} y_2 - 1, \ y_2^2 - 1, \ y_2^{-1} y_2^2 - 1$$

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

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

$$r := \text{prem}_1(f, g) = (f - y I_f(y_i^{(o)}) d_f - d_g)/c_g = I_f(y_i^{(o)}) d_f - d_g - c_f/c_g.$$

Let $h_r, h_f, h_g$ be the supports of $r, f, g$, respectively. Then

$$h_r = h_f - h_g.$$
Set \( f = r \) and repeat the procedure \( \text{prem}_1 \) for \( f \) and \( g \). Since \( d_f \) decreases strictly after each iteration, the procedure will end and return \( \text{prem}(f, g) = r \) which satisfies

\[
    r = \frac{f}{c_k} - h g = \frac{I_f}{I_g} (y_1^{(o)})^{d_f - k d_g} - \frac{c_f}{c_g} \tag{14}
\]

\[
    h_r = h_f - k h_g \tag{15}
\]

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 \( \sigma \)-remainder can be computed similar to the first case. Instead of \( g \), we consider \( \hat{g} = (I_g)^{-1} (y_1^{(o)})^{-d_g} - c_g^{-1} \). If \( |d_f| < d_g \), then set \( r = \text{prem}_1(f, g) \) to be \( f \). Otherwise, perform the following basic step

\[
    r := \text{prem}_1(f, g) = c_g (f - \hat{g} I_g I_f (y_1^{(o)})^{d_f + d_g}) = I_f I_g (y_1^{(o)})^{d_f + d_g} - c_f c_g.
\]

In this case, equation \( (13) \) becomes \( h_r = h_f + h_g \). To compute \( \text{prem}(f, g) \), repeat the above basic step for \( f = r \) until \( |d_f| < d_g \).

For two general \( \sigma \)-binomials \( f \) and \( g \), \( \text{prem}(f, g) \) is defined as follows: if \( f \) is reduced w.r.t \( g \), set \( \text{prem}(f, g) = f \). Otherwise, let \( y_l = \text{i} \text{var}(g) \), \( o_f = \text{ord}(f, y_l) \), and \( o_g = \text{ord}(g, y_l) \). Define

\[
    \text{prem}(f, g) = \text{prem}(\ldots, \text{prem}(\text{prem}(f, g (^{o_f-o_g})^{d_f + d_g}) \ldots, g)).
\]

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

\[
    \text{prem}(f, \mathcal{A}) = \text{prem}(\ldots, \text{prem}(\text{prem}(f, A_s), A_{s-1}), \ldots, A_1).
\]

In summary, we have

**Lemma 4.5** Let \( \mathcal{A} = A_1, \ldots, A_s \) be a Laurent binomial \( \sigma \)-chain, \( f \) a \( \sigma \)-binomial, and \( r = \text{prem}(f, \mathcal{A}) \). Then \( r \) is reduced w.r.t. \( \mathcal{A} \) and satisfies

\[
    c f \equiv r \mod [\mathcal{A}], \tag{16}
\]

where \( c \in \mathcal{F}^\ast \). Furthermore, let the supports of \( r \) and \( f \) be \( h_r \) and \( h_f \), respectively. Then \( h_f - h_r \) 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 \( \sigma \)-chains can be extended to the Laurent case. Since any \( \sigma \)-monomial is a unit in \( \mathcal{F}\{\mathbb{Y}^\pm\} \), the concept of regular \( \sigma \)-chain need to be strengthened as follows. A \( \sigma \)-chain \( \mathcal{A} \) is called *Laurent regular* if \( \mathcal{A} \) is regular and any \( \sigma \)-monomial is invertible w.r.t \( \mathcal{A} \). Then, following [9], Theorem 2.1 can be extended to the following Laurent version straightforwardly.

**Theorem 4.6** A Laurent \( \sigma \)-chain \( \mathcal{A} \) is a characteristic set of \( \text{sat}(\mathcal{A}) \) if and only if \( \mathcal{A} \) is coherent and Laurent regular.

For Laurent binomial \( \sigma \)-chains, we have

**Lemma 4.7** Any Laurent binomial \( \sigma \)-chain \( \mathcal{A} \) is Laurent regular.
In the rest of this section, we will establish a connection between $A$ invertible w.r.t $A$ w.r.t an extension $A$. It can be shown that sat($A$) is Laurent binomial, $B$ and $M$ the initial. Then the Sylvester resultant of $I - n$ By Theorem 4.8, $A$ is Laurent regular.

Proof: Since the initials of Lemma 4.11 3.6, we have $I \in A$ of $I$ is also Laurent regular. By Theorem 4.6, $A$ is a proper Laurent binomial $\sigma$-ideal. By Lemma 4.7, $A$ is also Laurent regular. By Theorem 4.6, $A$ is a characteristic set of $I = \text{sat}(A)$. Then $I$ is proper.

We now give the first canonical representation for Laurent binomial $\sigma$-ideals.

Theorem 4.8 $I$ is a proper Laurent binomial $\sigma$-ideal if and only there exists a Laurent coherent $\sigma$-chain $A$ such that $I = \text{sat}(A) = [A]$.

Proof: Let $I \neq [1]$ and $A$ the characteristic set of $I$. Then $[A] \subset I \subset \text{sat}(A)$. From 10, we have sat($A$) $\subset [A]$ and then $I = \text{sat}(A) = [A]$. By Theorem 4.6, $A$ is coherent. To prove the other side of the theorem, let $A$ be a Laurent coherent $\sigma$-chain. By Lemma 4.7, $A$ is also Laurent regular. By Theorem 4.6, $A$ is a characteristic set of $I = \text{sat}(A)$. Then $I$ is proper.

Corollary 4.9 Let $I$ be a Laurent reflexive prime binomial $\sigma$-ideal in $\mathcal{F}\{y^\pm\}$. Then $\dim(I) = n - \text{rk}(L(I))$.

Proof: By Theorem 4.8, $I = [A]$, where $A : \mathbb{Y}^{c_1} - c_1, \ldots, \mathbb{Y}^{c_s} - c_s$. Let $C = [c_1, \ldots, c_s]$ is the matrix representation for $I$ and in the form of 10. Since $I$ is reflexive and prime, by Theorem 4.3 of 9, $\dim(I) = n - t = n - \text{rk}(L(I))$.

Corollary 4.10 A Laurent binomial $\sigma$-ideal is radical.

Proof: By Theorem 4.8, $I = [A]$, where $A : \mathbb{Y}^{h_1} - c_1, \ldots, \mathbb{Y}^{h_r} - c_r$ is the characteristic set of $I$. Let $A_i = \mathbb{Y}^{h_i} - c_i$ and $y^{(o_i)}$ $= \text{id}(A_i)$. $A$ is also saturated in the sense that its separant $\frac{\partial A_i}{\partial y^{(o_i)}}$ are $\sigma$-monomials and hence units in $\mathcal{F}\{y^\pm\}$. Then similar to the differential case 2, it can be shown that sat($A$) $= [A]$ is a radical $\sigma$-ideal.

Let $f_1 < f_2 < \cdots < f_s$ be elements in $\mathbb{Z}[x]^n$, $c_i \in \mathcal{F}^*$, and

$$f = \{f_1, \ldots, f_s\} \subset \mathbb{Z}[x]^n$$

$$A_f = \{A_1, \ldots, A_s\} \subset \mathcal{F}\{y^\pm\} \text{ with } A_i = \mathbb{Y}^{f_i} - c_i, i = 1, \ldots, s$$

(17)

In the rest of this section, we will establish a connection between $f$ and $A_f$. From Definition 3.6 we have

Lemma 4.11 For $i < j$, $A_j$ is reduced w.r.t. $A_i$ if and only if $f_j$ is $G$-reduced w.r.t. $f_i$. 13
Lemma 4.12 For \( \mathfrak{f} \) and \( A_\mathfrak{f} \) in (17) and a Laurent \( \sigma \)-binomial \( f = \mathbb{Y}^f - c \), if \( \text{prem}(f, A_\mathfrak{f}) = \mathbb{Y}^g - c_g \), then \( g = \text{grem}(f, \mathfrak{f}) \).

Proof: Let us first consider \( \text{prem}_1 \) in (12) for \( f \) and \( A_i = \mathbb{Y}^f - c_i = I_i(y_i^{o_i})^{d_i} - c_i \), where \( \text{ld}(A_i) = y_i \), and \( I_i \) is the initial of \( A_i \). From (13), the support of \( r = \text{prem}_1(f, A_i) \) is \( f_i \). It is clear that \( \text{LT}(f_i) = d_i x^{o_i} e_i \). Let \( f_i = d_i x^{o_i} e_i \). Similarly, write \( f = f_j x^{o_j} e_j + \overline{f} \), where \( d_j x^{o_j} e_j \) is the leading term of \( f \) w.r.t. \( e_j \) and \( d_j \geq 1 \). Then a basic step to compute \( \text{grem}(f, f_i) \) is to compute \( \text{grem}_1(f, f_i) = f - f_i = (f_d - d_i) x^{o_i} e_l + \overline{f} - \overline{f} \), which is the support of \( \text{prem}_1(f, A_i) \).

Using the basic step \( \text{grem}_1 \) to compute \( \text{grem}(f, \mathfrak{f}) \), we have a sequence of elements in \( \mathbb{Z}[x]^\mathfrak{f} : \mathfrak{g}_0 = f, \mathfrak{g}_1, \ldots, \mathfrak{g}_t = \text{grem}(f, \mathfrak{f}) \). Correspondingly, using the basic step \( \text{prem}_1 \) to compute \( \text{prem}(f, A_\mathfrak{f}) \), we have a sequence of \( \sigma \)-binomials \( f_0 = f, f_1, \ldots, f_t = \text{prem}(f, A_\mathfrak{f}) \) such that the support of \( f_i \) is \( g_i \) for \( i = 1, \ldots, t \).

Lemma 4.13 If \( \mathfrak{f} \) in (17) is a reduced Gröbner basis and \( [A_\mathfrak{f}] \neq [1] \), then \( A_\mathfrak{f} \) is a coherent \( \sigma \)-chain.

Proof: By Lemma 4.11, \( A_\mathfrak{f} \) is a \( \sigma \)-chain. Let \( A_i = \mathbb{Y}^f - c_i \) and \( A_j = \mathbb{Y}^{f_j} - c_j \) (\( i < j \)) have the same leading variable \( y_i \), and \( A_i = I_i y_i^{o_i} x^{c_i} - c_i \), \( A_j = I_j y_j^{o_j} x^{c_j} - c_j \). From Definition 3.6, we have \( o_i < o_j \) and \( d_j \mid d_i \). Let \( d_i = t d_j \) where \( t \in \mathbb{N} \). According to (14), we have

\[
\Delta(A_i, A_j) = \text{prem}(f_i x^{o_j - o_i}, A_j) = \frac{(I_j)^{x^{o_j - o_i}}}{I_j^{d_j}} - \frac{(c_i x^{o_j - o_i})}{c_j}.
\]  

Then the support of \( \Delta(A_i, A_j) \) is \( x^{o_j - o_i} f_i - \frac{d_i}{d_j} f_j \).

Since \( \text{LT}(A_i) = d_i x^{o_i} e_i \) and \( \text{LT}(A_j) = d_j x^{o_j} e_l \), we have \( N = \text{lcm}(d_i x^{o_i}, d_j x^{o_j}) = d_i x^{o_j} \). According to Definition 3.2, the S-vector of \( f_i \) and \( f_j \) is

\[
S(f_i, f_j) = x^{o_j - o_i} f_i - \frac{d_i}{d_j} f_j.
\]

Since \( \mathfrak{f} \) is a Gröbner basis, we have \( g = \text{grem}(S(f_i, f_j), \mathfrak{f}) = 0 \). Since the support of \( \Delta(A_i, A_j) \) is \( S(f_i, f_j) \), by Lemma 4.12 \( R = \text{prem}(\Delta(A_i, A_j), A_\mathfrak{f}) = \mathbb{Y}^g - c = 1 - c \) for some \( c \in \mathfrak{F} \). Since \([A_\mathfrak{f}]\) is proper and \( R = 1 - c \in [A_\mathfrak{f}] \), we have \( R = 0 \) and hence \( A_\mathfrak{f} \) is coherent.

We now give the main result of this section.

Theorem 4.14 For \( \mathfrak{f} \) and \( A_\mathfrak{f} \) defined in (17), \( A_\mathfrak{f} \) is a coherent \( \sigma \)-chain if and only if \( \mathfrak{f} \) is a reduced Gröbner basis and \([A_\mathfrak{f}] \neq [1]\).

Proof: Lemma 4.13 proves one side of the theorem. For the other direction, let \( A_\mathfrak{f} \) be a coherent \( \sigma \)-chain. By Lemma 4.11, \( f_i \) is G-reduced to \( f_j \) for \( i \neq j \). By Theorem 4.8, \([A_\mathfrak{f}]\) is proper. Use the notations introduced in the proof of Lemma 4.13. Since \( S(f_i, f_j) \) is the support of \( \Delta(A_i, A_j) \), by Lemma 4.12 \( f_{ij} = \text{grem}(S(f_i, f_j), \mathfrak{f}) \) is the support of \( \text{prem}(\Delta(A_i, A_j), A_\mathfrak{f}) \). Since \( A_\mathfrak{f} \) is coherent, \( \text{prem}(\Delta(A_i, A_j), A_\mathfrak{f}) = \mathbb{Y}^{f_{ij}} - c = 0 \) for any \( i \) and \( j \), and this is possible only when \( f_{ij} = \text{grem}(S(f_i, f_j), \mathfrak{f}) = 0 \) and \( c = 1 \) due to the fact \([A_\mathfrak{f}] \neq [1]\). Hence \( \mathfrak{f} \) is a reduced Gröbner basis.
4.3 Partial character and Laurent binomial \( \sigma \)-ideal

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

**Definition 4.15** A partial character \( \rho \) on \( \mathbb{Z}[x]^n \) is a homomorphism from a \( \mathbb{Z}[x] \)-lattice \( L_\rho \) to the multiplicative group \( \mathcal{F}^* \) satisfying \( \rho(x^f) = (\rho(f))^x = \sigma(\rho(f)) \) for \( f \in L_\rho \).

Let \( \rho \) be a partial character over \( \mathbb{Z}[x]^n \) and \( L_\rho = (f_1, \ldots, f_s) \), where \( f = \{f_1, \ldots, f_s\} \) is a reduced Gröbner basis. Define

\[
\mathcal{I}(\rho) := \{y^f - \rho(f) | f \in L_\rho\}, \quad (19)
\]

\[
\mathcal{A}(\rho) := y^{f_1} - \rho(f_1), \ldots, y^{f_s} - \rho(f_s). \quad (20)
\]

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

**Lemma 4.16** \( \mathcal{I}(\rho) = [\mathcal{A}(\rho)] \neq [1] \) and \( \mathcal{A}(\rho) \) is a characteristic set of \( \mathcal{I}(\rho) \).

**Proof:** By Lemma 4.1 and the property of partial character, \( \mathcal{I}(\rho) = [\mathcal{A}(\rho)] \). By Proposition 4.3 in order to prove \( \mathcal{I}(\rho) \neq [1] \), it suffices to show that for any syzygy \( \sum_i a_i f_i = 0 \) among \( f_i \), we have \( \prod_i \rho(f_i)^{a_i} = 1 \). Indeed, \( \rho(\sum_i a_i f_i) = \prod_i \rho(f_i)^{a_i} = 1 \), since \( \rho \) is a homomorphism from the \( \mathbb{Z}[x] \)-module \( L_\rho \) to \( \mathcal{F}^* \). Since \( f \) is a reduced Gröbner basis, by Theorem 4.14 \( \mathcal{A} \) is a characteristic set of \( \mathcal{I}(\rho) \). \( \Box \)

**Lemma 4.17** A Laurent \( \sigma \)-binomial \( y^f - c_f \) is in \( \mathcal{I}(\rho) \) if and only if \( f \in L_\rho \) and \( c_f = \rho(f) \).

**Proof:** By Lemma 4.16 \( \mathcal{A}(\rho) \) is a characteristic set of \( \mathcal{I}(\rho) \). Since \( f = y^f - c_f \) is a \( \sigma \)-binomial in \( \mathcal{I}(\rho) \), we have \( \tau = \text{prem}(f, \mathcal{A}) = 0 \). By Lemma 4.3 \( f \) is in the \( \mathbb{Z}[x] \)-module \( L_\rho \). The other side is obviously true and the lemma is proved. \( \Box \)

We now show that all Laurent binomial \( \sigma \)-ideals are defined by partial characters.

**Theorem 4.18** The map \( \rho \Rightarrow \mathcal{I}(\rho) \) gives a one to one correspondence between the set of proper Laurent binomial \( \sigma \)-ideals and partial characters on \( \mathbb{Z}[X]^n \).

**Proof:** By Lemma 4.16 a partial character defined a proper Laurent binomial \( \sigma \)-ideal. For the other side, let \( \mathcal{I} \subseteq \mathcal{F}\{Y^\pm\} \) be a proper Laurent binomial \( \sigma \)-ideal. \( \mathcal{I} \) is generated by its members of the form \( y^f - c_f \) for \( f \in \mathbb{Z}[x]^n \) and \( c_f \in \mathcal{F}^* \). Let \( L_\rho = \mathbb{L}(\mathcal{I}) \) which is defined in (21) and \( \rho(f) = c_f \). Since \( \mathcal{I} \) is proper, \( c_f \) is uniquely determined by \( f \). By Lemma 4.1 and Proposition 4.2 \( \rho \) is a partial character which is uniquely determined by \( \mathcal{I} \). It is clear \( \mathcal{I}(\rho) = \mathcal{I} \). To show the correspondence is one to one, it suffices to show \( \rho(\mathcal{I}(\rho)) = \rho \) which is a consequence of Lemma 4.17. The theorem is proved. \( \Box \)

As a summary of this section, we have the following canonical representations for a proper Laurent binomial \( \sigma \)-ideal, which follows directly from Theorems 4.8, 4.14, 4.18.

**Theorem 4.19** \( \mathcal{I} \) is a proper Laurent binomial \( \sigma \)-ideal if and only if
(1) \( I = [A] \), where \( A \) is a coherent Laurent binomial \( \sigma \) chain.

(2) \( I = [A] \), where \( A = Y^{f_1} - c_1, \ldots, Y^{f_s} - c_s \), \( f_i \in \mathbb{Z}[x]^n \), \( c_i \in \mathbb{F}^* \), \( f = \{f_1, \ldots, f_s\} \) is a reduced Gröbner basis of a \( \mathbb{Z}[x] \)-lattice, and \( [A] \neq [1] \).

(3) \( I = \mathcal{I}(\rho) = [A] \), where \( \rho \) is a partial character on \( \mathbb{Z}[x]^n \) and \( A = A(\rho) \).

Furthermore, \( A \) is a characteristic set of \( I \) and \( (f) \) is the support lattice of \( I \).

5 Criteria for prime, reflexive, and perfect Laurent binomial \( \sigma \)-ideals

In this section, we give criteria for a Laurent binomial \( \sigma \)-ideal to be prime, reflexive, well-mixed, and perfect in terms of its support lattice.

5.1 Reflexive and prime Laurent binomial \( \sigma \)-ideals

In this section, we first give criteria for reflexive and prime Laurent binomial \( \sigma \)-ideals and then give a decomposition theorem for perfect Laurent binomial \( \sigma \)-ideals.

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

\[
I_t = I \cap \mathbb{F}[Y^{[\pm t]}]
\]

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

Denote \( \mathbb{Z}[x]_t \) to be the set of elements in \( \mathbb{Z}[x] \) with degree \( \leq t \). Then \( \mathbb{Z}[x]_t^n \) is the \( \mathbb{Z} \)-module generated by \( x^i e_l \) 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 \( x^i e_l \) 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 \( \rho \) on \( \mathbb{Z}[x]_t^n \) becomes a partial character \( \rho_t \) on \( \mathbb{Z}^{n(t+1)} \).

Lemma 5.1 With the notations introduced above, we have \( I_t = I \cap \mathbb{F}[Y^{[\pm t]}] = \mathcal{I}(\rho_t) \).

Proof: It suffices to show that the support lattice of \( I_t \) is \( L_{\rho_t} = L_t \). By Lemma 4.17, \( Y^f - c_m \in I_t \) if and only if \( f \in L \cap \mathbb{Z}[x]_t^n \), or equivalently, \( \max_{m \in \text{deg}(m, x)} m \leq t \), which is equivalent to \( f \in L_t \). \( \square \)

Definition 5.2 Let \( L \) be a \( \mathbb{Z}[x] \)-module in \( \mathbb{Z}[x]^n \).

- \( L \) is called \( \mathbb{Z} \)-saturated if, for any \( a \in \mathbb{Z} \) and \( f \in \mathbb{Z}[x]^n \), if\( af \in L \) implies \( f \in L \).
• $L$ is called $x$-saturated if, for any $f \in \mathbb{Z}[x]^n$, $xf \in L$ implies $f \in L$.

