Criteria for Finite Difference Gröbner Bases of Normal Binomial Difference Ideals

Yu-Ao Chen
KLMM, UCAS, Academy of Mathematics and Systems Science, Chinese Academy of Sciences
Beijing, China 100190
chenyuao115@mails.ucas.ac.cn

Xiao-Shan Gao
KLMM, UCAS, Academy of Mathematics and Systems Science, Chinese Academy of Sciences
Beijing, China 100190
xgao@mmrc.iss.ac.cn

ABSTRACT

In this paper, we give decision criteria for normal binomial difference polynomial ideals in the univariate difference polynomial ring $\mathcal{F}\{y\}$ to have finite difference Gröbner bases and an algorithm to compute the finite difference Gröbner bases if these criteria are satisfied. The novelty of these criteria lies in the fact that complicated properties about difference polynomial ideals are reduced to elementary properties of univariate polynomials in $\mathbb{Z}[x]$.

CCS CONCEPTS

• **Computing methodologies → Symbolic and algebraic algorithms**;

KEYWORDS

Difference algebra; binomial difference polynomial ideal; Gröbner basis; difference Gröbner basis.

1 INTRODUCTION

Difference algebra founded by Ritt and Cohn aims to study algebraic difference equations in a similar way that polynomial equations are studied in commutative algebra [3, 12, 15]. The concept of difference Gröbner bases was extended to linear difference polynomial ideals in [9, 12] and nonlinear difference polynomial ideals in [9]. Difference Gröbner bases have many applications [6, 8, 11, 12].

Even for finitely generated difference polynomial ideals, their difference Gröbner bases could be infinite as shown by Example 2.2 in this paper. This makes it impossible to compute difference Gröbner bases for general difference polynomial ideals and thus it is a crucial issue to give criteria for difference polynomial ideals to have finite difference Gröbner bases.

Let $\mathcal{F}$ be a difference field and y a difference indeterminate. In this paper, we will give decision criteria for normal binomial difference polynomial ideals in $\mathcal{F}\{y\}$ to have finite difference Gröbner bases and an algorithm to compute these finite difference Gröbner bases under these criteria. A difference ideal $\mathcal{I}$ in $\mathcal{F}\{y\}$ is called normal if $MP \in \mathcal{I}$ implies $P \in \mathcal{I}$ for any difference monomial M in $\mathcal{F}\{y\}$ and $P \in \mathcal{F}\{y\}$. $\mathcal{I}$ is called binomial if it is generated by difference polynomials with at most two terms [4, 6].

For $f \in \mathbb{Z}[x]$, let $f^+, f^- \in \mathbb{N}[x]$ be the positive part and the negative part of f such that $f = f^+ - f^-$. For $h = \sum_{i=0}^{m} a_i x^i \in \mathbb{N}[x]$, denote $y^h = \prod_{i=0}^{m} (\sigma^i y)^{a_i}$, where σ is the difference operator of $\mathcal{F}$. For a given $f \in \mathbb{Z}[x]$ with a positive leading coefficient, we consider the following normal binomial difference polynomial ideal in $\mathcal{F}\{y\}$:

$$\mathcal{I}_f = \mathrm{sat}(y^{f^+} - y^{f^-}) = [\{y^{h^+} - y^{h^-} \mid h = gf, g \in \mathbb{Z}[x]\}],$$

where sat is the difference saturation ideal. Let

$$\begin{aligned} \Phi_0 &\triangleq \{h \in \mathbb{Z}[x] \mid \mathrm{lt}(h) = h^+\}, \\ \Phi_1 &\triangleq \{h \in \mathbb{Z}[x] \mid hg \in \Phi_0, g \in \mathbb{Z}[x] \text{ and is monic}\}. \end{aligned}$$

We prove that $\mathcal{I}_f$ has a finite difference Gröbner basis if and only if $f \in \Phi_1$. This criterion is then extended to general normal binomial difference ideals in $\mathcal{F}\{y\}$.

The decision of $f \in \Phi_1$ is quite nontrivial and we give the following criteria for $f \in \Phi_1$ based on the roots of f:

(1) if f has no positive roots, then $f \in \Phi_1$;
(2) if f has more than one positive root, then $f \notin \Phi_1$;
(3) if f has one positive root x_+ and a root z such that $|z| > x_+$, then $f \notin \Phi_1$;
(4) if $f \notin \Phi_0$ has a unique positive real root x_+ and $x_+ < 1$, then $f \notin \Phi_1$;

With these and some extra criteria, only one case is open: f has a unique positive real root x_+, $x_+ > 1$, and $x_+ > |z|$ for any other root z of f. We conjecture that $f \in \Phi_1$ in the above case based on numerical computations.

As far as we know the above criteria are the first non-trivial ones for a difference polynomial ideal to have a finite difference Gröbner basis. The novelty of these criteria lies in the fact that complicated properties about difference polynomial ideals are reduced to elementary properties of univariate polynomials in $\mathbb{Z}[x]$.

2 PRELIMINARIES

2.1 Difference Gröbner basis

An ordinary difference field, or simply a σ-field, is a field $\mathcal{F}$ with a third unitary operation σ satisfying: for any $a, b \in \mathcal{F}$, $\sigma(a+b) = \sigma(a) + \sigma(b)$, $\sigma(ab) = \sigma(a)\sigma(b)$, and $\sigma(a) = 0$ if and only if $a = 0$. We call σ the *difference or transforming operator* of $\mathcal{F}$. A typical example of σ-field is $\mathbb{Q}(\lambda)$ with $\sigma(f(\lambda)) = f(\lambda + 1)$. In this paper, we use σ- as the abbreviation for difference.

Partially supported by an NSFC grant 11688101.

ISSAC '17, July 25-28, 2017, Kaiserslautern, Germany

ACM ISBN 978-1-4503-5064-8/17/07…$15.00
https://doi.org/10.1145/3087604.3087615

For a in any σ-extension ring of $\mathcal{F}$ and $n \in \mathbb{N}_{>0}$, denote $a^{x^n} = \sigma^n(a)$, with the usual assumption $a^0 = 1$ and $x^0 = 1$. More generally, for $p = \sum_{i=0}^{s} c_i x^i \in \mathbb{N}[x]$, denote $a^p = \prod_{i=0}^{s} (\sigma^i a)^{c_i}$ [6]. For instance, $a^{3x^2+x+4} = (\sigma^2(a))^3 \sigma(a) a^4$.