• $L$ is called saturated if it is both $\mathbb{Z}$- and $x$-saturated.

**Theorem 5.3** Let $\rho$ be a partial character over $\mathbb{Z}[x]^n$. If $\mathcal{F}$ is algebraically closed and inversive, then

(a) $L_\rho$ is $\mathbb{Z}$-saturated if and only if $\mathcal{I}(\rho)$ is prime;

(b) $L_\rho$ is $x$-saturated if and only if $\mathcal{I}(\rho)$ is reflexive;

(c) $L_\rho$ 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 $\sigma$-ideal if and only if $\mathcal{I}_t$ is a Laurent prime ideal for all $t$. From Lemma 4.17, the support of $\mathcal{I}_t$ is $L_t$. Then by [7, Thm 2.1], $\mathcal{I}_t$ is a Laurent prime ideal if and only if $L_t$ is a $\mathbb{Z}$-saturated $\mathcal{Z}$-module. Furthermore, a $\mathbb{Z}[x]$-lattice $L$ is $\mathbb{Z}$-saturated if and only if $L_t$ is a $\mathbb{Z}$-saturated $\mathcal{Z}$-module for all $t$. Thus, (a) is valid.

(b): Suppose $\mathcal{I}$ is reflexive. For $xf \in L$, by Lemma 4.17, there is a $\mathcal{F}_x - c \in \mathcal{I}$. Since $\mathcal{F}$ is reflexive, $c = d^x$ for $d \in \mathcal{F}$. Then $\sigma(\mathcal{F} - d) \in \mathcal{I}$ and hence $\mathcal{F} - d \in \mathcal{I}$ since $\mathcal{I}$ is reflexive. By Lemma 4.17 again, $f \in L$ 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

$$f^x = \sum_{i=1}^{s} f_i (\mathcal{F}^i - c_i) \quad (21)$$

where $\mathcal{F}^i - c_i \in \mathcal{I}$ and $f_i \in \mathcal{F}\{\mathcal{F}^\pm\}$. Let $d = \max_{i=1}^{s} \deg(\mathcal{F}^i - c_i, y_1)$ and assume $\mathcal{F}^i = M_1 y_1^d$. Replace $y_d^i$ by $c_1/M_1$ in (21). Since (21) is an identity for the variables $y_d^{(j)}$, this replacement is meaningful and we obtain a new identity. $\mathcal{F}^i - c_1$ becomes zero after the replacement. Due to the way to chose $d$, if another summand, say $\mathcal{F}^2 - c_2$, is affected by the replacement, then $\mathcal{F}^2 = M_2 y_1^d$. After the replacement, $\mathcal{F}^2 - c_2$ becomes $c_1(M_2/M_1 - c_2/c_1)$ which is also in $\mathcal{I}$ by Lemma 4.17. In summary, after the replacement, the right hand side of (21) has less than $s$ summands and the left hand side of (21) does not changed. Repeat the above procedure, we will eventually obtain a new identity

$$f^x = \sum_{i=1}^{\tilde{s}} \tilde{f}_i (\mathcal{F}^i - \tilde{c}_i) \quad (22)$$

where $\mathcal{F}^i - \tilde{c}_i \in \mathcal{I}$ and $\tilde{f}_i \in \mathcal{F}\{\mathcal{F}^\pm\}$. We may assume that any $y_i$ does not appear in $\tilde{f}_i$. Otherwise, by setting $y_i$ to be $1$, the left hand side of (22) is not changes and a new identity is obtained. Since $\mathcal{F}$ is inversive, $\tilde{c}_i = e_1^2$ and $\tilde{f}_i = g_i^2$ for $e_i \in \mathcal{F}$ and $g_i \in \mathcal{F}\{\mathcal{F}^\pm\}$. By Lemma 4.17, $\mathcal{F}^i - c_i \in \mathcal{I}$ implies $xg_i \in L$. Since $L$ is $x$-saturated, $xg_i \in L$ and hence $\mathcal{F}^i - c_i \in \mathcal{I}$ by Lemma 4.17 again. From (22), $\sigma(f - \sum_{i=1}^{\tilde{s}} g_i(\mathcal{F}^i - e_i)) = 0$ and hence $f = \sum_{i=1}^{\tilde{s}} g_i(\mathcal{F}^i - e_i) \in \mathcal{I}$. (b) is proved. \qed
Definition 5.4 Let $L \subset \mathbb{Z}[x]^n$ be a $\mathbb{Z}[x]$-lattice. The $\mathbb{Z}$-saturation of $L$ is $\text{sat}_\mathbb{Z}(L) = \{ f \in \mathbb{Z}[x]^n \mid \exists a \in \mathbb{Z} \text{ s.t. } af \in L \}$. The $x$-saturation of $L$ is $\text{sat}_x(L) = \{ f \in \mathbb{Z}[x]^n \mid xf \in L \}$. The saturation of $L$ is $\text{sat}(L) = \{ f \in \mathbb{Z}[x]^n \mid \exists a \in \mathbb{Z}, \exists k \in \mathbb{N} \text{ s.t. } ax^kf \in L \}$.

It is clear that the $\mathbb{Z}$-saturation ($x$-saturation) of $L$ is $\mathbb{Z}$-saturated ($x$-saturated) and

$$\text{sat}(L) = \text{sat}_\mathbb{Z}(\text{sat}_x(L)) = \text{sat}_x(\text{sat}_\mathbb{Z}(L)).$$

Theorem 5.5 Let $I$ be a Laurent binomial $\sigma$-ideal and $L$ the support lattice of $I$. If $F$ is inversive, then the reflexive closure of $I$ is also a Laurent binomial $\sigma$-ideal whose support lattice is the $x$-saturation of $L$.

Proof: Let $I_x$ be the reflexive closure of $I$ and $L_x = \text{sat}_x(L)$. Suppose $I = \{ f_1, \ldots, f_r \}$, where $f_i = \mathbb{Y}^t_i - c_i$. Then $L = (f_1, \ldots, f_r)$. If $L$ is $x$-saturated, by Theorem 5.3, $I$ is reflexive. Otherwise, there exist $k_1 \in \mathbb{N}, b_i \in \mathbb{Z}[x]$, and $h_1 \in \mathbb{Z}[x]^n$ such that $h_1 \notin L$ and

$$x^{k_1}h_1 = \sum_{i=1}^r b_if_i \in L. \quad (23)$$

By Lemma 5.4, $x^{k_1}h_1 - \bar{a}$ is in $I$, where $\bar{a} = \prod_{i=1}^r c_i$. Since $F$ is inversive, $\bar{a} = \sigma^{-k_1}(\bar{a}) \in F$. Then, $\sigma^{k_1}(\mathbb{Y}^{h_1} - \bar{a}) \in I$, and hence $\mathbb{Y}^{h_1} - \bar{a} \in I_x$. Let $I_1 = \{ f_1, \ldots, f_r, \mathbb{Y}^{h_1} - \bar{a} \}$. It is clear that $L_1 = (f_1, \ldots, f_r, h_1)$ is the support lattice of $I_1$. Then $I \subset I_1 \subset I_x$ and $L \subset L_1 \subset L_x$. Repeating the above procedure for $I_1$ and $L_1$, we obtain $I_2$ and $L_2 = (f_1, \ldots, f_r, h_1, h_2)$ such that $h_2 \notin L_1$ and $x^{k_2}h_2 \in L_1$. We claim that $L_2 \subset L_x$. Indeed, let $x^{k_2}h_2 = \sum_{i=1}^r c_i f_i + c_0 h_1$. Then by (23), $x^{k_1+k_2}h_2 = x^{k_1}(x^{k_2}h_2) = x^{k_1} \sum_{i=1}^r c_i f_i + c_0 (x^{k_1}h_1) = x^{k_1} \sum_{i=1}^r c_i f_i + c_0 \sum_{i=1}^r b_i f_i \in L$ and the claim is proved. As a consequence, $L_2 \subset I_x$.

Continuing the process, we have $I \subset I_1 \subset \cdots \subset I_t \subset I_x$ and $L \subset L_1 \subset \cdots \subset L_t \subset L_x$ such that $L_t$ is the support lattice of $I_t$. The process will terminate, since $\mathbb{Z}[x]^n$ is Noetherian. The final $\mathbb{Z}[x]$-lattice $L_t$ is $x$-saturated and hence $I_t$ is reflexive by Theorem 5.3. Since $L_t$ 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 $I_t = I_x$. \qed

Corollary 5.6 Let $L \subset \mathbb{Z}[x]^n$ be a $\mathbb{Z}[x]$-lattice. Then $\text{rk}(L) = \text{rk}(\text{sat}_x(L))$ and $\text{rk}(L) = \text{rk}(\text{sat}_\mathbb{Z}(L))$.

Proof: From the proof of Theorem 5.5, $\text{sat}_x(L) = (L, h_1, \ldots, h_t)$ and for each $h_i$, there is a positive integer $n_i$ such that $x^{n_i}h_i \in L$. 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, $\text{rk}(A) = \text{rk}(B)$. We can prove $\text{rk}(L) = \text{rk}(\text{sat}_\mathbb{Z}(L))$ similarly. \qed

We now give a decomposition theorem for perfect $\sigma$-ideals.

Theorem 5.7 Let $I$ be a Laurent binomial $\sigma$-ideal, $L$ the support lattice of $I$, and $L_S$ the saturation of $L$. If $F$ is algebraically closed and inversive, then $\{ I \}$ is either $[1]$ or can be written as the intersection of Laurent reflexive prime binomial $\sigma$-ideals whose support lattice is $L_S$. 

18
Well-mixed and perfect Laurent binomial $\sigma$-ideals

In this section, we give criteria for a Laurent binomial $\sigma$-ideal to be well-mixed and perfect in terms of its support lattice and show that the well-mixed and perfect closures of a Laurent binomial $\sigma$-ideal are still binomial.

For $S \subseteq F\{\mathbb{Y}^{\pm}\}$, let $S' = \{fg^\pm \mid fg \in S\}$. 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 $\sigma$-ideal and is contained in every well-mixed $\sigma$-ideal containing $S$. Hence this union is $\langle S \rangle$. If $I \subseteq F\{\mathbb{Y}^{\pm}\}$ is a Laurent $\sigma$-ideal, then $\langle I \rangle$ is called the well-mixed closure of $I$. We first prove some basic properties of well-mixed $\sigma$-ideals. Note that these properties are also valid in $F\{\mathbb{Y}\}$.

Lemma 5.9 Let $I_1, \ldots, I_n$ be prime $\sigma$-ideals. Then $I = \cap_{i=1}^n I_i$ is a well-mixed $\sigma$-ideal.
Proof: It is obvious. \hfill \Box

Lemma 5.10 Let $S_1, S_2$ be two subsets of $\mathcal{F}\{\mathbb{Y}^\pm\}$ which satisfy $a \in S_i$ implies $\sigma(a) \in S_i$, $i = 1, 2$. Then $[S_1]_n[S_2]_n \subset [S_1S_2]_n$.

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, $f_1 g_1 f_2 g_2 \in [S_1S_2]$, and $st = f_1 f_2 (g_1 g_2)^x \in [S_1S_2]_1$. Hence, $[S_1]_1[S_2]_1 \subset [S_1S_2]_1$. By induction, $[S_1]_n[S_2]_n \subset [S_1S_2]_n$. \hfill \Box

Lemma 5.11 Let $S_1, S_2$ be two subsets of $\mathcal{F}\{\mathbb{Y}^\pm\}$ which satisfy $a \in S_i$ implies $\sigma(a) \in S_i$, $i = 1, 2$. Then $\sqrt{[S_1S_2]_n} = \sqrt{[S_1]_n \cap [S_2]_n}$ for $n \geq 1$, and $\sqrt{[S_1]_n} \cap \sqrt{[S_2]_n} = \sqrt{[S_1S_2]_n}$.

Proof: The last statement is an immediate consequence of the first one. Since $[S_1S_2]_n \subset [S_i]_n$ for $i = 1, 2$, and $[S_1S_2]_n \subset [S_1]_n \cap [S_2]_n$ follows. Hence, $\sqrt{[S_1S_2]_n} \subset \sqrt{[S_1]_n \cap [S_2]_n}$. Let $a \in [S_1]_n \cap [S_2]_n$ we have $a^2 \in [S_1S_2]_n$. By Lemma 5.10, $a^2 \in [S_1S_2]_n$. Hence $a \in \sqrt{[S_1S_2]_n}$, and $\sqrt{[S_1]_n \cap [S_2]_n} \subset \sqrt{[S_1S_2]_n}$ follows. \hfill \Box

Lemma 5.12 Let $\mathcal{I}_1, \ldots, \mathcal{I}_m$ be Laurent $\sigma$-ideals. Then $\sqrt{\cap_{i=1}^m \mathcal{I}_i} = \cap_{i=1}^m \sqrt{\mathcal{I}_i}$.

Proof: Let $\mathcal{I} = \cap_{i=1}^m \mathcal{I}_i$. Then $\sqrt{\mathcal{I}} = \sqrt{\prod_{i=1}^m \mathcal{I}_i}$. By Lemma 5.11, we have $\sqrt{\prod_{i=1}^m \mathcal{I}_i} = \sqrt{\prod_{i=1}^{m-1} \mathcal{I}_i \cap \sqrt{\mathcal{I}_n} = \ldots = \cap_{i=1}^m \sqrt{\mathcal{I}_i}}$. Now we show that $\sqrt{\mathcal{I}} = \cap_{i=1}^m \sqrt{\mathcal{I}_i}$. Since $\prod_{i=1}^m \mathcal{I}_i \subset \mathcal{I}$, we have $\sqrt{\prod_{i=1}^m \mathcal{I}_i} \subset \sqrt{\mathcal{I}}$. By Lemma 5.11, $\sqrt{\mathcal{I}} = \sqrt{\mathcal{I}_1 \cap \cdots \cap \sqrt{\mathcal{I}}} = \sqrt{\prod_{i=1}^m \mathcal{I}_i}$, and hence $\sqrt{\mathcal{I}} = \cap_{i=1}^m \sqrt{\mathcal{I}_i}$. Then, $\sqrt{\mathcal{I}} = \cap_{i=1}^m \sqrt{\mathcal{I}_i}$. \hfill \Box

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

Lemma 5.13 Let $\zeta_m = e^{2\pi i \frac{m}{m}}$ be the primitive $m$-th root of unity, where $i = \sqrt{-1}$ and $m \in \mathbb{Z}_{\geq 2}$. If $\mathcal{F}$ is algebraically closed, 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 $\sigma$-ideal $\{y^m - 1\}$ in $\mathcal{F}\{y\}$ is

$$\{y^m - 1\} = \{y^m - 1, y^x - y^{o_m}\}$$

(25)

where $y$ is a $\sigma$-indeterminate.

Proof: Since $\mathcal{F}$ is algebraically closed, $\zeta_m$ is in $\mathcal{F}$. From $y^m - 1 = \prod_{j=0}^{m-1} (y - \zeta_m^j) = 0$, we have $\sigma(y^m - 1) = \prod_{j=0}^{m-1} (\sigma(y) - \zeta_m^j) = 0$. Then, there exists an $o_m$ such that $0 \leq o_m \leq m - 1$ 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 $\sigma(\zeta_m) = \zeta_m^{o_m} = \zeta_m^{dk} = \zeta_m^{km} = 1$, which implies $\zeta_m^s = 1$, a contradiction.

By the difference Nullstellensatz \cite[1, p.87]{null}, we have $\{y^m - 1\} = \cap_{j=0}^{m-1} [y - \zeta_m^j]$. In order to show (25), it suffices to show $\cap_{j=0}^{m-1} [y - \zeta_m^j] = [y^m - 1, y^x - y^{o_m}]$. Since $y^x - y^{o_m} = (y - \zeta_m^j)^x + \zeta_m^j y^{o_m} = (y - \zeta_m^j)^x + \zeta_m^{o_m} y^{o_m} \in [y - \zeta_m^j]$ for any $0 \leq j \leq m - 1$, 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
The number \( o_m \) introduced in Lemma 5.13 depends on \( F \) only and is called the \( m \)-th transforming degree of unity. In the following corollaries, \( F \) is assumed to be algebraically closed and hence \( o_m \) is fixed for any \( m \in \mathbb{N} \). From the proof of Lemma 5.13, we have

**Corollary 5.14** \( y^x - y^{o_m} \in \cap_{j=0}^{m-1} [y - \zeta_j^m] \).

**Corollary 5.15** For \( n, m, k \) in \( \mathbb{N} \), if \( n = km \) then \( o_n = o_m \mod m \).

**Proof:** By definition, \( \zeta_n^k = \zeta_m \). Then, \( \sigma(\zeta_n^k) = \zeta_n^{k o_m} = \zeta_m^{o_m} \). From, \( \sigma(\zeta_n^k) = \sigma(\zeta_m) = \zeta_m^{o_m} \), we have \( \zeta_m^{o_m} = \zeta_m^{o_m} \). Then \( o_n = o_m \mod m \).

**Lemma 5.16** \( \langle y^m - 1 \rangle = \{ y^m - 1 \} = [y^m - 1, y^x - y^{o_m}] \).

**Proof:** By Lemma 5.13 it suffices to show \( y^x - y^{o_m} \in (y^m - 1) \). Since \( y^m - 1 = \prod_{j=0}^{m-1} (y - \zeta_j^m) \) and \( (y - \zeta_j^m)^x = [y^x - \zeta_j^{o_m}] \), we have \( f_i = (y^x - \zeta_j^{o_m}) \prod_{0 \leq j \leq m-1, j \neq i} (y - \zeta_j^m) \in (y^m - 1) \) 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 \( \frac{1}{y^m - 1} = \sum_{i=0}^{m-1} \frac{1}{m(\zeta_m)^m - 1} \). For \( y^m - 1 \) from [11, p. 494]. We have

\[
\frac{1}{m} \sum_{i=0}^{m-1} \zeta_{m}^i f_i = \frac{1}{m} \sum_{i=0}^{m-1} \zeta_{m}^i \frac{y^m - 1}{y - \zeta_m^i} (y^x - \zeta_m^{o_m}) = \frac{1}{m} \sum_{i=0}^{m-1} \zeta_{m}^i \frac{y^m - 1}{y - \zeta_m^{o_m}} y^x = \frac{1}{m} \sum_{i=0}^{m-1} \zeta_{m}^i \frac{y^m - 1}{y - \zeta_m^{o_m}} = y^x - \frac{1}{m} \sum_{i=0}^{m-1} \frac{y^m - 1}{y - \zeta_m^{o_m}} \zeta_{m}^i \zeta_{m}^{(o_m+1)i}.
\]

Let \( g(y) = \frac{1}{m} \sum_{i=0}^{m-1} \frac{y^m - 1}{y - \zeta_m^{o_m}} \zeta_{m}^i \zeta_{m}^{(o_m+1)i} \). Then, \( g(\zeta_m) = \frac{1}{m} \sum_{i=0}^{m-1} \frac{y^m - 1}{y - \zeta_m^{o_m}} |_{y=\zeta_m} = \frac{1}{m} \sum_{i=0}^{m-1} \zeta_{m}^i \zeta_{m}^{(o_m+1)i} \). From \( y^x - y^{o_m} \in (f_0, \ldots, f_{m-1}) \), we have \( g(y) = y^{o_m} \). Hence \( y^x - y^{o_m} \in (f_0, \ldots, f_{m-1}) \in \langle y^m - 1 \rangle \).

**Corollary 5.17** For \( m \in \mathbb{N} \), \( a \in F^* \), and \( f \in \mathbb{Z}[x]^n \), we have \( \langle y^{x-o_m} f - a^{x-o_m} \rangle \in \langle y^{mf} - a^m \rangle \).

**Proof:** Let \( z = \frac{y^f}{a} \) and \( I = \langle y^{mf} - a^m \rangle \). Then \( z^{m-1} \in I \). By Lemma 5.16 \( z^{x-o_m} - 1 \in \langle z^{m-1} \rangle \). Then \( \langle y^f \rangle^{x-o_m} - 1 \in I \) or \( y^{x-o_m} f - a^{x-o_m} \in I \).
Let $F = \mathbb{Q}(\sqrt{-3})$ and $p = y_2^3 - 1$. Following Lemma 5.13, if $\sigma(\sqrt{-3}) = \sqrt{-3}$, we have $o_3 = 1$ and $\langle p \rangle = \{p\} = [p, y_1^3 - y_1]$. If $\sigma(\sqrt{-3}) = -\sqrt{-3}$, we have $o_3 = 2$ and $\langle p \rangle = \{p\} = [p, y_1^3 - y_1^2]$.

Motivated by Corollary 5.17, we have the following definition.

**Definition 5.19** If a $\mathbb{Z}[x]$-lattice $L$ satisfies

\[mf \in L \Rightarrow (x - o_m)f \in L\]  \hspace{1cm} (26)

where $m \in \mathbb{N}$, $f \in \mathbb{Z}[x]^n$, and $o_m$ is defined in Lemma 5.13, then it is called M-saturated. 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 $\text{sat}_M(L)$.

The following result gives an effective version for condition (26).

**Lemma 5.20** A $\mathbb{Z}[x]^n$-lattice $L$ is M-saturated if and only if the following condition is true: Let $L_1 = \text{sat}_M(L) = (g_1, \ldots, g_s)$ such that $m_i g_i \in L$ for $m_i \in \mathbb{N}$. Then $(x - o_{m_i})g_i \in L$.

**Proof:** We need only to show $(x - o_{m_i})g_i \in L$ implies (26). For any $mf \in L$, we have $f \in L_1$ and hence $f = \sum_{i=1}^r q_i g_i$, where $q_i \in \mathbb{Z}[x]$. Let $t = \text{lcm}(m, m_1, \ldots, m_s)$. By Corollary 5.15, we have $o_t = o_{m_i} + c m_i$, where $c_i \in \mathbb{Z}$. Then $(x - o_t)f = \sum_{i=1}^r q_i (x - o_t)g_i = \sum_{i=1}^r q_i (x - o_{m_i})g_i - \sum_{i=1}^r q_i c_i m_i g_i \in L$. By Corollary 5.15, $o_t = o_{m_i} + c m_i$, where $c \in \mathbb{Z}$. Then $(x - o_{m_i})f = (x - o_t)f + c mf \in L$. \hfill $\Box$

We now give a criterion for a Laurent binomial $\sigma$-ideal to be well-mixed.

**Theorem 5.21** Let $\rho$ be a partial character and $\mathcal{F}$ an algebraically closed and inverse $\sigma$-field. If $\mathcal{I}(\rho)$ is well-mixed, then $L_\rho$ is M-saturated. Conversely, if $L_\rho$ is M-saturated, then either $\mathcal{I}(\rho) = [1]$ or $\mathcal{I}(\rho)$ is well-mixed.

**Proof:** Suppose that $\mathcal{I}(\rho)$ is well-mixed. If there exists an $m \in \mathbb{N}$ such that $mf \in L_\rho$, then by Lemma 4.17, there exists a $c \in F^*$ such that $Y^mf - c \in \mathcal{I}(\rho)$. Since $F$ is algebraically closed, there exists an $a \in F^*$ such that $c = a^m$. Then, $Y^mf - a^m \in \mathcal{I}(\rho)$. Since $\mathcal{I}(\rho)$ is well-mixed, by Corollary 5.17, $Y^{(x-o_m)f} - a^{x-o_m} \in \mathcal{I}(\rho)$, and by Lemma 4.17 again, $(x - o_m)f \in L_\rho$ follows and $L_\rho$ is M-saturated.

Conversely, let $L_\rho$ be M-saturated. If $L_\rho$ is Z-saturated, then by Theorem 5.3, $\mathcal{I}(\rho)$ is prime and hence well-mixed by Lemma 5.9. Otherwise, there exists an $m_1 \in \mathbb{N}$, and $f \in \mathbb{Z}[x]^n$ such that $f \not\in L_\rho$ and $m_1 f \in L_\rho$. By Lemma 4.17, there exists an $a \in F^*$ such that $Y^{m_1 f} - a^{m_1} \in \mathcal{I}(\rho)$. We claim that either $\langle \mathcal{I}(\rho) \rangle = [1]$ or

\[\mathcal{I}(\rho) = \bigcap_{l_1=0}^{n_1-1} \mathcal{I}_{l_1}\]  \hspace{1cm} (27)

where $\mathcal{I}_{l_1} = [\mathcal{I}(\rho), Y^f - a^{\zeta_{m_1}}]$ and $\zeta_{m_1} = e^{2\pi i}{m_1}$. By (26), $(x - o_{m_1})f \in L_\rho$. By Lemma 4.17, there exists a $b \in F^*$ such that $Y^{(x-o_{m_1})f} - b \in \mathcal{I}(\rho)$. Since $Y^{m_1 f} - a^{m_1} \in \mathcal{I}(\rho)$, by Corollary 5.14, we have $Y^{(x-o_{m_1})f} - a^{x-o_{m_1}} \in [Y^f - a^{\zeta_{m_1}}]$ for any $l_1$. Then $b - a^{x-o_{m_1}} = \ldots$
\( \text{we have either} \)

\[
\begin{align*}
\gamma^{(x-o_{m_1})} f - a^{x-o_{m_1}} \in \mathcal{I}_{l_1} & \quad \text{for any } l_1. & \text{If } b \neq a^{x-o_{m_1}} \text{, } \mathcal{I}_{l_1} = [1] \text{ for all } l_1, \\
\text{and hence } 1 \in \bigcap_{l_1=0}^{m_{l_1}} \mathcal{I}_{l_1} & \subset \langle \mathcal{I}(\rho) \rangle \text{ by Lemma } 5.16 \\
\text{and there follows. } \text{Now suppose } & \begin{cases} \text{b \in a^{x-o_{m_1}}} \text{ or } a^x \in b. \\
\text{To prove } (27), \text{ it suffices to show } \cap_{l_1=0}^{m_{l_1}} \mathcal{I}_{l_1} \subset \langle \mathcal{I}(\rho) \rangle. \\
\text{Let } f \in \bigcap_{l_1=0}^{m_{l_1}} \mathcal{I}_{l_1}. \text{ From } f \in \mathcal{I}_{l_1}, \text{ we have } f = f_{l_1} + \sum_{j=0}^{s} p_j \sigma^j (\gamma f - a \zeta_{1_{m_1}}), \text{ where } f_{l_1} \in \mathcal{I}(\rho). \text{ By Lemma } 5.13, \sigma(\zeta_{m_1}) = \zeta_{m_1}. \text{ We thus have} \\
\sigma(\gamma f - a \zeta_{1_{m_1}}) = \gamma f - b \gamma^{(x-o_{m_1})} f + b \gamma^{(x-o_{m_1})} f - \sigma(a \zeta_{1_{m_1}}) \\
= \gamma^{(x-o_{m_1})} f (\gamma^{(x-o_{m_1})} f - b) + (\gamma^{(x-o_{m_1})} f - a \zeta_{1_{m_1}}) + (ba^{(x-o_{m_1})} - a f) \zeta_{1_{m_1}}.
\end{cases}
\end{align*}
\]

Since \( \gamma^{(x-o_{m_1})} f - b \in \mathcal{I}(\rho) \) and \( ba^{(x-o_{m_1})} - \sigma(a) = ba^{(x-o_{m_1})} - a^x = 0 \), we have \( \sigma(\gamma f - a \zeta_{1_{m_1}}) = g_{l_1} + q_{l_1} (\gamma f - a \zeta_{1_{m_1}}), \) where \( g_{l_1} \in \mathcal{I}(\rho) \). Using the above equation repeatedly, we have \( f = h_{l_1} + p_{l_1} (\gamma f - a \zeta_{1_{m_1}}), \) where \( h_{l_1} \in \mathcal{I}(\rho) \). Then, \( f_{l_1} = \prod_{l_1=0}^{m_{l_1}-1} (h_{l_1} + p_{l_1} (\gamma f - a \zeta_{1_{m_1}})) = s + \prod_{l_1=0}^{m_{l_1}-1} p_{l_1} (\gamma f - a \zeta_{1_{m_1}}) = \gamma^{(x-o_{m_1})} f \sum_{l_1=0}^{m_{l_1}-1} p_{l_1} \in \mathcal{I}(\rho), \) where \( s \) is in \( \mathcal{I}(\rho) \). By Corollary 5.10, we have \( f \in \mathcal{I}(\rho) \). The claim is proved.

The support lattice for any of \( \mathcal{I}_{l_1} \) is \( L_1 = (L_\rho, \sigma) \). Similar to the proof of Theorem 5.3, we can show that \( \mathcal{I}(\rho) \not\subset \mathcal{I}_{l_1} \) and \( L_\rho \not\subset L_1 \). If \( L_1 \) is not \( \mathbb{Z} \)-saturated, there exists a \( k > 1 \) and \( g \in \mathbb{Z}[x^m] \) such that \( g \notin L_1 \) and \( kg \notin L_1 \). Let \( m_2 = km_1 \). We have \( m_2 g = km_1 g \in L_\rho \) and there exists a \( c \in F^* \) such that \( \gamma^{(x-o_{m_2})} c^{m_2} \in \mathcal{I}(\rho) \). Hence, \( (x-o_{m_2}) g \in L_\rho \subset L_1 \) and there exists a \( c \in F^* \), such that \( \gamma^{(x-o_{m_2})} c - d \in I(\rho) \). Let \( L_2 = (L_1, g) \) and \( \mathcal{I}_{l_1,l_2} = [I_{l_1}, \gamma g - c^{l_{m_2}}, l_2 = 0, \ldots, m_2 - 1]. \) Then \( L_1 \not\subset L_2 \) 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 \( \mathcal{I}_{l_1,l_2} = [1] \) by Lemma 5.16. Since Laurent binomial \( \sigma \)-ideals are radical, \( \mathcal{I}(\rho) = \bigcap_{l_1=0}^{m_{l_1}-1} \mathcal{I}_{l_1} = [1] \) by Lemma 5.12 and (27). If \( d - c^{(x-o_{m_2})} = 0 \), it can be similarly proved that \( \mathcal{I}_{l_1} = \bigcap_{l_2=0}^{m_{l_2}-1} \mathcal{I}_{l_1,l_2} \) for any \( l_1 \). As a consequence, we have either \( \langle \mathcal{I}(\rho) \rangle = [1] \) or \( \mathcal{I}(\rho) = \bigcap_{l_1=0}^{m_{l_1}-1} \mathcal{I}_{l_1} = \bigcap_{l_1=0}^{m_{l_1}-1} \mathcal{I}_{l_1,l_2} \).

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

\[
\mathcal{I}(\rho) = \bigcap_{l_1=0}^{m_{l_1}-1} \mathcal{I}_{l_1} = \cdots = \bigcap_{l_1=0}^{m_{l_1}-1} \mathcal{I}_{l_1, \ldots, l_t}
\]

where \( L_\rho \not\subset L_1 \not\subset \cdots \not\subset L_t \subset sat_\mathbb{Z}(L_\rho). \) Since \( \mathbb{Z}[x]^n \) is Noetherian, the procedure will terminate and \( L_t \) is \( \mathbb{Z} \)-saturated. Since each \( \mathcal{I}_{l_1, \ldots, l_t} \) is either \([1] \) or a prime \( \sigma \)-ideal, and hence either \( \langle \mathcal{I}(\rho) \rangle = [1] \) or \( \mathcal{I}(\rho) \) is well-mixed by Lemma 5.9. □

The following example shows that \( \langle \mathcal{I}(\rho) \rangle = [1] \) can indeed happen in Theorem 5.21.

Example 5.22 Let \( \mathcal{I} = [A] \), where \( A = \{ y_1^2 + 1, y_1^2 - y_1, y_1^2 + 1, y_2^2 + y_2 \} \) is a \( \sigma \)-chain. The support lattice of \( \mathcal{I} \) is \( M \)-saturated. We have \( y_2^2 - y_1^2 = y_2^2 + 1 - (y_1^2 + 1) \in \mathcal{I} \). Then by Corollary 5.17, \( y_1 y_2 - y_1^2 y_2 \in \mathcal{I} \). From \( y_1^2 - y_1, y_2^2 + y_2 \in \mathcal{I} \), we have \( y_1 y_2 \in \mathcal{I} \) and hence \( 1 \in \mathcal{I} \). This also shows that a binomial \( \sigma \)-ideal is generally not well-mixed.

Theorem 5.23 Let \( \mathcal{F} \) be an algebraically closed and inversive \( \sigma \)-field and \( \mathcal{I} = \mathcal{I}(\rho) \) a Laurent binomial \( \sigma \)-ideal. Then the well-mixed closure of \( \mathcal{I} \) is either \([1]\) or a Laurent binomial \( \sigma \)-ideal whose support lattice is \( sat_M(L_\rho) \).
Proof: Suppose that $\langle I(\rho) \rangle \neq \{1\}$. If $L$ is not M-saturated, then there exists an $m \in \mathbb{N}$ and $f \in \mathbb{Z}[x]^n$ such that $f \not\in L$, $mf \in L$, and $(x-o_m)f \not\in L$. By Lemma 4.17 there exists a $c \in \mathcal{F}$ such that $v^{mf} - c^{o_m} \in I(\rho)$. Let $I_1 = [I, y^{(x-o_m)f} - c^{x-o_m}]$ and $L_1 = (L, (x-o_m)f)$. By Corollary 5.17 $y^{(x-o_m)f} - c^{x-o_m} \in (I(\rho))$. Let $L_M = \text{sat}_M(L)$. Then $I \subsetneq I_1 \subsetneq I$ and $L \not\subset L_1 \subset L_M$. Repeat the procedure to construct $I_i$ and $L_i$ for $i = 2, \ldots, t$ such that $I \subsetneq I_1 \subsetneq \cdots \subsetneq I_t \subsetneq \cdots \subsetneq I_t \subsetneq L_M$. Since $\mathbb{Z}[x]^n$ is Noetherian, the procedure will terminate at, say $t$. Then $L_t = L_M$ is M-saturated. By Lemma 5.27 $L_t$ is also $x$-saturated. By Theorem 5.21 $I_t \subset (I)$ is well-mixed and hence $I_t = (I)$.

By the proof of Theorem 5.21 we have

**Corollary 5.24** A $\mathbb{Z}[x]$-lattice and its M-saturation have the same rank.

**Example 5.25** Let $p = y_2^2 - y_1^2$. Following the proof of Theorem 5.21, it can be shown that $\langle p \rangle = \{p\} = [y_1^2 y_2^2 - 1, y_1^{2} x^{2} y_2^2 - 1] = [y_2^2 - y_1^2, y_1 y_2^2 - y_1^2 y_2]$.

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

**Definition 5.26** 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 $\text{sat}_P(L)$.

**Lemma 5.27** For any $\mathbb{Z}[x]$-lattice $L$, $\text{sat}_P(L) = \text{sat}_x(\text{sat}_M(L)) = \text{sat}_M(\text{sat}_x(L))$.

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

For the other direction, we claim that $L_2$ is $x$-saturated. Let $xf \in \text{sat}_M(\text{sat}_x(L)) \subset \text{sat}_x(\text{sat}_M(\text{sat}_x(L)))$. Then there exists an $m \in \mathbb{N}$ such that $mf \in \text{sat}_x(L)$ which implies $(x-o_m)f \in \text{sat}_M(\text{sat}_x(L))$ and hence $o_m f = xf - (x-o_m)f \in \text{sat}_M(\text{sat}_x(L))$ follows. By Lemma 5.13 $\gcd(o_m, m) = 1$. Then $f \in \text{sat}_M(\text{sat}_x(L))$, and the claim is true. Since $\text{sat}_M(L) \subset \text{sat}_M(\text{sat}_x(L)) = L_2 = \text{sat}_x(\text{sat}_M(\text{sat}_x(L)))$, we have $L_1 \subset L_2$.

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

**Theorem 5.28** Let $\rho$ be a partial character and $\mathcal{F}$ an algebraically closed and inversive $\sigma$-field. If $I(\rho)$ is perfect, then $L_\rho$ is P-saturated. Conversely, if $L_\rho$ is P-saturated, then either $\{I(\rho)\} = \{1\}$ or $I(\rho)$ is perfect. Furthermore, the perfect closure of $I(\rho)$ is either $\{1\}$ or a Laurent binomial $\sigma$-ideal whose support lattice is $\text{sat}_P(L_\rho)$.
Proof: If $I(\rho)$ is perfect, then it is well-mixed and reflexive. By Theorems 5.21 and Theorem 5.3, $L_\rho$ is M-saturated and $x$-saturated, and hence P-saturated. Conversely, if $L_\rho$ is P-saturated, it is M-saturated and $x$-saturated. By Theorem 5.21, either $\langle I(\rho) \rangle = [1]$ or $I(\rho)$ is well-mixed. If $\langle I(\rho) \rangle = [1]$, $\{ I(\rho) \} = [1]$. Otherwise, by Theorem 5.3 $I(\rho)$ is reflexive. By Corollary 4.10 $I(\rho)$ is radical. Then $I(\rho)$ is perfect.

By Lemma 5.27 $L_\rho = sat_P(L_\rho) = sat_M(sat_x(L_\rho))$. Then the perfect closure of $I(\rho)$ is the well-mixed closure of the reflexive closure of $I(\rho)$, and then is either [1] or a Laurent binomial $\sigma$-ideal whose support lattice is $L_P$ by Theorems 5.5 and 5.23. □

6 Binomial $\sigma$-ideal

6.1 Basic properties of binomial $\sigma$-ideal

In this section, it is shown that certain results from [7] can be extended to the difference case using the theory of infinite Gröbner basis.

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

$$f = a\mathbb{Y}^a + b\mathbb{Y}^b = a\mathbb{Y}^g \cdot (\mathbb{Y}^{f^+} - c\mathbb{Y}^{f^-}) \quad (28)$$

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

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

In this section, $\mathcal{F}\{\mathbb{Y}\}$ is considered as a polynomial ring in infinitely many algebraic variables $\Theta(\mathbb{Y}) = \{y_i^j, i = 1, \ldots, n; j \geq 0\}$ and denoted by $S = \mathcal{F}\{\Theta(\mathbb{Y})\}$. A theory of Gröbner basis in the case of infinitely many variables is developed in [14] and will be used in this section. For any $m \in \mathbb{N}$, denote $\Theta^{(m)}(\mathbb{Y}) = \{y_i^j, i = 1, \ldots, n; j = 0, 1, \ldots, m\}$ and $S^{(m)} = \mathcal{F}\{\Theta^{(m)}(\mathbb{Y})\}$ is a polynomial ring in finitely many variables.

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

Let $I$ be a $\sigma$-ideal in $\mathcal{F}\{\mathbb{Y}\}$. Then $I$ is an algebraic ideal in $S$. By [14], we have

Lemma 6.1 Let $I$ be a binomial $\sigma$-ideal in $\mathcal{F}\{\mathbb{Y}\}$. Then for a compatible monomial order, the reduced Gröbner basis $G$ of $I$ exists and satisfies

$$G = \cup_{m=0}^\infty G^{(m)} \quad (29)$$

where $G^{(m)} = G \cap S^{(m)}$ is the reduced Gröbner basis of $I^{(m)} = I \cap S^{(m)}$ in $S^{(m)}$.

Contrary to the Laurent case, a binomial $\sigma$-ideal may be infinitely generated, as shown by the following example.
Example 6.2 Let \( \mathcal{I} = \langle y_1^i y_2^j - y_1^j y_2^i : 0 \leq i < j \in \mathbb{N} \rangle \). It is clear that \( \mathcal{I} \) does not have a finite set of generators and hence a finite Gröbner basis. The Gröbner basis of \( \mathcal{I}^{(m)} = \mathcal{I} \cap \mathbb{Q}[y_1, y_2; y_1^1, y_2^1; \ldots; y_1^m, y_2^m] \)

is \( \{ y_1^i y_2^j - y_1^j y_2^i : 0 \leq i < j \leq m \} \) with a monomial order satisfying \( y_1 < y_2 < y_1^1 < y_2^1 < \cdots < y_1^m < y_2^m \). Then \( \{ y_1^i y_2^j - y_1^j y_2^i : 0 \leq i < j \in \mathbb{N} \} \) is an infinite reduced Gröbner basis for \( \mathcal{I} \) in the sense of [14] when \( y_1^1, y_2^1 \) are treated as independent algebraic variables.

Remark 6.3 The above concept of Gröbner basis does not consider the difference structure. The concept may be refined by introducing the reduced \( \sigma \)-Gröbner basis [12]. A \( \sigma \)-monomial \( M_1 \) is called reduced w.r.t. another \( \sigma \)-monomial \( M_2 \) if there do not exist a \( \sigma \)-monomial \( M_0 \) and a \( k \in \mathbb{N} \) such that \( M_1 = M_0 M_2^k \). Then the reduced \( \sigma \)-Gröbner basis of \( \mathcal{I} \) in Example 6.2 is \( \{ y_1 y_2 - y_1 x_2 : i \in \mathbb{Z}_{\geq 1} \} \) which is still infinite. Since the purpose of Gröbner basis in this paper is theoretic and not computational, we will use the version of infinite Gröbner basis in the sense of [14].

With Lemma 6.1, a large portion of the properties for algebraic binomial ideals proved by Eisenbud and Sturmfels in [7] 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 \( \mathcal{I}^{(m)} \), and then the corresponding statement from [7] will be used to show that the property is indeed valid for \( \mathcal{I}^{(m)} \). We will illustrate the procedure in the following corollary. For other results, we omit the proofs.