Let S be a subset of a σ-field $\mathcal{G}$ which contains $\mathcal{F}$. We will denote $\Theta(S) = \{\sigma^k a \,|\, k \in \mathbb{N}, a \in S\}$, $\mathcal{F}\{S\} = \mathcal{F}[\Theta(S)]$. Now suppose $\mathbb{Y} = \{y_1, \ldots, y_n\}$ is a set of σ-indeterminates over $\mathcal{F}$. The monomials in $\Theta(\mathbb{Y})$ are called σ-monomials in $\mathbb{Y}$. The elements of $\mathcal{F}\{\mathbb{Y}\} = \mathcal{F}[\Theta(\mathbb{Y})]$ are called *σ-polynomials* over $\mathcal{F}$ in $\mathbb{Y}$. A *σ-polynomial ideal* $\mathcal{I}$, or simply a σ-ideal, in $\mathcal{F}\{\mathbb{Y}\}$ is a *possibly infinitely generated* ordinary algebraic ideal satisfying $\sigma(\mathcal{I}) \subset \mathcal{I}$. If S is a subset of $\mathcal{F}\{\mathbb{Y}\}$, we use (S) and $[S]$ to denote the algebraic ideal and the σ-ideal generated by S.

A monomial order in $\mathcal{F}\{\mathbb{Y}\}$ is called *compatible* with the σ-structure, if $y_i^{x^{k_1}} < y_j^{x^{k_2}}$ for $k_1 < k_2$. Only compatible monomial orders are considered in this paper. When a monomial order is given and $P \in \mathcal{F}\{\mathbb{Y}\}$, we use $\mathbf{LM}(P)$ and $\mathbf{LC}(P)$ to denote the largest monomial and its coefficient in P respectively, and $\mathbf{LT}(P) = \mathbf{LC}(P)\mathbf{LM}(P)$ the leading term of P.

Definition 2.1. $\mathbb{G} \subset \mathcal{F}\{\mathbb{Y}\}$ is called a *σ-Gröbner basis* of a σ-ideal $\mathcal{I}$ if for any $P \in \mathcal{I}$, there exist $m \in \mathbb{N}$ and $G \in \mathbb{G}$ such that $(\mathbf{LM}(G))^{x^m} | \mathbf{LM}(P)$.

From the definition, $\mathbb{G}$ is a σ-Gröbner basis of $\mathcal{I}$ if and only if $\Theta(\mathbb{G})$ is an algebraic Gröbner basis of $\mathcal{I}$ treated as an algebraic polynomial ideal in $\mathcal{F}[\Theta(\mathbb{Y})]$. Note that $\mathcal{I}$ is generally an infinitely generated ideal and the concept of infinite Gröbner basis [10] is adopted here. From this observation, we may see that a σ-Gröbner basis satisfies most of the properties of the usual algebraic Gröbner basis. For instance, $\mathbb{G}$ is a σ-Gröbner basis of a σ-ideal $\mathcal{I}$ if and only if for any $P \in \mathcal{I}$, we have $\mathrm{grem}(P, \Theta(\mathbb{G})) = 0$, where $\mathrm{grem}(P, \Theta(\mathbb{G}))$ is the normal form of P modulo $\Theta(\mathbb{G})$. The concepts of *reduced σ-Gröbner bases* could be similarly introduced [6].

The following example shows that even a finitely generated σ-ideal may have an infinite σ-Gröbner basis.

Example 2.2. Let $\mathcal{I} = [y_1 y_2^x - y_1^x y_2, y_1 y_3 - 1]$. Assume $y_1 < y_2 < y_3$. Under a compatible monomial order, the reduced σ-Gröbner basis of the ideal $\mathcal{I} \cap \mathcal{F}\{y_1, y_2\}$ is $\{y_1 y_2^{x^i} - y_1^{x^i} y_2 \,|\, i \in \mathbb{N}_{>0}\}$ [6, Example 63].

2.2 Difference characteristic set

The *elimination ranking* $\mathscr{R}$ on $\Theta(\mathbb{Y}) = \{\sigma^k y_i | 1 \le i \le n, k \in \mathbb{N}\}$ is used in this paper: $\sigma^k y_i > \sigma^l y_j$ if and only if $i > j$ or $i = j$ and $k > l$, which is a total order over $\Theta(\mathbb{Y})$. By convention, $1 < \sigma^k y_j$ for $k \in \mathbb{N}$.

Let $f \in \mathcal{F}\{\mathbb{Y}\}$. The greatest $y_j^{x^k}$ appearing effectively in f is called the *leader* of f, denoted by $\mathrm{ld}(f)$ and y_j is called the *leading variable* of f, denoted by $\mathrm{lvar}(f) = y_j$. The leading coefficient of f as a univariate polynomial in $\mathrm{ld}(f)$ is called the *initial* of f and is denoted by $\mathrm{init}(f)$.

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

A finite sequence of nonzero σ-polynomials $\mathcal{A} : A_1, \ldots, A_m$ is called a *σ-chain* if $m = 1$ and $A_1 \neq 0$ or $m > 1$, $A_j > A_i$ and A_j is Ritt-reduced w.r.t. A_i for $1 \le i < j \le m$. A σ-chain $\mathcal{A}$ can be written as the following form [7]

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

where $\mathrm{ld}(A_{ij}) = y_{c_i}^{x^{o_{ij}}}$, $o_{is} < o_{it}$ and $\deg(A_{is}, \mathrm{ld}(A_{is})) > \deg(A_{it}, \mathrm{ld}(A_{it}))$ for $s < t$. Here is an example of σ-chain: $\mathcal{A} : y_1^x - 1, y_1^2 y_2^2 - 1, y_2^x - 1$.

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

$$\prod_{i=1}^{t} I_i^{e_i} \cdot P \equiv R, \mathrm{mod}\,[\mathcal{A}],$$

where the $e_i \in \mathbb{N}[x]$ and denote $R = \mathrm{prem}(P, \mathcal{A})$ [7].