Corollary 6.4 Let \( \mathcal{I} \subset \mathcal{F}\{\mathcal{Y}\} \) be a binomial \( \sigma \)-ideal. Then the Gröbner basis \( \mathcal{G} \) of \( \mathcal{I} \) consists of \( \sigma \)-binomials and the normal form of any \( \sigma \)-term modulo \( \mathcal{G} \) is again a \( \sigma \)-term.

Proof: By a \( \sigma \)-term, we mean the multiplication of an element from \( \mathcal{F}* \) and a \( \sigma \)-monomial. By [29], it suffices to show that corollary is valid for all \( \mathcal{G}^{(m)} \), that is, the Gröbner basis \( \mathcal{G}^{(m)} \) of \( \mathcal{I}^{(m)} \) consists of binomials and the normal form of any term modulo \( \mathcal{G}^{(m)} \) is again a term. Since \( \mathcal{G}^{(m)} \) is the Gröbner basis of \( \mathcal{I}^{(m)} = \mathcal{I} \cap \mathcal{S}^{(m)} \) and \( \mathcal{I}^{(m)} \) is a binomial ideal in a polynomial ring with finitely many variables, the corollary follows from Proposition 1.1 in [7].

\[ \square \]

Corollary 6.5 A \( \sigma \)-ideal \( \mathcal{I} \) is binomial if and only if the reduced Gröbner basis for \( \mathcal{I} \) consists of \( \sigma \)-binomials.

Corollary 6.6 If \( \mathcal{I} \) is a binomial \( \sigma \)-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 6.7 If \( \mathcal{I} \) and \( \mathcal{J} \) are binomial \( \sigma \)-ideals in \( \mathcal{F}\{\mathcal{Y}\} \) then we have \( \mathcal{I} \cap \mathcal{J} = [t\mathcal{I} + (1 - t)\mathcal{J}] \cap \mathcal{F}\{\mathcal{Y}\} \) where \( t \) is a new \( \sigma \)-indeterminate.

The intersection of binomial \( \sigma \)-ideals is not binomial in general, but from Lemma 6.7 and [7] we have
Corollary 6.8 If $\mathcal{I}$ and $\mathcal{I}'$ are binomial $\sigma$-ideals and $\mathcal{J}_1, \ldots, \mathcal{J}_s$ are $\sigma$-ideals generated by $\sigma$-monomials, then $[\mathcal{I} + \mathcal{I}'] \cap [\mathcal{I} + \mathcal{J}_1] \cap \ldots \cap [\mathcal{I} + \mathcal{J}_s]$ is binomial.

Corollary 6.9 Let $\mathcal{I}$ be a binomial $\sigma$-ideal and let $\mathcal{J}_1, \ldots, \mathcal{J}_s$ be monomial $\sigma$-ideals.

(a) The intersection $[\mathcal{I} + \mathcal{J}_1] \cap \cdots \cap [\mathcal{I} + \mathcal{J}_s]$ is generated by $\sigma$-monomials modulo $\mathcal{I}$.

(b) Any $\sigma$-monomial in the sum $\mathcal{I} + \mathcal{J}_1 + \cdots + \mathcal{J}_s$ lies in one of the $\sigma$-ideals $\mathcal{I} + \mathcal{J}_i$.

Corollary 6.10 If $\mathcal{I}$ is a binomial $\sigma$-ideal, then for any $\sigma$-monomial $M$, the $\sigma$-ideal quotients $[\mathcal{I} : M]$ and $[\mathcal{I} : M^\infty]$ are binomial.

Corollary 6.11 Let $\mathcal{I}$ be a binomial $\sigma$-ideal and $\mathcal{J}$ a monomial $\sigma$-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 [7, Theorem 3.1], we have

Theorem 6.12 If $\mathcal{I}$ is a binomial $\sigma$-ideal, then the radical of $\mathcal{I}$ is binomial.

Finally, we consider the reflexive closure of binomial $\sigma$-ideals.

Lemma 6.13 A binomial $\sigma$-ideal $\mathcal{I}$ is reflexive if and only if $b^x \in \mathcal{I} \Rightarrow b \in \mathcal{I}$ for any $\sigma$-binomial $b \in \mathcal{F}\{\mathcal{Y}\}$.

**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 $\sigma$-binomial $b$ then $\mathcal{I}$ is reflexive. Let $p$ be a $\sigma$-polynomial such that $p^x \in \mathcal{I}$. Then, there exists an $m \in \mathbb{N}$ such that $p^x \in \mathcal{I}^{(m)} = \mathcal{I} \cap S^{(m)}$. Let $\mathcal{G}$ be the (finite) reduced Gröbner basis of $\mathcal{I}^{(m)}$ in $S^{(m)}$ under the variable order $y_i^x < y_k$ for any $i, k, j > 0$. By Proposition 1.1 in [7], $\mathcal{G}$ consists of binomials. $p^x$ can be reduced to zero by $\mathcal{G}$. Due to the chosen variable order, we have $p^x = \sum_i e_i g_i^x$, where $e_i \in S^{(m)}$ and $g_i^x$ is a $\sigma$-binomial in $S^{(m)}$. Since $g_i^x$ are $\sigma$-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. \hfill $\square$

Theorem 6.14 If $\mathcal{I}$ is a binomial $\sigma$-ideal, then the reflexive closure of $\mathcal{I}$ is binomial.

**Proof:** Let $\mathcal{I}_1$ be the $\sigma$-ideal generated by the $\sigma$-binomials $p$ such that $p^x \in \mathcal{I}$ 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 $\sigma$-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 6.13. \hfill $\square$

### 6.2 Normal binomial $\sigma$-ideal

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

Let $\mathfrak{m}$ be the multiplicative set generated by $y_i^x$ for $i = 1, \ldots, n, j \in \mathbb{N}$. A $\sigma$-ideal $\mathcal{I}$ is called normal if for $M \in \mathfrak{m}$ and $p \in \mathcal{F}\{\mathcal{Y}\}$, $Mp \in \mathcal{I}$ implies $p \in \mathcal{I}$. For any $\sigma$-ideal $\mathcal{I}$,

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

27
is a normal $\sigma$-ideal. For any $\sigma$-ideal $I$ in $\mathcal{F}\{Y\}$, it is easy to check that

$$\mathcal{F}\{Y^\pm\}I \cap \mathcal{F}\{Y\} = I : m.$$  \hspace{1cm} (30)

We first prove a property for general normal $\sigma$-ideals.

**Lemma 6.15** A normal $\sigma$-ideal $I$ in $\mathcal{F}\{Y\}$ is reflexive (radical, well-mixed, perfect, prime) if and only if $\mathcal{F}\{Y^\pm\}I$ is reflexive (radical, well-mixed, perfect, prime) in $\mathcal{F}\{Y^\pm\}$.

**Proof:** Let $\mathcal{T} = \mathcal{F}\{Y^\pm\}I$ be a Laurent $\sigma$-ideal. Since $I$ is normal, from (30) we have $\mathcal{T} \cap \mathcal{F}\{Y\} = I$. If $\mathcal{T}$ is reflexive, it is clear that $I$ is reflexive. For the other direction, if $f^x \in \mathcal{T}$, then by clearing denominators of $f^x$, there exists a $\sigma$-monomial $M^x$ in $Y$ such that $M^x f^x \in \mathcal{T} \cap \mathcal{F}\{Y\} = I$. Since $I$ is reflexive, $M f \in I$ and hence $f \in \mathcal{T}$, that is, $\mathcal{T}$ is reflexive. The results about radical and perfect $\sigma$-ideals can be proved similarly.

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

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

$$I^+(\rho) = [Y^f+ - \rho(f)Y^f- \mid f \in L_\rho].$$ \hspace{1cm} (31)

We will show that any normal binomial $\sigma$-ideal can be written as the form (31).

**Lemma 6.16** Let $\rho$ be a partial character on $\mathbb{Z}[x]^n$ and $I(\rho)$ defined in (19). Then $I^+(\rho) = I(\rho) \cap \mathcal{F}\{Y\}$. As a consequence, $I^+(\rho)$ is proper and normal.

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

$$M f = \sum_{i=1}^s f_i N_i (Y^{f_i}_+ - \rho(f_i) Y^{f_i}_-) \in I^+(\rho),$$ \hspace{1cm} (32)

where $N_i$ is a $\sigma$-monomial in $Y$. We will prove $f \in I^+(\rho)$ from the above equation. Without loss of generality, we may assume that $M = y^c_-$ for some $c$ and $o \in \mathbb{N}$. Note that (32) is an algebraic identity in $y^k_i, i = 1, \ldots, n, k \in \mathbb{N}$. If $N_i$ contains $y^o_-$ as a factor, we move $F_i = f_i N_i (Y^{f_i}_+ - \rho(f_i) Y^{f_i}_-)$ to the left hand side of (32) and let $f_1 = f - F_i / y^c_+$. Then $f \in I^+(\rho)$ if and only if $f_1 \in I^+(\rho)$. Repeat the above procedure until no $N_i$ contains $y^c_-$ as a factor.

If $s = 0$ in (32), then $f = 0$ and the lemma is proved. Since $\gcd(Y^{f_1}_+, Y^{f_1}_-) = 1$, $y^c_-$ cannot be a factor of both $Y^{f_1}_+$ and $Y^{f_1}_-$. Let $Y^{f_1}_+$ be the largest $\sigma$-monomial in (32) not containing $y^c_-$ under a given $\sigma$-monomial total order. If $Y^{f_1}_-$ is the largest $\sigma$-monomial in (32) not containing $y^c_-$, the proving process is similar. There must exists another $\sigma$-binomial $f_j N_j (Y^{f_j}_+ - \rho(f_j) Y^{f_j}_-) \in I^+(\rho)$. Let $N_i = Y^{p_i}, N_j = Y^{p_j}$. Then
\[ \mathcal{Y}_{i_j}^{f_i^+} + p_i = \mathcal{Y}_{i_j}^{f_i^-} + p_j \] and \( f_i^+ + p_i = f_j^- + p_j \). We have \( p = f_i N_i (\mathcal{Y}_{i_j}^{f_i^+} - \rho(f_i)\mathcal{Y}_{i_j}^{f_i^-}) + f_j N_j (\mathcal{Y}_{i_j}^{f_j^+} - \rho(f_j)\mathcal{Y}_{i_j}^{f_j^-}) \). Since \( f = f_j^+ + p_j - (f_i^+ + p_i) = f_i^+ - f_i^- + f_j^+ = f_i + f_j \in L_\rho \), we have \( \mathcal{Y}_{i_j}^{f_i^+} + p_i = N(\mathcal{Y}_{i_j}^{f_i^+} - \rho(f)\mathcal{Y}_{i_j}^{f_i^-}) \in \mathcal{I}^+(\rho) \), where \( N \) is a \( \sigma \)-monomial. As a consequence, \( p \in \mathcal{I}^+(\rho) \). If \( N \) contains \( y_{\xi}^{x^o} \), move the term \( \frac{f_j}{\rho(f_j)} N(\mathcal{Y}_{i_j}^{f_i^+} - \rho(f)\mathcal{Y}_{i_j}^{f_i^-}) \) to the left hand side of (32) as we did in the first phase of the proof. After the above procedure, equation (32) is still valid. Furthermore, the number of \( \sigma \)-binomials in (32) does not increase, no \( N_i \) contains \( y_{\xi}^{x^o} \), and the largest \( \sigma \)-monomial \( \mathcal{Y}_{i_j}^{f_i^+} \) or \( \mathcal{Y}_{i_j}^{f_i^-} \) not containing \( y_{\xi}^{x^o} \) becomes smaller. The above procedure will stop after a finite number of steps, which means \( s = 0 \) in (32) and hence \( y_{\xi}^{x^o} f = 0 \) which means the original \( f \) is in \( \mathcal{I}^+(\rho) \). Then \( \mathcal{I}^+(\rho) = \mathcal{I}(\rho) \cap \mathcal{F}\{\mathcal{Y}\} \) is proper. For otherwise \( \mathcal{I}(\rho) = [1] \), contradicting to Lemma 4.16. Note that \( \mathcal{I}^+(\rho) \mathcal{F}\{\mathcal{Y}\} = \mathcal{I}(\rho) \). Then \( \mathcal{I}^+(\rho) = \mathcal{I}(\rho) \cap \mathcal{F}\{\mathcal{Y}\} = \mathcal{I}^+(\rho) \mathcal{F}\{\mathcal{Y}\} \cap \mathcal{F}\{\mathcal{Y}\} = \mathcal{I}^+(\rho) : m \), and \( \mathcal{I}^+(\rho) \) is normal. \( \square \)

Lemma 6.17 Let \( \rho \) be a partial character over \( \mathbb{Z}[x]^n \). Then \( \mathcal{Y}_{i_j}^{f_i^+} - c \mathcal{Y}_{i_j}^{f_i^-} \in \mathcal{I}^+(\rho) \) if and only if \( f \in L_\rho \) and \( c = \rho(f) \).

Proof: By Lemma 6.16, \( \mathcal{Y}_{i_j}^{f_i^+} - c \mathcal{Y}_{i_j}^{f_i^-} \in \mathcal{I}^+(\rho) \) if and only if \( \mathcal{Y}_{i_j}^{f} - c \in \mathcal{I}(\rho) \) which is equivalent to \( f \in L_\rho \) and \( c = \rho(f) \) by Lemma 4.17. \( \square \)

Lemma 6.18 If \( \mathcal{I} \) is a normal binomial \( \sigma \)-ideal, then there exists a unique partial character \( \rho \) on \( \mathbb{Z}[x]^n \) such that \( \mathcal{I} = \mathcal{I}^+(\rho) \) and \( L_\rho = \{ f \in \mathbb{Z}[x]^n | \mathcal{Y}_{i_j}^{f_i^+} - \rho(f)\mathcal{Y}_{i_j}^{f_i^-} \in \mathcal{I} \} \) which is called the support lattice of \( \mathcal{I} \).

Proof: We have \( \mathcal{I} \mathcal{F}\{\mathcal{Y}\} \cap \mathcal{F}\{\mathcal{Y}\} = \mathcal{I} : m \). By Theorem 4.18 there exists a partial character \( \rho \) such that \( \mathcal{I} \mathcal{F}\{\mathcal{Y}\} = \mathcal{I}(\rho) \). Then by Lemma 6.16 \( \mathcal{I} = (\mathcal{I} : m) = \mathcal{I} \mathcal{F}\{\mathcal{Y}\} \mathcal{F}\{\mathcal{Y}\} = \mathcal{I}(\rho) \mathcal{F}\{\mathcal{Y}\} = \mathcal{I}^+(\rho) \). By Lemma 6.17 we have \( L_\rho = \{ f \in \mathbb{Z}[x]^n | \mathcal{Y}_{i_j}^{f_i^+} - \rho(f)\mathcal{Y}_{i_j}^{f_i^-} \in \mathcal{I} \} = \mathcal{I}^+(\rho) \}. \) The uniqueness of \( \rho \) comes from the fact that \( L_\rho \) is uniquely determined by \( \mathcal{I} \). \( \square \)

By Lemmas 6.16 and 6.18 we have

Theorem 6.19 The map \( \mathcal{I}(\rho) \Rightarrow \mathcal{I}^+(\rho) \) gives a one to one correspondence between Laurent binomial \( \sigma \)-ideals in \( \mathcal{F}\{\mathcal{Y}\} \) and normal binomial \( \sigma \)-ideals in \( \mathcal{F}\{\mathcal{Y}\} \).

Due to Lemma 6.16 and Theorem 6.19 most properties of Laurent binomial \( \sigma \)-ideals can be extended to normal binomial \( \sigma \)-ideals. As a consequence of Corollary 4.10, Lemma 6.15, and Lemma 6.16 we have

Corollary 6.20 A normal binomial \( \sigma \)-ideal is radical.

As a consequence of Theorem 5.5, Lemma 6.15, and Theorem 6.19

Corollary 6.21 If \( \mathcal{F} \) is inversive, then the reflexive closure of \( \mathcal{I}^+(\rho) \) is also a normal binomial \( \sigma \)-ideal whose support lattice is the \( x \)-saturation of \( L_\rho \).
Corollary 6.22  If $\mathcal{F}$ is algebraically closed and inversive, then

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

Proof: It is easy to show that $\mathcal{I}(\rho) = \mathcal{I}^+(\rho) \mathcal{F}\{Y\pm\}$. Then the corollary is a consequence of Theorem 5.3, Lemma 6.15, and Lemma 6.16. □

For properties related with perfect $\sigma$-ideals, it becomes more complicated. Direct extension of Theorems 5.7, and 5.28 to the normal binomial case is not correct as shown by the following example.

Example 6.23 Let $\mathcal{I} = [y_1^2 - y_1, y_2^2 - y_1, y_2, y_2 + y_1]$ which is a normal binomial $\sigma$-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, $L_s = \text{sat}(L) = \begin{bmatrix} x - 1 \\ 0 \\ 1 \end{bmatrix}$. 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 5.28 are not correct. Theorem 5.7 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 $\sigma$-ideal is not necessarily normal.

It can be seen that the problem is due to the occurrence of $\sigma$-monomials. For any partial character $\rho$, it can be shown that

$$\{\mathcal{I}^+(\rho)\} : m = \{\mathcal{I}(\rho)\} \cap \mathcal{F}\{Y\}. \quad (33)$$

We thus have the following modifications for Theorems 5.28 and 5.7.

Corollary 6.24 Let $\mathcal{F}$ be an inversive and algebraically closed $\sigma$-field. If $\mathcal{I}^+(\rho)$ is perfect, then $L_\rho$ is $P$-saturated. Conversely, if $L_\rho$ is $P$-saturated, then either $\{\mathcal{I}\} : m = [1]$ or $\mathcal{I}$ is perfect. For any $\rho$, either $\{\mathcal{I}^+(\rho)\} : m = [1]$ or $\{\mathcal{I}^+(\rho)\} : m$ is a binomial $\sigma$-ideal whose support lattice is the $P$-saturation of $L_\rho$.

Proof: If $\mathcal{I}$ is perfect, by Lemma 6.15, $\mathcal{I}(\rho) = \mathcal{I}\mathcal{F}\{Y\pm\}$ is also perfect. By Theorem 5.28, $L_\rho$ is $P$-saturated and $x$-saturated, by Theorem 5.28, either $\mathcal{I}(\rho)$ is $\sigma$-saturated or $\mathcal{I}(\rho) = [1]$. If $\mathcal{I}(\rho)$ is perfect, by Lemma 6.15, $\mathcal{I} = \mathcal{I}^+(\rho)$ is also perfect. □

Similar results hold for normal well-mixed $\sigma$-ideals.

In the rest of this section, we give decomposition theorems for perfect binomial $\sigma$-ideals. We first consider normal binomial $\sigma$-ideals. By Corollary 6.20 and Example 5.22 a normal binomial $\sigma$-ideal is radical but may not be perfect.

Theorem 6.25 Let $\mathcal{I} = \mathcal{I}^+(\rho)$ be a normal binomial $\sigma$-ideal and $\mathcal{F}$ an inversive and algebraically closed $\sigma$-field. Then $\{\mathcal{I}\} : m$ is either $[1]$ or can be written as the intersection of reflexive prime binomial $\sigma$-ideals whose support lattice is the saturation lattice of $L_\rho$.

30
Proof: By Theorem 5.7, 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 \( \sigma \)-ideals whose support lattices are \( \text{sat}(L_\rho) \). By (33) and Lemma 6.16 either \( \{\mathcal{I}^+(\rho)\} : m = [1] \) or \( \{\mathcal{I}^+(\rho)\} : m = \{\mathcal{I}(\rho)\} \cap \mathcal{F}\{\mathcal{Y}\} = \bigcap_{i=1}^{s} \mathcal{I}(\rho_i) \cap \mathcal{F}\{\mathcal{Y}\} = \bigcap_{i=1}^{s} \mathcal{I}^+(\rho_i) \). By Corollary 6.22 \( \mathcal{I}^+(\rho_i) \) is reflexive and prime whose support lattices are the saturation of \( L_\rho \).

Now, consider general binomial \( \sigma \)-ideals.

**Lemma 6.26** \( \mathcal{I} \subset \mathcal{F}\{\mathcal{Y}\} \) is a reflexive prime binomial \( \sigma \)-ideal if and only if \( \mathcal{I} = \{y_1, \ldots, y_s\} + \mathcal{I}_1 \), where \( \{y_1, \ldots, y_s\} = \mathcal{Y} \cap \mathcal{I}, \{z_1, \ldots, z_t\} = \mathcal{Y} \setminus \mathcal{I}, \) and \( \mathcal{I}_1 \) is a normal binomial reflexive prime \( \sigma \)-ideal in \( \mathcal{F}\{z_1, \ldots, z_t\} \).