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

Let $\mathcal{A} : A_1, \ldots, A_t$ be a σ-chain, $I_i = \mathrm{init}(A_i)$, and $y_{l_i}^{x^{o_i}} = \mathrm{ld}(A_i)$. $\mathcal{A}$ is called *regular* if for any $j \in \mathbb{N}$, $I_i^{x^j}$ is invertible w.r.t $\mathcal{A}$ [7]. To introduce the concept of coherent σ-chain, we need to define the *Δ-polynomial* first. If A_i and A_j have distinct leading variables, we define $\Delta(A_i, A_j) = 0$. If A_i and A_j $(i < j)$ have the same leading variable y_l, $\mathrm{ld}(A_i) = y_l^{x^{o_i}}$, and $\mathrm{ld}(A_j) = y_l^{x^{o_j}}$, then $o_i < o_j$ [7]. Define $\Delta(A_i, A_j) = \mathrm{prem}((A_i)^{x^{o_j - o_i}}, A_j)$. $\mathcal{A}$ is called *coherent* if $\mathrm{prem}(\Delta(A_i, A_j), \mathcal{A}) = 0$ for all $i < j$ [7].

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

$$\mathrm{sat}(\mathcal{A}) = [\mathcal{A}] : \mathbb{I}_{\mathcal{A}} = \{P \in \mathcal{F}\{\mathbb{Y}\} \,|\, \exists M \in \mathbb{I}_{\mathcal{A}}, MP \in [A]\}.$$

The following result is needed in this paper.

Theorem 2.3. *[7, Theorem 3.3] A σ-chain $\mathcal{A}$ is a characteristic set of* $\mathrm{sat}(\mathcal{A})$ *if and only if $\mathcal{A}$ is regular and coherent.*

We also need the concept of algebraic saturation ideal. Let C be an algebraic triangular set in $\mathcal{F}[x_1, \ldots, x_n]$ and I the product of the initials of the polynomials in C. Define

$$\mathrm{asat}(C) = \{P \in \mathcal{F}[x_1, \ldots, x_n] \,|\, \exists k \in \mathbb{N}, I^k P \in (C)\}.$$

2.3 σ-Gröbner basis for a binomial σ-ideal

A σ-monomial in $\mathbb{Y}$ can be written as $\mathbb{Y}^{\mathbf{f}} = \prod_{i=1}^{n} y_i^{f_i}$, where $\mathbf{f} = (f_1, \ldots, f_n)^\tau \in \mathbb{N}[x]^n$. A nonzero vector $\mathbf{f} = (f_1, \ldots, f_n)^\tau \in \mathbb{Z}[x]^n$ is said to be *normal* if the leading coefficient of f_s is positive, where s is the largest subscript such that $f_s \neq 0$. All given vectors in this paper are assumed to be normal. For $\mathbf{f} \in \mathbb{Z}[x]^n$, let $\mathbf{f}^+, \mathbf{f}^- \in \mathbb{N}^n[x]$ denote respectively the positive part and the negative part of $\mathbf{f}$ such that $\mathbf{f} = \mathbf{f}^+ - \mathbf{f}^-$. Then for a normal $\mathbf{f} \in \mathbb{Z}[x]^n$, $\mathbf{LT}(\mathbb{Y}^{\mathbf{f}^+} - c\mathbb{Y}^{\mathbf{f}^-}) = \mathbb{Y}^{\mathbf{f}^+}$.

A *σ-binomial* in $\mathbb{Y}$ is a σ-polynomial with at most two terms. A σ-ideal in $\mathcal{F}\{\mathbb{Y}\}$ is called *binomial* if it is generated by, possibly infinitely many, σ-binomials [6]. We have

Proposition 2.4. *[6, Corollary 5.5] A σ-ideal $\mathcal{I}$ is binomial if and only if the reduced σ-Gröbner basis for $\mathcal{I}$ consists of σ-binomials.*

Let $\mathbb{m}$ be the multiplicative set generated by $y_i^{x^j}$ for $i = 1, \ldots, n$, $j \in \mathbb{N}$. A σ-ideal $\mathcal{I}$ is called *normal* if for $M \in \mathbb{m}$ and $P \in \mathcal{F}\{\mathbb{Y}\}$, $MP \in \mathcal{I}$ implies $P \in \mathcal{I}$. Normal σ-ideals in $\mathcal{F}\{\mathbb{Y}\}$ are closely related with the $\mathbb{Z}[x]$-modules in $\mathbb{Z}[x]^n$ [5, 6]. We first introduce a new concept.

Definition 2.5. A *partial character* ρ on $\mathbb{Z}[x]^n$ is a homomorphism from a $\mathbb{Z}[x]$-module L_ρ in $\mathbb{Z}[x]^n$ to the multiplicative group $\mathcal{F}^*$ satisfying $\rho(x\mathbf{f}) = (\rho(\mathbf{f}))^x$ for $\mathbf{f} \in L_\rho$.

A $\mathbb{Z}[x]$-module generated by $\mathbf{h}_1, \ldots, \mathbf{h}_m \in \mathbb{Z}[x]^n$ is denoted as $(\mathbf{h}_1, \ldots, \mathbf{h}_m)_{\mathbb{Z}[x]}$. Let ρ be a partial character over $\mathbb{Z}[x]^n$ and $\mathbb{f} = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$ a reduced Gröbner basis of the $\mathbb{Z}[x]$-module $L_\rho = (\mathbb{f})_{\mathbb{Z}[x]}$. For $\mathbf{h} \in \mathbb{Z}[x]^n$ and $H \subset L_\rho$, denote $\mathbb{P}_\mathbf{h} = \mathbb{Y}^{\mathbf{h}^+} - \rho(\mathbf{h})\mathbb{Y}^{\mathbf{h}^-}$ and $\mathbb{P}_H = \{\mathbb{P}_\mathbf{h} \mid \mathbf{h} \in H\}$. Introduce the following notations associated with ρ:

$$\mathcal{I}^+(\rho) := [\mathbb{P}_{L_\rho}] = [\mathbb{Y}^{\mathbf{f}^+} - \rho(\mathbf{f})\mathbb{Y}^{\mathbf{f}^-} \mid \mathbf{f} \in L_\rho] \quad (1)$$
$$\mathcal{A}^+(\rho) := \mathbb{P}_\mathbb{f} = \{\mathbb{Y}^{\mathbf{f}_1^+} - \rho(\mathbf{f}_1)\mathbb{Y}^{\mathbf{f}_1^-}, \ldots, \mathbb{Y}^{\mathbf{f}_s^+} - \rho(\mathbf{f}_s)\mathbb{Y}^{\mathbf{f}_s^-}\}.$$

It is shown that [6] $\mathcal{A}^+(\rho)$ is a regular and coherent σ-chain and hence is a characteristic set of $\mathrm{sat}(\mathcal{A}^+(\rho))$ by Theorem 2.3. Furthermore, we have [6]

Theorem 2.6. *The following conditions are equivalent.*

(1) *$\mathcal{I}$ is a normal binomial σ-ideal in $\mathcal{F}\{\mathbb{Y}\}$.*
(2) *$\mathcal{I} = \mathcal{I}^+(\rho)$ for a partial character ρ over $\mathbb{Z}[x]^n$.*
(3) *$\mathcal{I} = \mathrm{sat}(\mathcal{A}^+(\rho))$ for a partial character ρ over $\mathbb{Z}[x]^n$.*

From Proposition 2.4 and Theorem 2.6, we have

Corollary 2.7. *Let ρ be a partial character over $\mathbb{Z}[x]^n$. Then $\mathbb{P}_{L_\rho}$ is a σ-Gröbner basis of $\mathcal{I}^+(\rho)$.*

Corollary 2.8. *Let ρ be a partial character over $\mathbb{Z}[x]^n$ and $H \subset L_\rho$. Then $\mathbb{P}_H$ is a σ-Gröbner basis of $\mathcal{I}^+(\rho)$ if and only if for any normal $\mathbf{g} \in L_\rho$, there exist $\mathbf{h} \in H$ and $j \in \mathbb{N}$, such that $\mathbf{g}^+ - x^j\mathbf{h}^+ \in \mathbb{N}[x]^n$.*

Proof: By Corollary 2.7, $\mathbb{P}_{L_\rho}$ is a σ-Gröbner basis of $\mathcal{I}^+(\rho)$. Then $\mathbb{P}_H$ is a σ-Gröbner basis of $\mathcal{I}^+(\rho)$ if and only if for any normal $\mathbf{g} \in L_\rho$, there exist $\mathbf{h} \in H$ and $j \in \mathbb{N}$ such that $\mathbf{LM}(x^j\mathbb{P}_\mathbf{h}) | \mathbf{LM}(\mathbb{P}_\mathbf{g})$, that is, $\mathbf{g}^+ - x^j\mathbf{h}^+ \in \mathbb{N}[x]^n$.

Example 2.9. Let $\mathbf{f} = [1 - x, x - 1]$, $L = (\mathbf{f})_{\mathbb{Z}[x]}$, and ρ the trivial partial character on L, that is, $\rho(\mathbf{h}) = 1$ for $\mathbf{h} \in$L. Then $\mathbb{P}_\mathbf{f} = y_1y_2^x - y_1^x y_2$. By Theorem 2.6, $\mathcal{I}^+(\rho) = \mathrm{sat}(\mathbb{P}_\mathbf{f})$. By Example 2.2, $\mathrm{sat}(\mathbb{P}_\mathbf{f}) = [\mathbb{P}_\mathbf{f}, y_1y_3 - 1] \cap \mathbb{Q}\{y_1, y_2\} = [y_1y_2^{x^i} - y_1^{x^i}y_2 \mid i \in \mathbb{N}_{>0}]$, and a reduced σ-Gröbner basis of $\mathcal{I}^+(\rho)$ is $\{y_1y_2^{x^i} - y_1^{x^i}y_2 \mid i \in \mathbb{N}_{>0}\}$.

3 FINITE σ-GRÖBNER BASIS CRITERIA

In this section, we give criteria for the σ-Gröbner basis of a normal binomial σ-ideal in $\mathcal{F}\{y\}$ to be finite, where y is a σ-indeterminate. From Theorem 2.6, this is to decide whether the σ-Gröber basis of a σ-ideal $\mathcal{I}$ is finite when the characteristic set of $\mathcal{I}$ is given. Without loss of generality, we assume $\rho(\mathbf{h}) = 1$ for all partial characters ρ and $\mathbf{h} \in L_\rho$.

3.1 Singleton characteristic set case

In this subsection, we consider the simplest case: $n = 1$ and $L_\rho = (f)_{\mathbb{Z}[x]}$ is generated by one polynomial $f \in \mathbb{Z}[x]$. We will see that even this case is highly nontrivial. For a nonzero $g \in \mathbb{Z}[x]$, we use $\mathrm{lc}(g)$, $\mathrm{lm}(g)$, and $\mathrm{lt}(g)$ to represent the leading coefficient, leading monomial, and leading term of g, respectively.

In the rest of this section, we assume $f \in \mathbb{Z}[x]$ and $\mathrm{lc}(f) > 0$. Then $\mathbb{P}_f = y^{f^+} - y^{f^-}$ and $\mathbf{LT}(\mathbb{P}_f) = y^{f^+}$. By Theorem 2.6, all normal binomial σ-ideals in $\mathcal{F}\{y\}$ whose characteristic set consists of a single σ-polynomial can be written as:

$$\mathcal{I}_f = \mathrm{sat}(\mathbb{P}_f) = [y^{h^+} - y^{h^-} \mid h = fg, g \in \mathbb{Z}[x], \mathrm{lc}(g) > 0]. \quad (2)$$

In this section, we will give a criterion for $\mathcal{I}_f$ to have a finite σ-Gröbner basis. Define

$$\Phi_0 \triangleq \{f \in \mathbb{Z}[x] \mid \mathrm{lt}(f) = f^+\}.$$
$$\Phi_1 \triangleq \{f \in \mathbb{Z}[x] \mid fg \in \Phi_0, g \in \mathbb{Z}[x] \text{ and is monic}\}. \quad (3)$$

We now give the main result of this section, which can be deduced from Lemma 3.3 and Lemma 3.6.

Theorem 3.1. *$\mathcal{I}_f$ in (2) has a finite σ-Gröbner basis if and only if $f \in \Phi_1$.*

For h_1 and $h_2 \in \mathbb{Z}[x]$, denote $h_1 \succeq h_2$ if $h_1 - h_2 \in \mathbb{N}[x]$. For h_1 and $h_2 \in \mathbb{N}[x]$, we have $h_1 \succeq h_2$ if and only if $y^{h_2} \mid y^{h_1}$.