Proof: If \( \mathcal{I} \) is reflexive and prime, then \( (y_i^{t_1})^d \in \mathcal{I} \) if and only if \( y_i \in \mathcal{I} \). Let \( \mathcal{I}_1 = \mathcal{I} \cap \mathcal{F}\{z_1, \ldots, z_t\} \). Then \( \mathcal{I} = \{y_1, \ldots, y_s\} + \mathcal{I}_1 \). \( \mathcal{I}_1 \) is clearly reflexive and prime. We still need to show that \( \mathcal{I}_1 \) is normal. Let \( Nf \in \mathcal{I} \) for a \( \sigma \)-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 \( \{z_1, \ldots, z_t\} = \mathcal{Y} \setminus \mathcal{I} \). Therefore, \( f \in \mathcal{I}_1 \) and \( \mathcal{I}_1 \) is normal. The other direction is trivial.

The \( \sigma \)-ideal \( \mathcal{I} \) in Lemma 6.26 is said to be quasi-normal. The following result can be proved similarly to Theorem 5.7.

**Theorem 6.27** Let \( \mathcal{I} \) be a binomial \( \sigma \)-ideal. If \( \mathcal{F} \) is algebraically closed and inversive, then the perfect \( \sigma \)-ideal \( \{\mathcal{I}\} \) is either \([1]\) or the intersection of quasi-normal reflexive prime binomial \( \sigma \)-ideals.

Proof: We prove the theorem by induction on \( n \). Let \( \mathcal{I}_1 = \{\mathcal{I}\} : m \). Then \( \{\mathcal{I}\} = \mathcal{I}_1 \cap \bigcap_{i=1}^{n}\mathcal{I}, y_i \). It is easy to check \( \mathcal{I}_1 = \{\mathcal{I} : m\} : m \). Since \( \mathcal{I} : m \) is normal, by Theorem 6.25, \( \mathcal{I}_1 \) is either \([1]\) or intersection of normal reflexive prime \( \sigma \)-ideals. If \( n = 1 \), then \( \{\mathcal{I}, y_i\} \) must be either \([y_i]\) or \([1]\). Then the theorem is proved for \( n = 1 \). Suppose the theorem is valid for \( n = 1, \ldots, k - 1 \). Still use \( \{\mathcal{I}\} = \mathcal{I}_1 \cap \bigcap_{i=1}^{n}\mathcal{I}, y_i \). Let \( \mathcal{I}_i \) be the \( \sigma \)-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 \( \sigma \)-ideals in \( \mathcal{F}\{\mathcal{Y} \setminus \{y_i\}\} \). 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 \( \sigma \)-ideal

The theory of characteristic set given in Section 4.2 will be extended to the normal \( \sigma \)-binomial case.

Let \( \rho \) be a partial character over \( \mathbb{Z}[x]^n \), \( L_\rho = (f_1, \ldots, f_s) \) where \( \mathfrak{f} = \{f_1, \ldots, f_s\} \) is a reduced Gröbner basis, and

\[
A^+(\rho) : \mathcal{Y}f_1^+ - \rho(f_1)\mathcal{Y}f_1^+, \ldots, \mathcal{Y}f_s^+ - \rho(f_s)\mathcal{Y}f_s^+. \tag{34}
\]

We have the following canonical representation for normal binomial \( \sigma \)-ideals.

31
Theorem 6.28 Use the notations in \([37]\). Then \(I^+(\rho) = \text{sat}(A^+(\rho))\). Furthermore, \(A^+(\rho)\) is a regular and coherent \(\sigma\)-chain and hence is a characteristic set of \(I^+(\rho)\).

Proof: Let \(I_1 = [A^+(\rho)]: m\). We claim \(I_1 = \text{sat}(A^+(\rho))\). It is clear that \(\text{sat}(A^+(\rho)) \subset [A^+(\rho)]: m = I_1\). For the other direction, let \(p \in I_1\) and \(p_1 = \text{pre}(p, A^+(\rho))\) which is reduced w.r.t. \(A^+(\rho)\). By \([3] , p_1 \in I_1\). As a consequence, \(p_1 \in [A(\rho)]\) as Laurent \(\sigma\)-polynomials in \(F\{\overline{\rho}\}\). By Lemma 4.16 \(A(\rho)\) is a characteristic set of \([A(\rho)]\). Since \(p_1\) is reduced w.r.t. \(A^+(\rho)\), it is also reduced w.r.t. \(A(\rho)\). Then \(p_1 = 0\) and hence the claim is proved.

We now prove \(I^+(\rho) = \text{sat}(A^+(\rho))\). By the above claim, Lemma 4.16 and Lemma 6.16, \(\text{sat}(A^+(\rho)) = [A^+(\rho)]: m = [A^+(\rho)]F\{\overline{\rho}\} \cap F\{\overline{\rho}\} = [A(\rho)] \cap F\{\overline{\rho}\} = I(\rho) \cap F\{\overline{\rho}\} = I^+(\rho)\).

It remains to prove that \(A^+(\rho)\) is a characteristic set of \(I_1 = [A^+(\rho)]: m\). By definition, it suffices to show that if \(p \in I_1\) is reduced w.r.t. \(A^+(\rho)\) then \(p = 0\). Let \(A_i = \overline{\rho}_{f_i} - \rho(f_i)\) and \(A_i^+ = \overline{\rho}_{f_i} - \rho(f_i)\overline{\rho}^\infty\). Since \(p \in I_1\), there exist a \(\sigma\)-monomial \(M\) and \(f_{i,j} \in F\{\overline{\rho}\}\) such that \(M_p = \sum_{i,j} f_{i,j} (A_i^+)\). Then in \(F\{\overline{\rho}\}\), we have \(p = \sum_{i,j} g_{i,j} A_i^+ \in [A(\rho)]\), where \(g_{i,j} \in F\{\overline{\rho}\}\). Since \(p\) is reduced w.r.t. \(A^+(\rho)\), it is also reduced w.r.t. \(A(\rho)\). By Lemma 4.16 \(A(\rho)\) is a characteristic set of \([A(\rho)]\) and hence \(p = 0\). The claim is proved.

Since \(I_1 = \text{sat}(A^+(\rho))\), \(A^+(\rho)\) is also a characteristic set of \(\text{sat}(A^+(\rho))\). By Theorem 2.1 \(A^+(\rho)\) is regular and coherent. \(\square\)

Example 6.29 Let \(L = ([1 - x, x - 1])\) be a \(\mathbb{Z}[x]\)-module and \(\rho\) the trivial partial character on \(L\), that is, \(\rho(f) = 1\) for \(f \in L\). By Theorem 6.28 \(I^+(\rho) = \text{sat}(y_1 y_2 - y_1^2 y_2^2) \subset Q\{y_1, y_2\}\). By Theorem 6.16 \(I^+(\rho)\) is a reflexive prime \(\sigma\)-ideal. We can show that \(I^+(\rho) = [y_1^2 y_2^2 - y_1^2 y_2^2 | 0 \leq i < j \leq m]\), which is an infinitely generated \(\sigma\)-ideal.

As a consequence of Theorem 6.19 Theorem 6.28 and Lemma 4.16 we have

Corollary 6.30 Let \(A(\rho)\) and \(A^+(\rho)\) be defined in \([37]\) and \([37]\), respectively. Then \(([A(\rho)]F\{\overline{\rho}\}) \cap F\{\overline{\rho}\} = \text{sat}(A^+(\rho))\).

As a consequence of Theorem 5.3 Corollary 6.22 and Theorem 6.28

Corollary 6.31 \([A(\rho)]\) is a reflexive (prime) \(\sigma\)-ideal in \(F\{\overline{\rho}\}\) if and only if \(\text{sat}(A^+(\rho))\) is a reflexive (prime) \(\sigma\)-ideal in \(F\{\overline{\rho}\}\).

We now prove the converse of Theorem 6.28. Let \(f_i \in \mathbb{Z}[x]^n\) and \(c_i \in F^*, i = 1, \ldots, s\). Consider the following \(\sigma\)-chains

\[
\mathcal{A} : \overline{\rho}_{f_1} - c_1, \ldots, \overline{\rho}_{f_s} - c_s
\]

\[
A^+ : \overline{\rho}_{f_1}^+ - c_1 \overline{\rho}_{f_1}^+, \ldots, \overline{\rho}_{f_s}^+ - c_s \overline{\rho}_{f_s}^+
\]

in \(F\{\overline{\rho}\}\) and \(F\{\overline{\rho}\}\), respectively. Notice that, when talking about \(A^+\) (or \(A\)), all operations are performed in \(F\{\overline{\rho}\}\) (or \(F\{\overline{\rho}\}\)). Since \(f_i\) are assumed to be normal, \(A^+\) is a \(\sigma\)-chain if and only if \(A\) is a Laurent \(\sigma\)-chain.
Lemma 6.32 Use the notations in (33). Let \( p = a Y^a + b Y^b = a N(Y^r - c) \in F\{Y\} \), where \( a, b \in \mathbb{N}[x]^n \), \( f \in \mathbb{Z}[x]^n \), \( N \) is a \( \sigma \)-monomial, \( c \in F^* \). If \( A^+ \) is coherent and regular, then \( \text{prem}(p, A^+) = 0 \) implies \( \text{prem}(Y^r - c, A) = 0 \).

Proof: Since \( \text{prem}(p, A^+) = 0 \), there exists a \( \sigma \)-monomial \( M_1 \) such that \( M_1 p \in [A^+] \). Let \( p_1 = Y^r - c \). Since \( r = \text{prem}(p_1, A) = Y^g - c_g \), by Lemma 5.5 there exists a \( c_i \in F^* \) such that \( r_1 = c_1 p_1 \in [A] \). Then, there exists a \( \sigma \)-monomial \( M_2 \) such that \( M_2 r_1, M_2 N p_1 \in F\{Y\} \) and \( M_2 N (r_1 - c_1 p_1) \in [A^+] \) and hence \( M_2 M_1 N (r_1 - c_1 p_1) = M_2 M_1 N r_1 - \frac{M_2}{M_2} M_2 M_1 p \in [A^+] \). Let \( M = M_1 M_2 N \). From \( M_1 p \in [A^+] \), we have \( M r_1 \in [A^+] \subset \text{sat}(A^+) \).

Suppose \( A_i = Y^r_i - c Y^r_i = I^+_i y_{c_i}^{d_i s_i} - c I^-_i \), where \( y_{c_i} \) is the leading variable of \( A_i \). A variable like \( y_{c_i}^{s_i} \) for \( k \in \mathbb{N} \) is called a main variable of \( A_i \). A variable \( y_{c_i}^k \) is called a parameter of \( A^+ \) if it is not a main variable. If \( M \) contains a main variable of \( A^+ \) as a factor. Then let \( z = y_{c_i}^{s_i} \) be the largest one appearing in \( M \) under the variable ordering induced by the lexicographical order 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 \( s_1 = \frac{s}{d_i} \), \( s_0 = s - s_1 d_i \), and \( M = M z_i^{d_i s_0} - s_0 = M z_i^{d_i (s_1 + 1)} \). We still have \( M r_1 \in \text{sat}(A^+) \). We may use \( A_i = 0 \) to eliminate \( z \) from \( M \) as follows: \( M_1 z_i^{s_0} - I_i^-(z_i) z_i^{d_i} r_1 = M_1 z_i^{s_0} - I_i^-(z_i) z_i^{d_i} r_1 = M I_i^+(z_i) z_i^{d_i} r_1 = M_1 z_i^{s_0} - I_i^-(z_i) z_i^{d_i} r_1 \in \text{sat}(A^+) \). Note that \( \deg(M_1 z_i^{s_0} - I_i^-(z_i) z_i^{d_i} r_1, z) = s - d_i \). Repeat the above procedure, we may find a \( \sigma \)-monomial \( N \) such that \( N r_1 \in \text{sat}(A^+) \), \( N \) does not contain \( z \) as a factor, and any variable \( y_{c_i}^k \) in \( M \) is smaller than \( z \) in the given variable ordering. Repeat the procedure, we may finally obtain a \( \sigma \)-monomial \( L \) such that \( L \) does not contain main variables of \( A^+ \) as factors and \( L r_1 \in \text{sat}(A^+) \). Since \( L \) contains only parameters of \( A^+ \) and \( r_1 \) is reduced w.r.t. \( A^+ \), \( L r_1 \) is also reduced w.r.t. \( A^+ \). Since \( A^+ \) is regular and coherent, by Lemma 3.4 it is the characteristic set of \( \text{sat}(A^+) \). Therefore, \( L r_1 = 0 \), and \( r_1 = 0 \).

The following example shows that if \( \text{prem}(p, A^+) \neq 0 \) then the relation between \( \text{prem}(p, A^+) \) and \( \text{prem}(Y^r - c, A) \) may be complicated, where \( p = a Y^a + b Y^b = a N(Y^r - c) \).

Example 6.33 Let \( p = y_2(y_2 - 1) \), \( A_1 = y_1^{-1} y_2 - 1 \), and \( A_1^+ = y_2^2 - y_1 \). Then \( \text{prem}(p, A_1^+) = y_1 - y_2 \) in \( F\{y_2\} \). But in \( F\{y_2^2\} \), \( p \) is represented as \( \tilde{p} = y_2 - 1 \) and \( \text{prem}(\tilde{p}, A_1) = y_2 - 1 \).

Lemma 6.34 Use the notations in (33). \( A \) is a regular and coherent \( \sigma \)-chain in \( F\{Y\} \) if and only if \( A^+ \) is a regular and coherent \( \sigma \)-chain in \( F\{Y\} \).

Proof: If \( A \) is regular and coherent, by Theorem 4.18 and Corollary 4.19 there exists a partial character \( \rho \) over \( \mathbb{Z}[x]^n \) such that \( L_{\rho} = (f_1, \ldots, f_n) \), \( \rho(f_i) = c_i \), and \( L(\rho) = [A] \). By Theorem 6.28 \( A^+ = A^+(\rho) \) is regular and coherent.

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

Note that \( A \) is always regular since \( \sigma \)-monomials are invertible in \( F\{Y\} \). Then, it suffices to prove that \( A \) is coherent.
Lemma 6.38 If \( A_i = Y_i^t - c_i \) and \( A_j^+ = Y_j^t - c_j Y_j^r \). Assume \( A_i^+ \) and \( A_j^+ \) (\( i < j \)) have the same leading variable \( y_t \), and \( A_i^+ = I_i^+ y_i d_j^{x_i^j} - c_i I_i^- \), \( A_j^+ = I_j^+ y_j d_j^{x_j^j} - c_j I_j^- \), where \( I_i^- = Y_i^r \). From Definition 3.6, we have \( \alpha_j < \alpha_i \) and \( d_i | d_j \). Let \( d_i = td_j \) where \( t \in \mathbb{N} \). From (1),

\[
\Delta(A_i^+, A_j^+) = \text{prem}((A_i^+)^{x_j^j - \alpha_i}, A_j^+) = c_j^d (I_j^-)^t (I_i^x)^{x_j^j - \alpha_i} - (I_j^+)^t (c_j I_j^+) x_j^j - \alpha_i.
\]

Comparing to (18), if \( \Delta(A_i, A_j) = Y_h^j - c_f \), then \( \Delta(A_i^+, A_j^+) = c_j^d M(Y_h^j - c_f Y_h^j) \), where \( M \) is a \( \sigma \)-monomial. Since \( A^+ \) is coherent, \( \text{prem}(\Delta(A_i^+, A_j^+), A^+) = 0 \). By Lemma 6.32, \( \text{prem}(\Delta(A_i, A_j), A) = 0 \) which implies that \( A \) is coherent.

We now prove the converse of Theorem 6.28.

**Theorem 6.35** Use the notations in (75). If \( A^+ \) is a regular and coherent \( \sigma \)-chain, then there is a partial character \( \rho \) over \( \mathbb{Z}[x]^n \) such that \( L_\rho = (f_1, \ldots, f_i) \), \( \rho(f_i) = c_i \), \( I_\rho = [A] \), and \( I^+(\rho) = \text{sat}(A^+) \).

**Proof:** By Lemma 6.33, \( A \) is regular and coherent. By Theorem 4.14, \( f \) is a reduced Gröbner basis for a \( \mathbb{Z}[x] \)-lattice and \( [A] \subset \mathcal{F}\{Y^+\} \) is proper. By Theorem 4.18 and Corollary 4.19, there exists a partial character \( \rho \) such that \( L_\rho = (f_1, \ldots, f_i) \), \( \rho(f_i) = c_i \), and \( I_\rho = [A] \). By Theorem 6.28, \( I^+(\rho) = \text{sat}(A^+) = \text{sat}(A^+) \).

As a consequence of Theorem 6.35 and Lemma 6.16, we have the following canonical representation for a normal binomial \( \sigma \)-ideal.

**Corollary 6.36** \( I \) is a normal binomial \( \sigma \)-ideal if and only if \( I = \text{sat}(A^+) \), where \( A^+ \) is a regular and coherent chain given in (75).

### 6.4 Perfect closure of binomial \( \sigma \)-ideal and binomial \( \sigma \)-variety

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

**Theorem 6.37** Let \( F \) be an algebraically closed and inversive \( \sigma \)-field. Then the perfect closure of a binomial \( \sigma \)-ideal \( I \) is binomial.

We first remark that it is not known whether the well-mixed closure of a binomial \( \sigma \)-ideal is still binomial. Before proving Theorem 6.37, we first prove several lemmas. In the rest of this section, we assume that \( I \subseteq S = F\{Y\} \) and \( m \) the set of \( \sigma \)-monomials in \( S \).

**Lemma 6.38** If \( I \) is a binomial \( \sigma \)-ideal, then \( \{I\} : m \) is either \([1] \) or a binomial \( \sigma \)-ideal.

**Proof:** It is easy to check \( \{I\} F\{Y^\pm\} = \{I F\{Y^\pm\}\} \). By (30), \( \{I\} : m = \{I\} F\{Y^\pm\} \cap F\{Y\} = \{I F\{Y^\pm\}\} \cap F\{Y\} \). Now the lemma follows from Theorem 5.28. \( \square \)
Lemma 6.39 If $\mathcal{I}$ is a $\sigma$-ideal in $\mathbb{F}\{\mathbb{Y}\}$, then
\[
\{\mathcal{I}\} = \{\mathcal{I} : m \cap \{\mathcal{I} + y_1\} \cap \cdots \cap \{\mathcal{I} + y_n\}\}
\] (36)

Proof: The right-hand side of (36) clearly contains $\{\mathcal{I}\}$. It suffices to show that every reflexive prime $P$ containing $\mathcal{I}$ contains one of the $\sigma$-ideals on the right-hand side of (36). If $\{\mathcal{I}\} : m \subseteq P$, we are done. Otherwise, there exists an element $f \in (\{\mathcal{I}\} : m) \setminus P$ which implies that there exists a $\sigma$-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. \hfill $\square$

Lemma 6.40 Let $\mathcal{I}$ be a binomial $\sigma$-ideal in $S = \mathbb{F}\{\mathbb{Y}\}$ and $S' = \mathbb{F}\{y_1, \ldots, y_{n-1}\}$. If $\mathcal{I} = \mathcal{I} \cap S'$, then $[\mathcal{I} + y_n]$ is the sum of $[\mathcal{I}'S + y_n]$ and a monomial $\sigma$-ideal in $S'$.

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

Lemma 6.41 Let $\mathcal{I}$ be a perfect binomial $\sigma$-ideal in $S = \mathbb{F}\{\mathbb{Y}\}$. If $\mathcal{M}$ is a $\sigma$-monomial $\sigma$-ideal, then $[\mathcal{I} + \mathcal{M}] = [\mathcal{I} + \mathcal{M}_1]$ for some monomial $\sigma$-ideal $\mathcal{M}_1$.