Lemma 3.2. *If $f \in \Phi_0$ then $\{\mathbb{P}_f\}$ is a σ-Gröbner basis of $\mathcal{I}_f$.*

Proof: For $h \in (f)_{\mathbb{Z}[x]}$ with $\mathrm{lc}(h) > 0$, $\exists\, g \in \mathbb{Z}[x]$ with $\mathrm{lc}(g) > 0$ such that $h = fg$. Since $f \in \Phi_0$, we have $\mathrm{lt}(f) = f^+$. Then, $x^{\deg(g)}f^+ = \mathrm{lt}(g)f^+/\mathrm{lc}(g) \preceq \mathrm{lt}(g)f^+ = \mathrm{lt}(g)\mathrm{lt}(f) = \mathrm{lt}(h) \preceq h^+$. By Corollary 2.8, $\{\mathbb{P}_f\}$ is a σ-Gröbner basis of $\mathcal{I}_f$.

Lemma 3.3. *If $f \in \Phi_1$ then $\mathcal{I}_f$ has a finite σ-Gröbner basis.*

Proof: Let $h = fg \in \Phi_0$, where g is monic. Then $\mathrm{lc}(h) = \mathrm{lc}(f)$ and $\mathrm{lt}(h) = \mathrm{lt}(f)\mathrm{lm}(g) = h^+$.

$$\mathcal{I}_{\deg(h)} = \mathcal{I}_f \bigcap \mathcal{F}[y, y^x, \cdots, y^{x^{\deg(h)}}]$$

is a polynomial ideal in a polynomial ring with finitely many variables, which has a finite algebraic Gröbner basis denoted by $\mathbb{G}_{\leqslant \deg(h)}$ with the same monomial order of the σ-Gröbner basis. Let $\mathbb{P}_u \in \mathcal{I}_f$ and $\mathrm{lc}(u) > 0$. If $\deg(u) \leqslant \deg(h)$, then there exists a $\mathbb{P}_t \in G_{\leqslant \deg(h)}$ such that $t \preceq u$. Otherwise, we have $\deg(u) > \deg(h)$ and $\mathrm{lc}(u) \geq \mathrm{lc}(f)$. Then

$$\begin{aligned} & x^{\deg(u)-\deg(h)}h^+ = x^{\deg(u)-\deg(f)-\deg(g)}\mathrm{lt}(f)\mathrm{lm}(g) \\ = \;& x^{\deg(u)-\deg(f)}\mathrm{lt}(f) = x^{\deg(u)-\deg(f)}\mathrm{lc}(f)\mathrm{lm}(f) \\ = \;& \mathrm{lc}(f)\mathrm{lm}(u) \preceq \mathrm{lt}(u) \preceq u^+. \end{aligned}$$

Since that $\mathbb{P}_h \in \mathcal{I}_{\deg(h)}$, by Corollary 2.8, $\mathbb{G}_{\leqslant \deg(h)}$ is a finite σ-Gröbner basis of $\mathcal{I}_f$.

Corollary 3.4. *Let $f \in \Phi_1$, $h = gf \in \Phi_0$, g a monic polynomial in $\mathbb{Z}[x]$, and $D = \deg(h)$. Then any finite Gröbner basis of the polynomial ideal $\mathcal{I}_D = \mathcal{I}_f \bigcap \mathcal{F}[y, y^x, \cdots, y^{x^D}]$ is a finite σ-Gröbner basis for $\mathcal{I}_f$.*

Let D be $\mathbb{R}$ or $\mathbb{Z}$. We will use the following new notation

$$D^{>0}[x] \triangleq \{\sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{N},\ \forall i(a_i \in D_{>0})\}.$$

Lemma 3.5. $\mathbb{N}[x] \subseteq \Phi_1$.

Proof: Let $g = a_n x^n + \cdots + a_0 \in \mathbb{N}[x]$ with $d = \max\{d \in \mathbb{N} \mid x^d \mid g\}$. Then $a_d > 0$. Let $s = (x^{n-d} + x^{n-d-1} + \cdots + 1)g = a_n x^{2n-d} + (a_n + a_{n-1})x^{2n-d-1} + \cdots + (a_n + \cdots + a_d)x^n + (a_{n-1} + \cdots + a_d)x^{n-1} + \cdots + a_d x^d$. Rewrite $s = b_{2n-d}x^{2n-d} + \cdots + b_d x^d$. Then $s/x^d \in \mathbb{Z}^{>0}[x]$. Let $M = \lceil \max\{b_{i-1}/b_i \mid d+1 \leqslant i \leqslant 2n-d\} \rceil + 1$. Then $(x-M)s = b_{2n-d}x^{2n-d+1} + (b_{2n-d-1} - Mb_{2n-d})x^{2n-d} + \cdots + (b_d - Mb_{d+1})x^{d+1} - Mb_d x^d \in \Phi_0$. So both s and g are in Φ_1.

Lemma 3.6. *If $f \notin \Phi_1$, then $\mathcal{I}_f$ does not have a finite σ-Gröbner basis.*

Proof: Suppose otherwise, $\mathcal{I}_f$ has a finite σ-Gröbner basis $\mathbb{G} = \mathbb{P}_H$, where $H = \{f_1, \cdots, f_l\} \subset \mathbb{Z}[x]$ with each $\mathrm{lc}(f_i) > 0$. Since f has the lowest degree in $(f)_{\mathbb{Z}[x]}$, we have $f \in H$.

Let $H_c \triangleq \{h \in H \mid \mathrm{lc}(h) = \mathrm{lc}(f)\}$. Since $f \notin \Phi_1$, we have $H_c \bigcap \Phi_1 = \emptyset$ by the definition of Φ_1. For all $h \in H_c$, h^+ has at least two terms by Lemma 3.2 and h^- has at least one term by Lemma 3.5. For $u \in \mathbb{Z}[x]$, define a function

$$\widetilde{\deg}(u) = \deg(u) - (\deg(u^+ - \mathrm{lt}(u))) \tag{4}$$

which is the degree gap between the first two highest monomials of u^+. Suppose h_1 is an element in H_c such that $\widetilde{\deg}(h_1) = \max\{\widetilde{\deg}(h) \mid h \in H_c\}$. h_1 exists because $f \in H_c \neq \emptyset$ and H_c is a finite set. Denote $\mathrm{lt}(h_1) \triangleq ax^n$, $\tilde{h}_1 \triangleq h_1 - \mathrm{lt}(h_1)$, $\mathrm{lt}(\tilde{h}_1^+) \triangleq bx^m$, and $\tilde{\tilde{h}}_1^+ \triangleq \tilde{h}_1^+ - \mathrm{lt}(\tilde{h}_1^+)$. Then $h_1 = ax^n + bx^m + \tilde{\tilde{h}}_1^+ - h_1^-$. Since $h_1 \notin \Phi_1$, we have $ab > 0$. Let $c \triangleq \lceil b/a \rceil \geq 1$ and

$$\begin{aligned} s &= (x^n - cx^m)h_1 = ax^{2n} + x^n\tilde{\tilde{h}}_1^+ + cx^m h_1^- \\ &\quad -(ac-b)x^{m+n} - cx^m\tilde{h}_1^+ - x^n h_1^-. \end{aligned}$$