Proof: If $1 \in \mathcal{M}$, then the lemma is obviously valid. Otherwise, $[\mathcal{I} + \mathcal{M}] : m = [1]$. Lemma 6.39 yields $[\mathcal{I} + \mathcal{M}] = \bigcap_{i=1}^{n} [\mathcal{I} + \mathcal{M} + y_i]$. By Corollary 6.9 we need only to show that $[\mathcal{I} + \mathcal{M} + y_i]$ is the sum of $\mathcal{I}$ and a monomial $\sigma$-ideal. For simplicity, let $i = n$ and write $S' = \mathbb{F}\{y_1, y_2, \ldots, y_{n-1}\}$. Since $\mathcal{I}$ is perfect, the $\sigma$-ideal $\mathcal{I}' = \mathcal{I} \cap S'$ is perfect as well. By Lemma 6.40 $[\mathcal{I} + \mathcal{M} + y_n] = [\mathcal{I}'S + \mathcal{M}'S + y_n]$ where $\mathcal{M}'$ is a monomial $\sigma$-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 $\sigma$-ideal of $S'$. Putting this together, we have
\[
[\mathcal{I} + \mathcal{M} + y_n] = [\mathcal{I}'S + \mathcal{M}'S + y_n] = [\mathcal{I}'S + \mathcal{M}'_1S + y_n]
\] \[
\subseteq [\mathcal{I} + \mathcal{M}'_1S + y_n] \subseteq [\mathcal{I} + \mathcal{M} + y_n].
\]

So $[\mathcal{I} + \mathcal{M} + y_n] = [\mathcal{I} + \mathcal{M}'_1S + y_n]$ is $\mathcal{I}$ plus a monomial $\sigma$-ideal, as required. \hfill $\square$

Proof of Theorem 6.37 We will prove the theorem by induction on $n$. By Lemma 6.38, $\mathcal{I}_1 = \{\mathcal{I}\} : m$ is binomial. For $n = 1$, by Lemma 6.39 $\{\mathcal{I}\} = \mathcal{I}_1 \cap \{\mathcal{I} + y_1\}$. If $[\mathcal{I} + y_1] = 1$ then $[\mathcal{I}] = \mathcal{I}_1$ is binomial. Otherwise $[\mathcal{I} + y] = [y]$ and hence $\mathcal{I} \subseteq [y]$. Since $\mathcal{I} \subseteq \mathcal{I}_1$, $[\mathcal{I}] = \mathcal{I}_1 \cap [y] = [\mathcal{I} + \mathcal{I}_1] \cap [\mathcal{I} + y]$ is binomial by Lemma 6.8. Suppose the lemma is valid for $n - 1$ variables and let $\mathcal{I}$ be a binomial $\sigma$-ideal in $S = \mathbb{F}\{\mathbb{Y}\}$. 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 perfect in binomial. Adding these binomial $\sigma$-ideals to $\mathcal{I}$, we may assume that each $\mathcal{I}_j$ is perfect begin with. By Lemma 6.38 $\mathcal{I}_1 = \{\mathcal{I}\} : m$ is binomial. Then there exists a binomial $\sigma$-ideal $\mathcal{I}'$, say $\mathcal{I}' = \mathcal{I}_1$, such that $[\mathcal{I} + \mathcal{I}'] = [\mathcal{I} + \mathcal{I}']$. By Lemma 6.40 $[\mathcal{I} + y_j] = [\mathcal{I}_jS + \mathcal{J}_jS + y_j]$, where $\mathcal{J}_j$ is a monomial $\sigma$-ideal in $S_j$. Since $\mathcal{I}_j$ is perfect, the $\sigma$-ideal $\mathcal{J}_jS$ is perfect, so we can apply Lemma 6.41 with $\mathcal{M} = [\mathcal{J}_jS + y_j]$ to see that there exists a monomial $\sigma$-ideal $\mathcal{M}_j$ in $S$ such that $[\mathcal{I} + y_j] = [\mathcal{I}_jS + \mathcal{J}_jS + y_j] = [\mathcal{I}_jS + \mathcal{M}_j] = [\mathcal{I} + \mathcal{M}_j]$. By Lemma 6.39 and Corollary 6.8 $\{\mathcal{I}\} = [\mathcal{I} + \mathcal{I}'] \cap \mathcal{T}_j=1^{n}[\mathcal{I} + \mathcal{M}_j]$ is binomial. \hfill $\square$
Example 6.42 Let $p = y_2^2 - y_1^2$. Following the proof of Theorem 6.37, $\{p\} = (\{p\} : \mathfrak{m}) \cap [y_1, y_2]$. By Example 5.25 and Corollary 6.3 (I)_1 = \{p\} : \mathfrak{m} = \text{sat} \{y_2^2 - y_1^2, y_1 y_2 - y_1 y_2\} = [y_1 y_2^2 - y_1^3 y_2, y_2 x^j - y_1^{1+x^j} | 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 $\sigma$-ideal, which is a generalization of Theorem 4.1 in [7] to the difference case. The basic idea of the proof also follows [7], except we need to consider the distinction between the perfect $\sigma$-ideals and radical ideals.

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

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

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

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

The $\sigma$-coordinate ring of $(\mathbb{A}^n)^\Omega$ is the Laurent polynomial $\sigma$-ring $\mathcal{F}\{\Omega^\pm\} := \mathcal{F}\{y_i, y_i^{-1}, i \in \Omega\}$.

We can define a coordinate projection $(\mathbb{A}^n)^{\Omega'} \rightarrow (\mathbb{A}^n)^\Omega$ whenever $\Omega \subseteq \Omega' \subseteq \{1, 2, \ldots, n\}$ by setting all those coordinates not in $\Omega$ to zero.

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

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

where $\mathfrak{m}_\Omega = \{\prod_{i \in \Omega} y_i^{m_i(x)} | m_i(x) \in \mathbb{N}[x]\}$. Since $\mathcal{I}$ is perfect, by the difference Nullstellsatz [4] p.87

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

If $\mathcal{I}$ is binomial, then by Corollary 6.10 the $\sigma$-ideal $\mathcal{I}_\Omega$ is also binomial.

Lemma 6.43 Let $R := \mathcal{F}\{z_1, z_1^{-1}, \ldots, z_t, z_t^{-1}\} \subset R' := \mathcal{F}\{z_1, z_1^{-1}, \ldots, z_t, z_t^{-1}, y_1, \ldots, y_k\}$ be a Laurent polynomial $\sigma$-ring and a polynomial $\sigma$-ring over it. If $B \subset R'$ is a binomial $\sigma$-ideal and $M \subset R'$ is a monomial $\sigma$-ideal such that $[B + M]$ is a proper $\sigma$-ideal in $R'$, then $[B + M] \cap R = B \cap R$.

Proof: This is a $\sigma$-version of [7] Lemma 4.2], which can be proved similarly. ∎

We can make a classification of all binomial $\sigma$-varieties $X$ by intersecting $X$ with $(\mathbb{A}^n)^\Omega$, since by Theorem 6.37 the perfect closure of a binomial $\sigma$-ideal is still binomial.

Theorem 6.44 Let $\mathcal{F}$ be any algebraically closed and inversive $\sigma$-field. A $\sigma$-variety $X \subset \mathbb{A}^n$ is generated by $\sigma$-binomials if and only if the following three conditions hold.

1. For each $(\mathbb{A}^n)^\Omega$, the $\sigma$-variety $X \cap (\mathbb{A}^n)^\Omega$ is generated by $\sigma$-binomials.

2. The family of sets $U = \{\Omega \subseteq \{1, 2, \ldots, n\} | X \cap (\mathbb{A}^n)^\Omega \neq \emptyset\}$ is closed under taking intersections.

36
(3) If $\Omega_1, \Omega_2 \in U$ and $\Omega_1 \subset \Omega_2$, then the coordinate projection $(\mathbb{A}^*)^\Omega_2 \to (\mathbb{A}^*)^\Omega_1$ 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 6.45** Let $F$ be any algebraically closed and inversive $\sigma$-field. A perfect $\sigma$-ideal $I \subseteq F\{Y\}$ is binomial if and only if the following three conditions hold.

(1) For each $\Omega \subseteq \{1, \ldots, n\}$, $I_\Omega$ is binomial.

(2) $U = \{\Omega \subseteq \{1, 2, \ldots, n\} \mid \{I_\Omega\} \neq [1]\}$ is closed under taking intersections.

(3) If $\Omega_1, \Omega_2 \in U$ and $\Omega_1 \subset \Omega_2$, then $I_{\Omega_1} \cap F\{\Omega_1\} \subset I_{\Omega_2}$, where $F\{\Omega_1\} = F\{y_i \mid y_i \in \Omega_1\}$.

**Proof:** Suppose $I$ is a perfect $\sigma$-ideal in $F\{Y\}$. Since $I$ is binomial, by Lemma 6.10 $I_\Omega$ is also binomial and (1) is proved. To prove (2) by contradiction, assume that for $\Omega_1, \Omega_2 \in U$, $\{I_{\Omega_2}\} \neq [1], \{I_{\Omega_1} \cap \Omega_2\} = [1]$. We consider two cases. If $I_{\Omega_1} \cap \Omega_2 = [1]$, then for some $m(x) \in \mathbb{N}[x]$ we have $(\prod_{i \in \Omega_1 \cap \Omega_2} y_i)^{m(x)} \in [I + M(\Omega_1) + M(\Omega_2)]$. By Corollary 6.9 $(\prod_{i \in \Omega_1 \cap \Omega_2} y_i)^{m(x)}$ is either in $[I + M(\Omega_1)]$ or $[I + M(\Omega_2)]$, so $I_{\Omega_1}$ or $I_{\Omega_2}$ is [1]. For the second case, we have $I_{\Omega_2} \cap \Omega_2 \neq [1]$ and $\{I_{\Omega_1} \cap \Omega_2\} = [1]$. Then there exist a finite number of proper $\sigma$-binomials $B_1, \ldots, B_s$ and $\sigma$-monomials $m_1, \ldots, m_s$ in $F\{\Omega_1 \cap \Omega_2\}$ such that $m+B_i \in I$ 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 $m+B_i \in I \cap F\{\Omega_1 \cap \Omega_2\}$, we have $Bi \in I_{\Omega_1}$ and $B_i \in I_{\Omega_2}$ and thus $\{I_{\Omega_1}\} = [1]$. To prove (3), given $\Omega_1, \Omega_2 \in U$ and $\Omega_1 \subset \Omega_2$, we have $I_{\Omega_2} = [I_{\Omega_1} : m_{\Omega_1}]$. Set $R' = F\{\Omega_1^\perp\}\{y_i \mid y_i \in \Omega_1\}$, then

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

Since $\Omega_1 \in U$, the $\sigma$-ideal $[I + M(\Omega_1)]R'$ is proper. By Lemma 6.43 we have $[I + M(\Omega_1)]R' \cap F\{\Omega_1^\perp\} \subseteq I_{\Omega_2} R' \cap F\{\Omega_1^\perp\}$. So $I_{\Omega_1} \cap F\{\Omega_1^\perp\} \subseteq I_{\Omega_2}$.

To prove the other direction, let $I$ be a perfect $\sigma$-ideal satisfying the three conditions. By the difference Nullstellensatz, $I = \cap_{\Omega \in U}\{I_\Omega\}$. 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 $J(\Omega) = [I_\Omega \cap F\{\Omega\}]F\{Y\}$ with the properties that if $\Omega_1 \subset \Omega_2$, $\{J(\Omega_1)\} \subset \{J(\Omega_2)\}$. Note that $[M_{\Omega_1 \cap \Omega_2}] \subset [M_{\Omega_1} + M_{\Omega_2}]$. Then we have

$$I = \cap_{\Omega \in U}\{I_\Omega\} = \cap_{\Omega \in U}\{J(\Omega) + M(\Omega)\}.$$
\( \cap_{\Omega \in U} M(\Omega) \) and \( \{ M_{\Omega_1 \cap \Omega_2} \} \subset \{ M_{\Omega_1} + M_{\Omega_2} \} \). Let \( \Omega_0 \) be the smallest element of \( V \) such that \( P \supseteq M_{\Omega_0} \). At the same time, \( P \supseteq J(\Omega_0) \cap \cap_{\Omega \not\in \Omega_0} M(\Omega_\eta) \), then \( P \supseteq J(\Omega_0) \). Therefore, \( P \supseteq J(\Omega_0) + M(\Omega_0) \) and \( P \) contains the left hand side of (37) and (37) is proved. Since \( \cap_{\Omega \in U} M(\Omega) + \sum_{\Omega \in U} \{ J(\Omega) \cap \cap_{\Omega_\eta \not\in \Omega} M(\Omega_\eta) \} \) is binomial, the theorem follows from (37).

7 Algorithms

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

- **Algorithm GHNF.** Let \( \mathcal{F} \) be a finite set of \( \mathbb{Z}[x]^n \). The algorithm computes the generalized Hermite normal form of \( \mathcal{F} \), or equivalently, the reduced Gröbner basis of the \( \mathbb{Z}[x] \)-module \( (\mathcal{F}) \) [5, p. 197]. A polynomial-time algorithm is given in [15].

- **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 3.9.

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 \( M \) [3, p.68].

- **Algorithm KER.** For a matrix \( M \in \mathbb{D}^{n \times s} \), compute a basis for the \( \mathbb{D} \)-module: \( \ker_{\mathbb{D}}(M) = \{ X \in \mathbb{D}^s \mid MX = 0 \} \) [3, 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 \( f_1, \ldots, f_s \in \mathbb{Z}[x]^n \) and \( L = (f_1, \ldots, f_s) \). If \( L \) is not \( x \)-saturated, then there exist \( g_i \in \mathbb{Z}[x] \) such that \( \sum_{i=1}^s g_i f_i = x \mathbf{h} \) and \( \mathbf{h} \not\in L \). Setting \( g_i(x) = g_i(0) + x \tilde{g}_i(x) \) and \( \tilde{\mathbf{h}} = \mathbf{h} - \sum_{i=1}^s \tilde{g}_i(x) f_i \), we have

\[
\sum_{i=1}^s g_i(0)f_i = x\tilde{\mathbf{h}}
\]

where \( \tilde{\mathbf{h}} \not\in L \). Setting \( x = 0 \) in the above equation, we have

\[
\sum_{i=1}^s g_i(0)f_i(0) = 0,
\]
that is, \( G = (g_1(0), \ldots, g_s(0))^\tau \) is in the kernel of the matrix \( F = [f_1(0), \ldots, f_s(0)] \in \mathbb{Z}^{n \times s} \), which can be computed efficiently [3, page 74]. From \( G \) and (38), we may compute \( \tilde{h} \). This observation leads to the following algorithm.

Algorithm 1 — XFactor(\([f_1, \ldots, f_s]\))

**Input:** A generalized Hermite normal form \([f_1, \ldots, f_s] \subset \mathbb{Z}[x]^{n \times s}\).

**Output:** \( \emptyset \), if the \( \mathbb{Z}[x] \)-lattice \( L = (f_1, \ldots, f_s) \) is \( x \)-saturated; otherwise, a finite set \( \{ (h_i, e_i) \mid i = 1, \ldots, r \} \) such that \( e_i = (e_{i1}, \ldots, e_{is})^\tau \in \mathbb{Z}^s \), \( h_i \not\in L \), and \( x h_i = \sum_{l=1}^s e_{il} f_l \in L \), \( i = 1, \ldots, r \).

1. Set \( F = [f_1(0), \ldots, f_s(0)] \in \mathbb{Z}^{n \times s} \).
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 \( e = (e_1, \ldots, e_s)^\tau \in E \) and \( E = E \setminus \{ e \} \).
   4.2. Let \( h = (e_1 f_1 + \cdots + e_s f_s)/x \).
   4.3. If \( \text{grem}(h, \{ f_1, \ldots, f_s \}) \neq 0 \), then add \( (h, e) \) to \( H \).
5. Return \( H \).

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

Algorithm 2 — SatX(\(f_1, \ldots, f_s\))

**Input:** A finite set \( \mathcal{f} = \{ f_1, \ldots, f_s \} \subset \mathbb{Z}[x]^n \).

**Output:** A set of generators of \( \text{sat}_x(f_1, \ldots, f_s) \).

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

Note. \( \text{Col}(g) \) is the set of columns of \( g \).

Example 7.1 Let \( C \) be the following generalized Hermite normal form.

\[
C = [f_1, f_2, f_3] = \begin{bmatrix}
-x + 2 & 1 & 1 \\
3x + 2 & 1 & 2x + 1 \\
0 & 2x & x^2
\end{bmatrix}.
\]

In XFactor(\(C\)), the kernel of the following matrix \([f_1(0), f_2(0), f_3(0)] = \begin{bmatrix}
2 & 1 & 1 \\
2 & 1 & 1 \\
0 & 0 & 0
\end{bmatrix} \) is generated by \( e_1 = (0, -1, 1)^\tau \) and \( e_2 = (1, -2, 0)^\tau \). In step 4.2 of XFactor, we have \( h = (-f_2 + f_3)/x = (0, 2, x - 2)^\tau \). One can check that \( (0, 2, x - 2)^\tau \not\in \langle C \rangle \). In SatX,
computing the generalized Hermite normal form of $C \cup \{(0,2,x-2)^T\}$, we have

$$C_1 = \begin{bmatrix} -x+2 & 1 & 0 \\ 3x+2 & -3 & 2 \\ 0 & 4 & x-2 \end{bmatrix}.$$ 

\textbf{XFactor($C_1$) returns $\emptyset$. So, ($C_1$) is the $x$-saturation of ($C$).}

\textbf{Proposition 7.2} Algorithms \textbf{SatX} and \textbf{XFactor} are correct.

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

We first explain step 4.2 of Algorithm \textbf{XFactor}. Since $e \in \ker_\mathbb{Z}(F)$, $h(0) = [f_1(0), \ldots, f_s(0)]e = [0, \ldots, 0]^T$. Therefore, $x$ is a factor of $e_1f_1 + \cdots + e_sf_s$ and thus $h = (e_1f_1 + \cdots + e_sf_s)/x \in \mathbb{Z}[x]^n$.

To prove the correctness of Algorithm \textbf{XFactor}, it suffices to show that $L = \text{sat}_x(L)$ if and only if for each $e \in E$, $e_1f_1 + \cdots + e_sf_s = x\text{h}$ implies $h \in L$.

Let $E = \{e_1, \ldots, e_k\}$ where $e_i \in \mathbb{Z}^s$. If $L = \text{sat}_x(L)$, then it is clear that $(f_1, \ldots, f_s)e_i = xh_i$ implies $h_i \in L$. To prove the other direction, let $[f_1, \ldots, f_s]e_i = xh_i$ for $1 \leq i \leq k$, where $h_i \in L$. Let $xf \in L$. Then $xf = \sum_{i=1}^s c_i(x)f_i$, where $c_i(x) \in \mathbb{Z}[x]$. If for each $i$, $x|c_i(x)$, then we have $f = \sum_{i=1}^s (c_i(x)/x)f_i \in L$, and the lemma is proved. Otherwise, set $x = 0$ in $xf = \sum_{i=1}^s c_i(0)f_i$, we obtain $\sum_{i=1}^s c_i(0)f_i(0) = 0$. Hence $Q = [c_1(0), \ldots, c_s(0)]^T \in \ker_\mathbb{Z}(F)$ and hence there exist $a_i \in \mathbb{Z}$, $i = 1, \ldots, k$ such that $Q = \sum_{i=1}^k a_i e_i$. Then, $[f_1, \ldots, f_s]Q = \sum_i a_i[f_1, \ldots, f_s]e_i = \sum_{i=1}^k a_i xh_i = x\tilde{h}$, where $h = \sum_{i=1}^k a_i h_i \in L$. Then,

$$xf = \sum_{i=1}^s c_i(x)f_i = \sum_{i=1}^s c_i(0)f_i + \sum_{i=1}^s x\tilde{c_i}(x)f_i$$

$$= [f_1, \ldots, f_s]Q + x \sum_{i=1}^s \tilde{c_i}(x)f_i = xh + x \sum_{i=1}^s \tilde{c_i}(x)f_i,$$

where $\tilde{c_i}(x) = (c_i(x) - c_i(0))/x \in \mathbb{Z}[x]$. Hence, $f = \tilde{h} + \sum_{i=1}^s \tilde{c_i}(x)f_i \in L$ and the lemma is proved. \hfill \Box

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

The key idea to compute $\text{sat}_\mathbb{Z}(L)$ for a $\mathbb{Z}[x]$-lattice $L \in \mathbb{Z}[x]^n$ is as follows. Let $f = \{f_1, \ldots, f_s\}$. Then $(f)$ is not $\mathbb{Z}$-saturated if and only if a linear combination of $f_i$ contains a nontrivial prime factor in $\mathbb{Z}$, that is, $\sum g_i f_i = pf$, where $p$ is a prime number and $f \not\in (f)$. Furthermore, $\sum g_i f_i = pf$ with $g_i \neq 0 \mod p$ is valid if and only if $f_1, \ldots, f_s$ are linear 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 \cite{3}. The following algorithm is based on this observation.
Algorithm 3 — ZFactor

**Input:** A generalized Hermite normal form \( C = [c_1, \ldots, c_s] \subset \mathbb{Z}[x]^n \) of form (6).

**Output:**
- if \( L = \langle C \rangle \) is \( \mathbb{Z} \)-saturated; otherwise, a finite set \( \{(h_i, k_i, e_i) | i = 1, \ldots, r\} \), such that \( h_i \in \mathbb{Z}[x]^n \), \( k_i \in \mathbb{N} \), \( e_i = (e_{i1}, \ldots, e_{ir})^T \in \mathbb{Z}[x]^s \), \( h_i \notin L \) and \( k_i h_i = \sum_{l=1}^s e_{il} c_l \in L \) for \( i = 1, \ldots, r \).

1. Read the numbers \( t, r_1, t_1, c_{r_1,1,0}, i = 1, \ldots, t \) from (6).
2. Set \( q = \prod_{i=1}^t c_{r_1,1,0} \in \mathbb{N} \).
3. For any prime factor \( p \) of \( q \) do
   3.1. Compute a basis \( G \subset \mathbb{Z}_p[x]^s \) of the \( \mathbb{Z}_p[x] \)-module \( \ker_{\mathbb{Z}_p[x]}(F) \) with Algorithm KER.
   3.2. Compute the Hermite normal form \( B = \{b_1, \ldots, b_t\} \) of \( \{c_{r_1,1,1}, \ldots, c_{r_1,t}\} \) in \( \mathbb{Z}_p[x]^n \) with Algorithm HNF.
   3.3. If \( G \neq \emptyset \), for each \( g = [g_1, \ldots, g_t]^T \in G \), let \( \sum_{i=1}^t g_i c_{r_1,i} = ph \) in \( \mathbb{Z}[x]^n \).
      Return the set of \( \{(h_i, p, e_i) \mid \text{where } e_i \text{ is a vector in } \mathbb{Z}[x]^s \text{ such that } (c_1, \ldots, c_s)e_i = f_i + \sum_{k=1}^t a_{i,k} b_k = ph_i \} \).
   3.4. Compute the Hermite normal form \( B = \{b_1, \ldots, b_t\} \)
      of \( \{c_{r_1,1,1}, \ldots, c_{r_1,t}\} \) in \( \mathbb{Z}_p[x]^n \) with Algorithm HNF.
   3.5. Let \( C = \{f_1, \ldots, f_t\} \) be given in (5) and \( \tilde{f}_i = \text{grem}(f_i, B) = f_i + \sum_{k=1}^t a_{i,k} b_k \)
      in \( \mathbb{Z}_p[x]^n \), where \( a_{i,k} \in \mathbb{Z}_p[x] \).
   3.6. If \( f_i = 0 \) for some \( i \), then \( f_i + \sum_{k=1}^t a_{i,k} b_k = ph \) in \( \mathbb{Z}[x]^n \).
      Return the set of \( \{(h_i, p, e_i) \mid \text{where } e_i \text{ is a vector in } \mathbb{Z}[x]^s \text{ such that } (c_1, \ldots, c_s)e_i = f_i + \sum_{k=1}^t a_{i,k} b_k = ph_i \} \).
3.7. Set \( E = [\tilde{f}_1, \ldots, \tilde{f}_t] \in \mathbb{Z}_p[x]^{n \times t} \).
3.8. Compute a basis \( D \) of \( \{X \in \mathbb{Z}_p^t | EX = 0\} \) as a vector space over \( \mathbb{Z}_p \).
3.9. If \( D \neq \emptyset \), for each \( b = [b_1, \ldots, b_t]^T \in D \), \( \sum_{i=1}^t b_i f_i = ph \) in \( \mathbb{Z}[x]^n \).
      Return the set of \( \{(h_i, p, e_i) \mid \text{where } e_i \text{ is a vector in } \mathbb{Z}[x]^s \text{ such that } (c_1, \ldots, c_s)e_i = \sum_{i=1}^t b_i f_i = ph \} \).
4. Return \( \emptyset \).

**Remark 7.3** In steps 3.6 and 3.9, we need to compute \( e_i \) or \( e \). Since \( B = \{b_1, \ldots, b_t\} \) is the Hermite normal form of \( c = [c_{r_1,1,1}, \ldots, c_{r_1,t}] \) in \( \mathbb{Z}_p[x]^n \), there exists an invertible matrix \( M_{t \times t} \) such that \( [b_1, \ldots, b_t] = [c_{r_1,1,1}, \ldots, c_{r_1,t}]M \). In Step 3.6, \( e_i \) can be obtained from the relation \( f_i + \sum_{k=1}^t a_{i,k} b_k = ph_i \) and the relation \( [b_1, \ldots, b_t] = [c_{r_1,1,1}, \ldots, c_{r_1,t}]M \). Step 3.9 can be treated similarly.

**Remark 7.4** In step 3.8, we need to compute a basis for the vector space \( \{X \in \mathbb{Z}_p^t | EX = 0\} \) 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 (6) and \( \deg(c_{r_1,k_1}, x) < \deg(c_{r_1,k_2}, x) \) for \( i = 1, \ldots, t \) and \( k_1 < k_2 \).

The matrix \( E \in \mathbb{Z}_p[x]^{n \times t} \) can be transformed into standard form using the following operations: (1) exchange two columns and (2) add the multiplication of a column by an element from \( \mathbb{Z}_p \) to another column. Equivalently, there exists an invertible matrix \( U \in \mathbb{Z}_p^{t \times t} \).
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 [3, page 74].

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

Algorithm 4 — SatZ\((f_0,\ldots,f_s)\)

**Input:** A set of vectors \( f = \{f_0,\ldots,f_s\} \subset \mathbb{Z}[x]^n \).

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

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

**Example 7.5** Let \( C \) be the following generalized Hermite normal form:

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

Then, \( t = 2, r_1 = 1, l_1 = 1, r_2 = 2, l_2 = 2, q = 4, c_{11} = [x^2 + 2x - 2,0]^\tau, c_{21} = [x + 2,4]^\tau, c_{22} = [1,2x]^\tau \). Apply algorithm \text{ZFactor} to \( C \). 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 \( G = \{-1, x^2\} \). In step 3.3, \( x^2c_{22} - c_{11} = 2(1-x,x^3)^\tau \) and return \( (1-x,x^3)^\tau \).

In Algorithm \text{SatZ}, \( (1-x,x^3)^\tau \) is added into \( C \) 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 \text{ZFactor} to \( \mathcal{C}_1 \). We have \( p = 2 \) and \( t = 2 \). In steps 3.1-3.3, \( G = \emptyset \).

In step 3.4, \( B = \begin{bmatrix} x^2 & 1 - x \\
0 & x^3 \end{bmatrix} \). In step 3.5, \( C_\ast = \begin{bmatrix} x + 2 & 1 & x \\
4 & 2x & 2x^2 \end{bmatrix} \) and \( \overline{f}_i \neq 0 \) for all \( i \).

In step 3.7, \( E = \begin{bmatrix} x & 1 \\
0 & x \end{bmatrix} \). In Step 3.8, \( D = \{b\} \), where \( b = [1,0,-1]^\tau \). In Step 3.9, \( (x + 2,4)^\tau - (x,2x^3)^\tau = 2(1,2-x^2)^\tau \). 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 \text{ZFactor} again, it is shown that \( \mathcal{C}_2 \) is \( \mathbb{Z} \)-saturated.

We will prove the correctness of the algorithm. We denote by \( \text{sat}_p(L) \) the set \( \{f \in \mathbb{Z}[x]^n \mid pf \in L\} \) where \( p \in \mathbb{Z} \) is a prime number. An infinite set \( S \) is said to be linear independent over a ring \( R \) if any finite set of \( S \) is linear independent over \( R \), that is \( \sum_{i=1}^k a_i g_i = 0 \) for \( a_i \in R \) and \( g_i \in S \) implies \( a_i = 0, i = 1,\ldots,k \)
Lemma 7.6 Let \( C \) be a generalized Hermite normal form and \( L = (C) \). Then \( \text{sat}_p(L) = L \) if and only if \( C_\infty \) is linear independent over \( \mathbb{Z}_p \), where \( C_\infty \) is defined in \( \mathbb{Z}_p \).

Proof: “⇒” Assume the contrary, that is, \( C_\infty = \{h_1, h_2, \ldots \} \) defined in \( \mathbb{Z}_p \) is linear dependent over \( \mathbb{Z}_p \). Then there exist \( a_i \in \mathbb{Z}_p \) not all zero, such that \( \sum_{i=1}^{r} a_i h_i = 0 \) in \( \mathbb{Z}_p[x]^n \) and hence \( \sum_{i=1}^{r} a_i h_i = pg \) in \( \mathbb{Z}[x]^n \). By Lemma 3.11 \( h_i \) are linear independent over \( \mathbb{Z}_p \) and hence \( g \neq 0 \). Since \( \text{sat}_p(L) = L \), we have \( g \in L \). By Lemma 3.12 there exist \( b_i \in \mathbb{Z} \) such that \( g = \sum_{i=1}^{r} b_i h_i \). Hence \( \sum_{i=1}^{r} (a_i - pb_i) h_i = 0 \) in \( \mathbb{Z}[x]^n \). By Lemma 3.11 \( a_i \) = \( pb_i \) and hence \( a_i = 0 \) in \( \mathbb{Z}_p[x] \), a contradiction.

“⇐” Assume the contrary, that is, there exists a \( g \in \mathbb{Z}[x]^n \), such that \( g \notin L \) and \( pg \in L \). By Lemma 3.12 \( pg = \sum_{i=1}^{r} a_i h_i \), where \( a_i \in \mathbb{Z} \). \( p \) cannot be a factor of all \( a_i \). Otherwise, \( g = \sum_{i=1}^{r} \frac{a_i}{p} h_i \in L \). Then some of \( a_i \) is not zero in \( \mathbb{Z}_p \), which means \( \sum_{i=1}^{r} a_i h_i = 0 \) is nontrivial linear relation among \( C \) over \( \mathbb{Z}_p \), a contradiction.

From the “⇒” part of the above proof, we have

Corollary 7.7 Let \( \sum_{i=1}^{r} a_i h_i = 0 \) be a nontrivial linear relation among \( h_i \) in \( \mathbb{Z}_p[x]^n \), where \( a_i \in \mathbb{Z}_p \). Then, in \( \mathbb{Z}[x]^n \), \( \sum_{i=1}^{r} a_i h_i = ph \) and \( h \notin (C) \).

Lemma 7.8 Let \( C = [c_1, \ldots, c_s] \) be a generalized Hermite normal form and \( L = (C) \). Then \( \text{sat}_p(L) = L \) if and only if \( C_\infty \) is linear independent over \( \mathbb{Z}_p \) for the prime factors of \( q \) defined in step 2 of Algorithm ZFactor.

Proof: By Definition 3.6 the leading monomial of \( x^k c_{r_j,j} \in C_\infty \) is of the form \( c_{r_j,j,0} x^{k+d_{r_j,j}} e_{r_j} \) and \( c_{r_i,i,0} \cdots c_{r_i,2,0} | c_{r_i,1,0} \). If \( p \) is coprime with \( \prod_{i=1}^{s} c_{r_i,1,0} \), then \( c_{r_j,j,0} \neq 0 \) mod \( p \) for \( 1 \leq j \leq l_i \). Therefore, the leading monomials of the elements of \( C_\infty \) are linear independent over \( \mathbb{Z}_p \), and hence \( C_\infty \) is linear independent over \( \mathbb{Z}_p \). Therefore, it suffices to consider prime factors of \( \prod_{i=1}^{s} c_{r_i,1,0} \).}

To check whether \( C_\infty \) is linear independent over \( \mathbb{Z}_p \), we first consider a subset of \( C_\infty \) in the following lemma.

Lemma 7.9 Let \( C \) be the generalized Hermite normal form given in \( \mathbb{Z}_p \). Then \( C^+ \) defined in \( \mathbb{Z}_p \) is linear independent over \( \mathbb{Z}_p \) if and only if \( \{c_{r_1,i_1}, c_{r_2,i_2}, \ldots, c_{r_l,i_l}\} \) are linear independent over \( \mathbb{Z}_p[x] \).

Proof: This is obvious since \( \sum_{i=1}^{r} \sum_{j=0}^{d_{r,i}} a_{i,j} x^j c_{r_i,i} = \sum_{i} p_i c_{r_i,i} \), where \( a_{i,j} \in \mathbb{Z} \) and \( p_i = \sum_{j} a_{i,j} x^j \).

Lemma 7.10 Let \( B \) be a Hermite normal form in \( \mathbb{Z}_p[x]^n \) and \( g = \{g_1, \ldots, g_r\} \subset \mathbb{Z}_p[x]^n \). Then \( g \cup B_\infty \) is linear dependent over \( \mathbb{Z}_p \) if and only if

- either \( g_i = \text{grem}(g_i, B) = 0 \) in \( \mathbb{Z}_p[x]^n \) for some \( i \), or
- the residue set \( \{\text{grem}(g_i, B) : i = 1, \ldots, r\} \) are linear dependent over \( \mathbb{Z}_p \).
Proof: We may assume that \( \text{grem}(g_i, B) = 0 \) does not happen, since it gives a nontrivial linear relation of \( g \cup B_\infty \). By Lemma 3.12, \( \tilde{g}_i = g_i \mod B_\infty \). \( g \cup B_\infty \) is linear dependent over \( \mathbb{Z}_p \) if and only if there exist \( a_i \in \mathbb{Z}_p \) not all zero such that \( \sum a_i g_i = 0 \mod B_\infty \) over \( \mathbb{Z}_p \), which is valid if and only if \( \sum a_i \tilde{g}_i = 0 \mod B_\infty \). Since \( \tilde{g}_i \) are \( G \)-reduced with respect to \( B \), \( \sum a_i \tilde{g}_i = 0 \mod B_\infty \) if and only if \( \sum a_i g_i = 0 \), that is \( \tilde{g}_i \) are linear dependent over \( \mathbb{Z}_p \). \( \square \)

Proposition 7.11 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 \( C = [c_1, \ldots, c_s] \). By Lemma 7.6, to check whether \( \text{sat}_Z(c_1, \ldots, c_s) \) is \( \mathbb{Z} \)-saturated, it suffices to check for any prime \( p \), \( C_\infty \) is linear independent over \( \mathbb{Z}_p \). Furthermore, by Lemma 7.8, 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 \( C^+ \) in (3) is linear independent over \( \mathbb{Z}_p \). By Lemma 7.9, we need only to consider whether \( C_1 = \{c_{r_1,l_1}, c_{r_2,l_2}, \ldots, c_{r_t,l_t}\} \) is linear independent over \( \mathbb{Z}_p[x] \). It is clear that \( C_1 \) is linear independent over \( \mathbb{Z}_p[x] \) if and only if \( G = \emptyset \), where \( G \) is given in step 3.2.

In step 3.3, \( C_1 \) is linear dependent over \( \mathbb{Z}_p \). If \( G \neq \emptyset \) for any \( g = [g_1, \ldots, g_t]^T \in G \), \( \sum_{i=1}^t g_i c_{r_i,l_i} = 0 \) in \( \mathbb{Z}_p[x] \). Hence \( \sum_{i=1}^t g_i c_{r_i,l_i} = ph \) where \( h \in \mathbb{Z}[x]^n \). By Corollary 7.7, \( h \notin L \). The correctness of Algorithm ZFactor is proved in this case.

In steps 3.4 - 3.10, we handle the case where \( C^+ \) is linear independent over \( \mathbb{Z}_p \). In step 3.4, we compute the Hermite normal form of \( C_1 \) in \( \mathbb{Z}_p[x]^n \), which is possible because \( \mathbb{Z}_p[x]^n \) is a PID [3]. Furthermore, we have [3]

\[
[c_{r_1,l_1}, \ldots, c_{r_t,l_t}] N = [b_1, \ldots, b_t]
\]

where \( \{b_1, \ldots, b_t\} \) is a Hermite normal form and \( N \) is an inversive matrix in \( \mathbb{Z}_p[x]^{t \times t} \). Then \( C_\infty = C_- \cup C^+ \) is linear independent over \( \mathbb{Z}_p \) if and only if

\[
\tilde{C} = C_- \cup B_\infty = C_- \cup \bigcup_{j=0}^\infty \{x^j b_1, \ldots, x^j b_t\} \text{ is linear independent over } \mathbb{Z}_p. \quad (39)
\]

By Lemma 7.10, property (39) is valid if and only if \( \text{grem}(c, B) \neq 0 \) for all \( c \in C_- \) and the residue set \( C_- \) is linear 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 \( C_\infty \) over \( \mathbb{Z}_p \). By Corollary 7.7, such a relation leads to an \( h \in \text{sat}_Z(L) \setminus L \). The correctness of the algorithm is proved.

As a direct consequence of Lemma 5.20 and Algorithm ZFactor, we have the algorithm to compute the \( M \)-saturation.
Algorithm 5 — SatM($f_0, \ldots, f_s$)

**Input:** A set of vectors $f = \{f_0, \ldots, f_s\} \subset \mathbb{Z}[x]^n$.

**Output:** A generalized Hermite normal form $g$ such that $\text{sat}_M(f) = (g)$.

1. Using Algorithm ZFactor, we can compute $m_i \in \mathbb{N}$ and $g_i \in \mathbb{Z}[x]^n, i = 1, \ldots, s$ such that $\text{sat}_Z(f) = (g_1, \ldots, g_s)$ and $m_ig_i \in (f)$.
2. Let $S = \emptyset$ and for $i = 1, \ldots, s$, if $m_i \neq 1$ then $S = S \cup \{(x - o_{m_i})g_i\}$.
3. Compute the generalized Hermite normal form $g$ of $f \cup S$ and return $g$.

Notice that if $m_i = 1$ then $o_{m_i} = 0$ and $g_i \in (f)$. The numbers $m_i$ need not to be unique for the following reasons. Suppose $m_i = n_ik$ and $n_ig_i \in (f)$. Then by Corollary 5.15, $o_{m_i} = o_{n_i} + cn_i$ and hence $(x - o_{m_i})g_i = (x - o_{n_i})g_i + cn_ig_i \in (f)$. That is, we can replace $m_i$ by its factor $n_i$.

**Proposition 7.12** Algorithm SatM is correct.

**Proof:** Let $L_1 = (f)$ and $L_2 = (f, (x - o_{m_1})g_1, \ldots, (x - o_{m_s})g_s)$. We claim that $\text{sat}_Z(L_1) = \text{sat}_Z(L_2)$. Since $L_1 \subset L_2$, $\text{sat}_Z(L_1) \subset \text{sat}_Z(L_2)$. Since $\text{sat}_Z(L_1) = (g_1, \ldots, g_s)$, we have $L_2 \subset \text{sat}_Z(L_1)$ and hence $\text{sat}_Z(L_2) \subset \text{sat}_Z(L_1)$. The claim is proved. Then $\text{sat}_Z(L_2) = (g_1, \ldots, g_s)$ and $m_ig_i \in L_1 \subset L_2$. Since $(x - o_{m_i})g_i \in L_2, i = 1, \ldots, s$, $L_2$ is $M$-saturated by Lemma 5.20.

### 7.3 Algorithms for Laurent binomial and binomial $\sigma$-ideals

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

Algorithm 6 — CharSet

**Input:** $F$: a finite set of Laurent $\sigma$-binomials in $\mathcal{F}\{y^\pm\}$.

**Output:** if $|F| = 1$; otherwise, a regular and coherent Laurent binomial $\sigma$-chain $A$ such that $|A| = |F|$ and $A$ is a characteristic set of the $\sigma$-ideal $F$.

1. Let $F = \{y^{f_1} - c_1, \ldots, y^{f_r} - c_r\}$ and $f = \{f_1, \ldots, f_r\}$.
2. Compute a set of generators $H \subset \mathbb{Z}[x]^r$ of $\ker_{\mathbb{Z}[x]}([f_1, \ldots, f_r])$ with Algorithm GKER.
3. If for any $h = (h_1, \ldots, h_r)^T \in H, \prod_{i=1}^r c_i^{h_i} \neq 1$, then return $\emptyset$.
4. Compute the reduced Gröbner basis $g$ of $f$ with Algorithm GHNF.
5. Let $g = \{g_1, \ldots, g_s\}$ and $g_i = \sum_{k=1}^r a_{i,k}f_k$, where $a_{i,k} \in \mathbb{Z}[x], i = 1, \ldots, s$.
6. Return $A = \{g_1, \ldots, g_s\}$, where $g_i = y^{g_i} - d_i$ and $d_i = \prod_{k=1}^r c_k^{a_{i,k}}, i = 1, \ldots, s$.

**Proposition 7.13** Algorithm CharSet is correct.
Proof: Steps 1-3 uses Proposition 4.4 to check whether $[F] = [1]$. Note that $(\mathcal{F})$ and $(\mathcal{G})$ are the support lattices of the binomial $\sigma$-ideals $[F]$ and $[G]$, respectively. By Corollary 4.3, $[F] = [G]$. By Theorem 4.14, $A$ is a regular and coherent $\sigma$-chain and hence a characteristic set of $[A]$. □

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

Algorithm 7 — Reflexive

Input: $P$: a finite set of Laurent $\sigma$-binomials in $\mathcal{F}\{Y\}$, where $\mathcal{F}$ is inversive.

Output: $A$: a regular and coherent Laurent binomial $\sigma$-chain such that $[A]$ is the reflexive closure of $[P]$.

1. Let $G = \text{CharSet}(P)$. If $G = \emptyset$, return 1.
2. Let $G = \{g_1, \ldots, g_s\}$, $g_i = Y^{g_i} - d_i$, and $g = [g_1, \ldots, g_s] \in \mathbb{Z}[x]^{n \times s}$.
3. $H = \text{XFactor}(g)$.
4. If $H = \emptyset$, return $G$.
5. Let $H = \{(h_i, e_i) | i = 1, \ldots, r\}$ and $e_i = (e_{i1}, \ldots, e_{is})^T$.
6. Let $P := G \cup \{Y^{h_i} - \sigma^{-1}(\prod_{j=1}^s d_{j}^{e_{ij}}), i = 1, \ldots, r\}$, and go to step 1.

Proposition 7.14 Algorithm Reflexive is correct.