We have $s^+ \preceq s_0 \triangleq ax^{2n} + x^n\tilde{\tilde{h}}_1^+ + cx^m h_1^-$, and $\widetilde{\deg}(s) = \deg(s) - \deg(s^+ - \mathrm{lt}(s)) \geq \widetilde{\deg}(s_0) = \deg(s_0) - \deg(s_0^+ - \mathrm{lt}(s_0)) > n - m = \widetilde{\deg}(h_1) = \deg(h_1) - \deg(h_1^+ - \mathrm{lt}(h_1))$, that is $\widetilde{\deg}(s) > \widetilde{\deg}(h)$ for any $h \in H_c$.

Since $\mathbb{P}_H$ is a σ-Gröbner basis of $\mathcal{I}_f$, there exist $h \in H$ and $j \in \mathbb{N}$ such that $t = s^+ - x^j h^+ \in \mathbb{N}[x]$. We claim $\mathrm{lt}(t) = \mathrm{lt}(s^+)$. If $h \in H_c$, then $\widetilde{\deg}(s) > \widetilde{\deg}(h)$. Note that $\deg(s^+) = \deg(x^j h)$ implies that the coefficient of the second largest monomial of $s^+ - x^j h$ is negative contradicting to the fact $s^+ - x^j h \in \mathbb{N}[x]$. As a consequence, we must have $\deg(s^+) > \deg(x^j h)$ and the claim is proved in this case. Now let $h \in H \backslash H_c$. Since $\mathrm{lc}(h) > \mathrm{lc}(s) = \mathrm{lc}(f)$, we have $\deg(x^j h) < \deg(s)$ which implies $\mathrm{lt}(t) = \mathrm{lt}(s^+)$. The claim is proved. The fact $\mathrm{lt}(t) = \mathrm{lt}(s^+)$ implies that when computing the normal form $\mathbb{P}_u = \mathrm{grem}(\mathbb{P}_s, \Theta(\mathbb{P}_H))$, we always have $\mathrm{lt}(u) = \mathrm{lt}(s)$. As a consequence, $\mathbb{P}_u \neq 0$ which contradicts to the fact that $\mathbb{P}_H$ is a σ-Gröbner basis of $\mathcal{I}_f$ and $s \in (f)_{\mathbb{Z}[x]}$.

The proof of Lemma 3.6 gives a method to construct arbitrarily many elements in a σ-Gröbner basis.

Example 3.7. Let $f = x^2 - 2x + 1 \notin \Phi_1$. In the proof of Lemma 3.6, $c = \lceil b/a \rceil = 1$ and $s_1 = (x^2-1)f = x^4 + 2x - 2x^3 - 1$. Applying the above procedure to s_1, we obtain $s_2 = (x^4 - 2x)s_1 = x^8 + 3x^4 + 2x - 2x^7 - 4x^2$. Then $\widetilde{\deg}(f) < \widetilde{\deg}(s_1) < \widetilde{\deg}(s_2)$ and $\mathbb{P}_{s_2}$ is in a σ-Gröbner basis. The process can be repeated.

3.2 Normal binomial σ-ideal case

In this subsection, we consider the general normal binomial σ-ideals in $\mathcal{F}\{y\}$. By Theorem 2.6, all normal binomial σ-ideals in $\mathcal{F}\{y\}$ can be written as the following form:

$$\mathcal{I}_{\mathbb{G}} = \mathrm{sat}(\mathbb{P}_{\mathbb{G}}) = [y^{g^+} - y^{g^-} \mid \forall g \in (\mathbb{G})_{\mathbb{Z}[x]}, \mathrm{lc}(g) > 0] \tag{5}$$

where $\mathbb{G} = \{g_1, \ldots, g_t\} \subset \mathbb{Z}[x]$ is a reduced Gröbner basis of ideal $L = (\mathbb{G})_{\mathbb{Z}[x]}$. Gröbner bases in $\mathbb{Z}[x]$ have the following special structure [6, Lemma 3.6].

Lemma 3.8. *Let $\mathbb{G} = \{g_1, \ldots, g_k\}$ be a reduced Gröbner basis of an ideal in $\mathbb{Z}[x]$, $lm(g_1) < \cdots < lm(g_k)$, and $\mathrm{lt}(g_i) = c_i x^{d_i} \in \mathbb{N}[x]$. 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) $\frac{c_i}{c_k} | g_i$ for $1 \leq i < k$. If $\widetilde{b}_1$ is the primitive part of g_1, then $\widetilde{b}_1 | g_i$ for $1 < i \leq k$.

Here are two Gröbner bases in $\mathbb{Z}[x]$: $\{4, 2x\}$, $\{15, 5x, x^2+3\}$.

In the rest of this section, let $L = (\mathbb{G})_{\mathbb{Z}[x]}$ and define

$$L_t \triangleq \{f \in L \mid \mathrm{lc}(f) = c_t = \mathrm{lc}(g_t)\} \tag{6}$$

Theorem 3.9. *$\mathcal{I}_{\mathbb{G}}$ has a finite σ-Gröbner basis if and only if $L_t \bigcap \Phi_0 \neq \emptyset$.*

Proof: Suppose $L_t \bigcap \Phi_0 \neq \emptyset$ and let $g \in L_t \bigcap \Phi_0$. Then $\mathcal{I}_{\mathbb{G}} \bigcap \mathcal{F}[y, y^x, \cdots, y^{x^{\deg(g)}}]$ has a finite algebraic Gröbner basis denoted by $G_{\leq \deg}(g)$. Let $\mathbb{P}_u \in \mathcal{I}_{\mathbb{G}}$ and $\mathrm{lc}(u) > 0$. If $\deg(u) \leq \deg(g)$, then there exists a $\mathbb{P}_h \in G_{\leq \deg(g)}$ such that $h \preceq u$. Otherwise, we have $\deg(u) > \deg(g)$ and $\mathrm{lc}(u) \geq \mathrm{lc}(g)$. Then

$$\begin{aligned} & x^{\deg(u)-\deg(g)} g^+ = x^{\deg(u)-\deg(g)}\mathrm{lt}(g) \\ = \;& x^{\deg(u)-\deg(g)}\mathrm{lc}(g)\mathrm{lm}(g) = \mathrm{lc}(g)\mathrm{lm}(u) \leq \mathrm{lt}(u) \leq u^+. \end{aligned}$$

By Corollary 2.8, $\mathbb{G}_{\leq \deg(g)}$ is a finite σ-Gröbner basis of $\mathcal{I}_{\mathbb{G}}$, since $\mathbb{P}_g$ is in $\mathbb{G}_{\leq \deg(g)}$.