Proof: The algorithm basically follows the proof of Theorem 5.5. By CharSet, $[P] = [G]$ and $G$ is a regular and coherent $\sigma$-chain. In step 4, if $H = \emptyset$, then $(g)$ is $x$-saturated, and by Theorem 5.3, $[G]$ is reflexive and the theorem is proved. Otherwise, we execute steps 5 and 6. Let $\mathcal{I}_1 = [P]$, $L_1 = (\mathcal{F})$, $\mathcal{I}_2 = [G \cup \{Y^{h_i} - \sigma^{-1}(\prod_{j=1}^s d_{j}^{e_{ij}}), i = 1, \ldots, r\}]$, and $L_2 = \mathbb{L}(\mathcal{I}_2)$. Then, we have $\mathcal{I}_1 \subset \mathcal{I}_2 \subset \mathcal{I}_x$ and $L_1 \subset L_2 \subset L_x$, where $L_x = \text{sat}_x(\mathcal{L})$ and $\mathcal{I}_x$ is the reflexive closure of $\mathcal{I}_1$. Similar to the proof of Theorem 5.5, the algorithm will terminate and output the reflexive closure of $[P]$. □

Remark 7.15 Similar to Algorithm Reflexive, we can give algorithms to check whether a Laurent binomial $\sigma$-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 $\sigma$-ideals.

46
Algorithm 8 — DecLaurent

**Input:** $P$: a finite set of Laurent $\sigma$-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 $\sigma$-chains $C_1, \ldots, C_t$ such that $[C_i]$ are Laurent reflexive prime $\sigma$-ideals and $\{P\} = \cap_{i=1}^t[C_i]$ is a minimal decomposition.

1. Let $F = \text{Reflexive}(P)$. If $F = 1$, return $\emptyset$.
2. Set $R = \emptyset$ and $\mathcal{F} = \{F\}$.
3. While $\mathcal{F} \neq \emptyset$.
   1. Let $F = \{\mathbb{Y}^{f_1} - c_1, \ldots, \mathbb{Y}^{f_r} - c_r\} \in \mathcal{F}$, $F = \mathcal{F} \setminus \{F\}$.
   2. Let $G = \text{CharSet}(F)$. If $G = \emptyset$, goto step 3.
   3. Let $G = \{g_1, \ldots, g_s\}$, $g_i = \mathbb{Y}^{g_i} - d_i$, and $g = [g_1, \ldots, g_s] \in \mathbb{Z}[x]^n \times s$.
   4. $H = \text{ZFACTOR}(g)$.
   5. If $H = \emptyset$, add $G$ to $R$.
   6. Let $H = \{(h_i, k_i, e_i)\mid i = 1, \ldots, r\}$ and $e_i = (e_{i_1}, \ldots, e_{i_s})^\tau$.
   7. For $i = 1, \ldots, t$, let $r_{i,1}, \ldots, r_{i,k_i}$ be the $k_i$-th roots of $\prod_{j=1}^s d_j^{e_{i,j}}$.
   8. For $l_1 = 1, \ldots, k_1, \ldots, l_t = 1, \ldots, k_t$, add $G \cup \{\mathbb{Y}^{h_1} - r_{1,l_1}, \ldots, \mathbb{Y}^{h_t} - r_{t,l_t}\}$ to $\mathcal{F}$.
4. Return $R$.

**Example 7.16** Let $P = \{g_1, g_2, g_3\}$, where $g_1 = y_1^{-2}y_1^{k_1} - 1$, $g_2 = y_2^{-2}y_2^{k_2} - 1$, $g_3 = y_1y_2x^{-2}y_3^2 - 1$, and $k \geq 2$. $[P]$ is already reflexive, so step 1 does nothing. $P$ is already a regular and coherent chain, so $G = P$. Let $g_1 = [x^k - 2, 0, 0]^\tau$, $g_2 = [0, x^k - 2, 0]^\tau$, $g_3 = [1, -x, 2]^\tau$ be the supports of $g_1$, $g_2$, and $g_3$, respectively. Then $[g_1, g_2, g_3]$ is already a generalized Hermite normal form.

In Steps 3.4-3.6, $H = \{(h_1, k_1, e_1)\}$, where $h_1 = [1, -x, x^k]^\tau$, $k_1 = 2$, $e_1 = [-1, x, x^k]^\tau$.

In Step 3.7, $r_{1,1} = 1$ and $r_{1,2} = -1$. In Step 3.8, $P_1 = y_1y_2x^{-2}y_3^k - 1$ and $P_2 = y_1y_2^{-2}y_3^{k_2} + 1$ are added to $G$ to obtain $C_1 = \{g_1, g_2, g_3, P_1\}$ and $C_2 = \{g_1, g_2, g_3, P_2\}$. Both $[C_1]$ and $[C_2]$ are reflexive and prime, and are returned.

To see why the algorithm is correct, from $e_1 = [-1, x, x^k]$, we have $(g_1 + 1)^{-1}(g_2 + 1)^{x}(g_3 + 1)^{x^k} = y_1^2y_2^{2x}y_3^{2x^k} = 1 \mod [P]$. Hence, $P_1P_2 = y_1^2y_2^{-2x}y_3^{2x^k} - 1 \in [P]$.

**Proposition 7.17** Algorithm DecLaurent is correct.

**Proof:** The algorithm basically follows the proof of Theorem 7.4. The proof is similar to that of Theorem 7.4. By the proof of Theorem 7.4, we obtain a minimal decomposition. □

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

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

where $0 \neq f_i \in \mathbb{N}[x]$ and $\forall(y_c/S)$ 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: \((Y_0, B, Y_1)\): \(Y_0, Y_1\) are disjoint subsets of \(Y\) and \(B\) a finite set of \(\sigma\)-binomials or \(\sigma\)-monomials in \(F(Y)\).

Output: \((Y_0, B, Y_1)\): \(Y_0, Y_1\) are disjoint subsets of \(Y\), \(B\) consists of proper \(\sigma\)-binomials, and \(V(Y_0 \cup B/Y_1) = \bigcup_{i=1}^{r} V(Y_0i \cup Bi/Y_1i)\).

1. Set \(R = \emptyset\) and \(F = \{(Y_0, B, Y_1)\}\).
2. While \(F \neq \emptyset\).
   2.1. Let \(C = (Y_0, B, Y_1) \in F, F = F \setminus \{C\}\).
   2.2. For all \(y_c \in Y_0\), 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 \(\sigma\)-monomials, add \((Y_0, B_1, Y_1)\) to \(R\) and goto step 2.
   2.4. Let \(M = \prod_{i=1}^{k} y_i^{f_i} \in B_1\), where \(0 \neq f_i \in \mathbb{N}[x]\). \(B_1 = B_1 \setminus \{M\}\).
   2.5. Let \(Y_2 := \{y_{c_1}, \ldots, y_{c_s}\} \setminus Y_1\). If \(Y_2 = \emptyset\), go to step 2; else let \(Y_2 = \{y_{t_1}, \ldots, y_{t_s}\}\).
   2.6. For \(i = 1, \ldots, s\), add \((Y_0 \cup \{y_{t_i}\}, B_1, Y_1 \cup \{y_{t_1}, \ldots, y_{t_{i-1}}\})\) to \(F\).
3. Return \(R\).

We now give the main algorithm. The algorithm basically follows the proof of Theorem 6.27. The main modification is that instead of the perfect ideal decomposition \(\{F\} = \{(1) = m) \bigcap_{i=1}^{n} (F, y_i)\}\), we use the following zero decomposition

\[
V(F) = V(\{1\} = \bigcup_{i=1}^{n} V(F \cup \{y_i\}/\{y_1, \ldots, y_{i-1}\})).
\]

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

Algorithm 10 — DecBinomial

Input: \(F\): a finite set of \(\sigma\)-binomials in \(F(Y)\).

Output: \(\emptyset\), if \(\{F\} = [1]\) or \((C_1, Y_1), \ldots, (C_r, Y_r)\), where \(Y_i \subset Y\) and \(C_i\) are regular and coherent \(\sigma\)-chains containing \(\sigma\)-binomials or variables in \(Y \setminus Y_i\) such that \(\sigma(C_i)\) are reflexive prime \(\sigma\)-ideals and \(\{F\} = \bigcap_{i=1}^{r} \sigma(C_i)\).

1. Set \(R = \emptyset\) and \(F = DecMono(\emptyset, F, \emptyset)\).
2. While \(F \neq \emptyset\).
   2.1. Let \(C = (Z_0, B, Z_1) \in F, F = F \setminus \{C\}\).
   2.2. If \(B = \emptyset\), add \((Z_0, Z_1)\) to \(R\).
   2.3. Let \(E = DecLaurent(B)\) in \(F(Z^\pm)\), where \(Z = Y \setminus Z_0\) and \(m = |Z|\).
   2.4. If \(E = \emptyset\) goto step 2.
   2.5. Let \(E = \{E_1, \ldots, E_l\}\) and \(E_l = \{Z^{f_{l,1}} - c_{l,1}, \ldots, Z^{f_{l,s_l}} - c_{l,s_l}\}\), where \(f_{l,k} \in \mathbb{Z}[x]^m\).
   2.6. Add \((\{Z_0, Z^{f_{l,1}} - c_{l,1}Z_{c_{l,1}}, \ldots, Z^{f_{l,s_l}} - c_{l,s_l}Z_{c_{l,s_l}}\}, Z_1)\) to \(R\), \(l = 1, \ldots, k\).
   2.7. Let \(Z = \{y_{c_1}, \ldots, y_{c_s}\}\). For \(i = 1, \ldots, s\), do \(F = F \cup DecMono(Z_0 \cup \{y_{c_i}\}, B, Z_1 \cup \{y_{c_1}, \ldots, y_{c_{i-1}}\})\).
3. Return \(R\).
Example 7.18 Let \( A = \{A_1, A_2, A_3\} \), where \( A_1 = y_1^k - y_1^3 \), \( A_2 = y_2^k - y_2^3 \), \( A_3 = y_3^k - y_2^3 \), and \( k \geq 2 \). In Step 1, we have \( \mathbb{F} = \{\langle 0, A, 0 \rangle\} \). From Example 7.16 in Step 2.3, we have \( E = \{C_1, C_2\} \), where \( C_1 \) and \( C_2 \) are given in Example 7.16. In Step 2.7, \( \langle E_1, 0 \rangle \) and \( \langle E_2, 0 \rangle \) are added to \( \mathbb{F} \), where \( E_1 = \{A_1, A_2, A_3, Q_1\} \), \( E_2 = \{A_1, A_2, A_3, Q_2\} \), and \( Q_1 = y_3^k - y_2^3 \), \( Q_2 = y_3^k + y_2^3 \). In Step 2.8, \( Z = \{y_1, y_2, y_3\} \) and \( \langle (y_1, y_2, 0, 0), (y_2, y_3), \{A_1\}, \{y_1\} \rangle \) are added to \( \mathbb{F} \). Finally, we have the following decomposition \( \{A\} = \{y_1, y_2\} \cap \text{sat}(\mathbb{F}) \cap \text{sat}(C_1) \cap \text{sat}(C_2) \), where all components are reflexive and prime.

Remark 7.19 Using the algorithm in [9], the following decomposition is obtained: \( \{A\} = \{y_1, y_2\} \cap \text{sat}(\mathbb{F}) \cap \text{sat}(A) \). From Example 7.16, \( \text{sat}(\mathbb{F}) \) is not prime. Then, Algorithm DecBinomial is stronger than the general decomposition algorithm given in [9].

Proposition 7.20 Algorithm DecBinomial is correct.

Proof: In step 1, \( \sigma \)-monomials in \( \mathbb{F} \) are treated. In step 2, we will treat the components of \( \mathbb{F} \) one by one. In step 2.1, the component \( \langle Z_0, B, Z_1 \rangle \) is taken from \( \mathbb{F} \). In step 2.3, \( \{B\} \) is decomposed as \( \{B\} = \cap_{l=1}^{k} \{E_l\} \in \mathbb{F}(\mathbb{Z}^+) \), where \( E_l \) are regular and coherent \( \sigma \)-chains and \( \{E_l\} \) are reflexive prime ideals. By (30) and Corollary 6.30, we have

\[
\{B\} : m = \{B\} \cap \mathbb{F}(\mathbb{Z}) = \cap_{l=1}^{k} (\{E_l\} \cap \mathbb{F}(\mathbb{Z}^+)) \cap \mathbb{F}(\mathbb{F}) = \cap_{l=1}^{k} \text{sat}(E_l^+),
\]

where \( E_l^+ = \{Z_i^{l+1} - c_{i,l}Z_i^{l+1}, \ldots, Z_i^{l+1} - c_{i,k}Z_i^{l+1}\}, l = 1, \ldots, k \). Since \( E_l \) is regular and coherent, by Lemma 6.31, \( E_l^+ \) is also regular and coherent. Since \( \{E_l\} \) is reflexive and prime, by Corollary 6.31, \( \text{sat}(E_l^+) \) is also reflective and prime. Note that \( \emptyset = \emptyset \) in step 2.4 if and only if \( \{B\} \) contains a \( \sigma \)-monomial.

Since \( B \subset \mathbb{F}(\mathbb{Z}) \), we have the following decomposition

\[
\mathbb{V}(Z_0 \cup B/Z_1) = \mathbb{V}(Z_0 \cup \{B\} : m/Z_1) = \cup_{l=1}^{k} \mathbb{V}(Z_0 \cup B \cup \{y_{c_1}, \ldots, y_{c_{l-1}}\} \cup Z_1),
\]

where \( \mathbb{V}(Z_0 \cup B \cup \{y_{c_1}, \ldots, y_{c_{l-1}}\} \cup Z_1) \) is further simplified with Algorithm DecMono in step 2.8. From (40),

\[
\mathbb{V}(Z_0 \cup \{B\} : m/Z_1) = \cap_{l=1}^{k} \mathbb{V}(\text{sat}(Z_0, E_l^+)/Z_1) = \cup_{l=1}^{k} \mathbb{V}(\text{sat}(E_l^+)/Z_1),
\]

where \( \{Z_0, E_l^+\} \) is a regular and coherent \( \sigma \)-chain since \( E_l^+ \) does not contain variables in \( Z_0 \). The above formula explains why \( \{Z_0, E_l^+\} \) is added to \( \mathbb{F} \) in steps 2.5-2.7.

Let the algorithm returns \( \mathbb{R} = \{\langle C_i, Y_i \rangle ; i = 1, \ldots, m\} \). From the above proof, we have

\[
\mathbb{V}(F) = \cup_{l=1}^{k} \mathbb{V}(\text{sat}(C_i)/Y_i).\n\]

Since \( Y_i \cap C_i = \emptyset \) and \( \text{sat}(C_i) \) is a reflexive and prime \( \sigma \)-ideal, the Cohn closure of \( \mathbb{V}(\text{sat}(C_i)/Y_i) \) is \( \mathbb{V}(\text{sat}(C_i)) \) and hence

\[
\mathbb{V}(F) = \cup_{l=1}^{k} \mathbb{V}(\text{sat}(C_i)/Y_i).\n\]

By the difference Hilbert Nullstellensatz, \( \{F\} = \cap_{l=1}^{k} \{\text{sat}(C_i)\} = \cap_{l=1}^{k} \text{sat}(C_i) \). The algorithm terminates, since after each execution of step 2, in the new components \( \{Y_0, B_l, Y_{11}\} \) added to \( \mathbb{F} \) in step 2.8, \( B_l \) contains at least one less variables than \( B \). \( \square \)
8 Conclusion

In this paper, we initiate the study of binomial $\sigma$-ideals. Two basic tools used to study binomial $\sigma$-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 \cite{7}.

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

For binomial $\sigma$-ideals, we show that certain properties of algebraic binomial ideals given in \cite{7} can be extended to the difference case using the theory of Gröbner basis in the case of infinitely many variables. It is shown that most properties of Laurent binomial $\sigma$-ideal can be extended to the normal binomial $\sigma$-ideals.

Algorithms are given for the key results of the paper. We give algorithms to check whether a given Laurent binomial difference ideal $I$ is reflexive, prime, well-mixed, or perfect, and in the negative case, to compute the reflexive, well-mixed, and perfect closures of $I$. An algorithm is given to decompose a finitely generated perfect binomial difference ideal as the intersection of reflexive prime binomial difference ideals.

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 \cite{18} and were used to connect the differential Chow form \cite{8} and differential sparse resultant \cite{18}. But, contrary to the difference case, the defining ideal for a differential toric variety is generally not binomial.

References

[1] M. Barile, M. Morales, A. Thoma. Set-theoretic Complete Intersections on Binomials, Proc. AMS, 130(7), 1893-1903, 2001.

[2] D. Bouziane, A. Kandri Rody, H. Maârouf. Unmixed-dimensional Decomposition of a Finitely Generated Perfect Differential Ideal, Journal of Symbolic Computation, 31(6), 631-649, 2001.

[3] H. Cohen. A Course in Computational Algebraic Number Theory, Springer-Verlag, Berlin, 1993.

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

[5] D. Cox, J. Little, D. O'Shea. Using Algebraic Geometry, Springer-Verlag, New York, 1998.
[6] A. Dickenstein, L. F. Matusevich, E. Miller. Combinatorics of Binomial Primary Decomposition, *Mathematische Zeitschrift*, 264(4), 745-763, 2010.

[7] D. Eisenbud and B. Sturmfels. Binomial Ideals, *Duke Math. J.*, 84(1), 1-45, 1996.

[8] X. S. Gao, W. Li, C. M. Yuan. Intersection Theory in Differential Algebraic Geometry: Generic Intersections and the Differential Chow Form, *Trans. of Amer. Math. Soc.*, 365(9), 4575-4632, 2013.

[9] X. S. Gao, Y. Luo, C. M. Yuan. A Characteristic Set Method for Ordinary Difference Polynomial Systems, *Journal of Symbolic Computation*, 44(3), 242-260, 2009.

[10] X.S. Gao, J. Van der Hoeven, C.M. Yuan, G.L. Zhang, Characteristic Set Method for Differential-difference Polynomial Systems, *Journal of Symbolic Computation*, 44(9), 1137-1163, 2009.

[11] K. O. Geddes, S. R. Czapor, G. Labahn. *Algorithms for Computer Algebra*, Kluwer Academic Publishers, Boston, MA, 1992.

[12] V. P. Gerdt and D. Robertz. Computation of Difference Gröbner Bases, *Computer Science Journal of Moldova*, 20(2), 203-226, 2012.

[13] E. Hrushovski. The Elementary Theory of the Frobenius Automorphisms, Available from [http://www.ma.huji.ac.il/~ehud/](http://www.ma.huji.ac.il/~ehud/), July, 2012.

[14] K. I. Iima and Y. Yoshino. Gröbner Bases for the Polynomial Ring with Infinite Variables and Their Applications, *Communications in Algebra*, 37:10, 3424-3437, 2009.

[15] R. J. Jing, C. M. Yuan, X. S. Gao. A Polynomial-time Algorithm to Compute Generalized Hermite Normal Form of Matrices over $\mathbb{Z}[x]$, [arXiv:1601.01067](http://arxiv.org/abs/1601.01067), 2016.

[16] U. Koppenhagen and E. W. Mayr. An Optimal Algorithm for Constructing the Reduced Gröbner Basis of Binomial Ideals, *Proc. ISSAC’96*, ACM Press, 55-62, 1996.

[17] A. Levin. *Difference Algebra*, Springer-Verlag, New Work, 2008.

[18] W. Li, C. M. Yuan, X. S. Gao. Sparse Differential Resultant for Laurent Differential Polynomials, *Foundations of Computational Mathematics*, 15(2), 451-517, 2015.

[19] I. O. Martínez de Castilla, R. P. Sánchez. Cellular Binomial Ideals. Primary Decomposition of Binomial Ideals, *Journal of Symbolic Computation*, 30(4), 383-400, 2000.

[20] M. P. Millán, A. Dickenstein, A. Shiu, C. Conradi. Chemical Reaction Systems with Toric Steady States, *Bull. Math. Biol.*, 74, 1027-1065, 2012.

[21] E. Miller and B. Sturmfels. *Combinatorial Commutative Algebra*, Springer-Verlag, New York, 2005.

[22] L. Pachter and B. Sturmfels (eds). *Algebraic Statistics for Computational Biology*, Cambridge University Press, 2005.
[23] I. Peeva and B. Sturmfels. Syzygies of Codimension 2 Lattice Ideals, *Mathematische Zeitschrift*, 229(1), 163-194, 1998.

[24] J. F. Ritt and J. L. Doob. Systems of Algebraic Difference Equations, *American Journal of Mathematics*, 55(1), 505-514, 1933.

[25] M. Saleemi and K. H. Zimmermann. Linear Codes as Binomial Ideals, *International Journal of Pure and Applied Mathematics*, 61(2), 147-156, 2010.

[26] M. Wibmer. *Algebraic Difference Equations*, Preprint, 2013.