We will prove the other direction by contradiction. Suppose that $L_t \bigcap \Phi_0 = \emptyset$ and $\mathcal{I}_{\mathbb{G}}$ has a finite σ-Gröbner basis $\mathbb{P}_H = \{\mathbb{P}_{u_1}, \cdots, \mathbb{P}_{u_k}\}$. Let $H = \{u_1, \cdots, u_k\}$, and $H_c = H \bigcap L_t$. Since $\mathrm{grem}(\mathbb{P}_{g_t}, \Theta(\mathbb{P}_H)) = 0$, we have $H_c \neq \emptyset$. Let u_1 be an element of H_c with maximal $\widetilde{\deg}$ defined in (4). Since $L_t \cap \Phi_0 = \emptyset$, by Lemma 3.5 u_1^+ contains at least two terms and $u_1^- \neq 0$. Similar to the proof of Lemma 3.6, an $s \in L$ is constructed such that $\widetilde{\deg}(s) > \widetilde{\deg}(u_1)$ and $\mathrm{lc}(s) = \mathrm{lc}(u_1)$. Then, $\mathrm{grem}(\mathbb{P}_s, \Theta(\mathbb{P}_H)) \neq 0$ contrary to the fact that $\mathbb{P}_H$ is a σ-Gröbner basis.

Corollary 3.10. *If $g_t \in \Phi_1$, then $\mathcal{I}_{\mathbb{G}}$ has a finite σ-Gröbner basis.*

We show that $g_t \in \Phi_1$ is not a necessary condition.

Example 3.11. Let $\mathbb{G} = \{2(x^2-2), (x^2-2)(x+1)\}$. Then $(x^2-2)(x+1)(x-1) + 2(x^2-2) = x^4 - x^2 - 2 \in \Phi_0 \subset \Phi_1$, and hence $\mathcal{I}_{\mathbb{G}}$ has a finite σ-Gröbner basis. On the other hand, we will show $(x^2-2)(x+1) \notin \Phi_1$ in Example 4.9.

Corollary 3.12. *If $\mathcal{I}_{\mathbb{G}}$ has a finite σ-Gröbner basis, then $g_1 \in \Phi_1$.*

Proof: Let $\widetilde{b}_1$ be the primitive part of g_1. By Lemma 3.8, $\widetilde{b}_1 | h$ for $h \in L$. By Theorem 3.9, $\widetilde{b}_1$ and hence g_1 is in Φ_1.

We need the following effective Polya Theorem.

Lemma 3.13 ([13]). *Suppose that* $f(x)=\sum_{j=0}^{n} a_n x^n \in \mathbb{R}[x]$ *is positive on* $[0,\infty)$ *and* $F(x,y)$ *the homogenization of* f. *Then for* $N_f > \frac{n(n-1)L}{2\lambda}-n$, $(1+x)^{N_f} f(x) \in \mathbb{R}^{>0}[x]$, *where* $\lambda=\min\{F(x,1-x)\mid x\in[0,1]\}$ *and* $L=\max\{\frac{k!(n-k)!}{n!}|a_k|\}$.

Corollary 3.14. *If there exists an* $h \in L$ *with no positive real roots, then* $\mathcal{I}_{\mathbb{G}}$ *has a finite* σ*-Gröbner basis.*

Proof. Write $h=x^{m_1}h_1$ such that $h_1(0)\neq 0$. By Lemma 3.13, there exists an $N\in\mathbb{N}$ such that $h_2=(x+1)^N h\in\mathbb{Z}^{>0}[x]$. Take a sufficiently large N such that $\deg(h_2)>d_t=\deg(g_t)$. Then there exists a sufficiently large $M\in\mathbb{N}$, such that $\overline{g}=x^{m_1}(x^{\deg(h_2)-\deg(g_t)+1}g_t - Mh_2)\in\Phi_0$. Since $\overline{g}\in L_t$, by Theorem 3.9, $\mathcal{I}$ has a finite σ-Gröbner basis.

4 σ-GRÖBNER BASIS COMPUTATION

In this section, we will give criteria and an algorithm for deciding if $f\in\Phi_1$. If $f\in\Phi_1$, we also give an algorithm to compute the finite σ-Gröbner basis.

A necessarily condition for $f\in\Phi_1$ is $\mathrm{lc}(f)>0$. Also, it is easy to show that $f\in\Phi_1$ if and only if $cx^m f\in\Phi_1$ for any $c,m\in\mathbb{N}$. So in the rest of this paper, we assume

$$f=a_nx^n+\cdots+a_1x+a_0\in\mathbb{Z}[x]$$

such that $n>0$, $a_n>0$, $a_0\neq 0$, and $\gcd(a_0,a_1,\ldots,a_n)=1$.

4.1 Membership decision criteria for Φ_1

In this subsection, we will study whether $f\in\Phi_1$ by examining properties of the roots of $f(x)=0$.

Lemma 4.1. *If* $f\in\mathbb{Z}[x]$ *has no positive real roots, then* $f\in\Phi_1$.

Proof. By Lemma 3.13, there exists an $N\in\mathbb{N}$, such that $(x+1)^N f\in\mathbb{Z}^{>0}[x]\subseteq\mathbb{N}[x]$. By Lemma 3.5, $(x+1)^N f\in\mathbb{N}[x]\subseteq\Phi_1$, and thus $f\in\Phi_1$.

By Lemma 4.1, we need only consider those polynomials which have positive roots.

Lemma 4.2. *If* $f\in\Phi_0$, *then* f *has a simple and unique positive real root* x_+, *and for any root* z *of* f, $|z|\leq x_+$.

Proof. Since $f\in\Phi_0\setminus\mathbb{Z}$, the number of sign differences of f is one. Then by Descartes' rule of signs [14], the number of positive real roots of f (with multiplicities counted) is one or less than one by an even number. Then f has a simple and unique positive real root x_+. For any root z of f, since $-a_i\geq 0$ for $i=0,\ldots,n-1$, we have

$$a_n|z|^n=|-a_{n-1}z^{n-1}-\cdots-a_0|\leq -a_{n-1}|z|^{n-1}-\cdots-a_0. \tag{7}$$

Thus $f(|z|)\leqslant 0$ and hence f has at least one real root in $[|z|,\infty)$. Since f has a unique positive real root x_+, we have $|z|\leqslant x_+$.

We now consider those f which have a root $z\neq x_+$ and $|z|=x_+$. Such a z must be either $-x_+$ or a complex root.

Lemma 4.3. *Let* $f=a_nx^n+\cdots+a_0\in\Phi_0$ *and* x_+ *the unique positive root of* f. *If* f *has a root* $z\neq x_+$ *but* $|z|=x_+$, *then*

(1) $z^{\delta_f}\in\mathbb{R}_{>0}$ *and* z *is a simple root of* f, *where* $\delta_f=\gcd\{i\mid a_i\neq 0\}>1$.
(2) f *is a polynomial in* x^{δ_f}: $f=\widehat{f}\circ x^{\delta_f}$, *where* $\circ$ *is the function composition. Furthermore,* $\widehat{f}(w)=0$ *and* $|w|=x_+^{\delta_f}$ *imply* $w=x_+^{\delta_f}$.
(3) $\{z\mid f(z)=0,|z|=x_+\}=\{\zeta^k x_+\mid \zeta=e^{\frac{2\pi\mathbf{i}}{\delta_f}},k=1,\ldots,\delta_f\}$, *where* $\mathbf{i}=\sqrt{-1}$.

Proof. Let $z\neq x_+$ be a root of f such that $|z|=x_+$. Then $f(|z|)=f(x_+)=a_n|z|^n+a_{n-1}|z|^{n-1}+\cdots+a_0=0$, which, combining with (7), implies $|-a_{n-1}z^{n-1}-\cdots-a_0|=-a_{n-1}|z|^{n-1}-\cdots-a_0$. The above equation is possible if and only if $-a_iz^i\in\mathbb{R}_{>0}$ for each $i\leq n-1$ and $a_i\neq 0$. Also note, $z^n=(-a_{n-1}|z|^{n-1}-\cdots-a_0)/a_n\in\mathbb{R}_{>0}$. Then, $z^i\in\mathbb{R}_{>0}$ for each $i\leq n$ and $a_i\neq 0$. Note that $z^m\in\mathbb{R}_{>0}$ and $z^k\in\mathbb{R}_{>0}$ imply $z^{m-k}\in\mathbb{R}_{>0}$. As a consequence, $z^{\delta_f}\in\mathbb{R}_{>0}$ for $\delta_f=\gcd\{i\mid a_i\neq 0\}$. Since $z\neq x_+$, we have $\delta_f>1$. Part 1 of the lemma is proved.

From the definition of δ_f, f is a polynomial in x^{δ_f}: $f(x)=\widehat{f}(x)\circ(x^{\delta_f})$. It is easy to see that $\widehat{f}(x)\in\Phi_0$. Let $\widehat{f}(x)=b_kx^k+\cdots+b_1x+b_0$. Then $\gcd\{j\mid b_j\neq 0\}=1$. By the first part of this lemma, we know $x_+^{\delta_f}$ is the only root of f whose absolute value is $x_+^{\delta_f}$. Since z^{δ_f} and $x_+^{\delta_f}$ are both the unique positive real roots of $\widehat{f}(x)$, we have $z^{\delta_f}=x_+^{\delta_f}$ and hence z is a simple root of f. Part 2 of the lemma is proved. Part 3 of the lemma comes from the fact $z^{\delta_f}=x_+^{\delta_f}$ is the unique positive real root of f and $f(z)=\widehat{f}(z^{\delta_f})=0$.

Corollary 4.4. *If* $f\in\Phi_1$ *has at least one positive real root* x_+, *then* x_+ *is the unique positive real root of* f, x_+ *is simple and for any root* z *of* f, $x_+\geqslant|z|$. *If* f *has a root* $z\neq x_+$ *satisfying* $|z|=x_+$, *then* z *is simple, and* $z^\delta\in\mathbb{R}_{>0}$ *for some* $\delta\in\mathbb{N}_{>1}$.

Example 4.5. $f=(x^2-5)(x^2-2x+5)\notin\Phi_1$, because its root $z=1+2\mathbf{i}$ satisfies $|z|=\sqrt{5}$ but $z^\delta\notin\mathbb{R}_{>0}$ for any $\delta\in\mathbb{N}$.

Lemma 4.6. *Let* $q(x)\in\mathbb{Z}[x]$ *be a primitive irreducible polynomial and* $\delta\in\mathbb{N}_{>1}$. *Then* $(q)_{\mathbb{Z}[x]}\bigcap\mathbb{Z}[x^\delta]=(\widetilde{q}(x^\delta))_{\mathbb{Z}[x^\delta]}$, *where* $\widetilde{q}\in\mathbb{Z}[x]$ *is primitive and irreducible and* $\widetilde{q}(x^\delta)^m=R_u(u^\delta-x^\delta,q(u))$ *for some* $m\in\mathbb{N}$. *We use* R_u *to denote the Sylvester resultant w.r.t. the variable* u. *Furthermore, the roots of* $\widetilde{q}(x)$ *are* $\{z^\delta\mid q(z)=0\}$.

Proof. Let $q(x)=a\prod_{j=1}^n(x-z_j)$, $\zeta_\delta=e^{2\pi\mathbf{i}/\delta}$, and

$$\overline{R}(x^\delta) \quad = \quad R_u(u^\delta-x^\delta,q(u))=\prod_{l=1}^{\delta}q(\zeta_\delta^l x).$$

We claim that $\overline{R}(x^\delta)$ is primitive. We have $\mathrm{lc}(R_u(u^\delta-x^\delta,q(u)))=\mathrm{lc}(\prod_{l=1}^\delta q(\zeta_\delta^l x))=a^\delta$. Let $c\in\mathbb{Z}$ be a prime factor of a^δ or a. Since q is primitive, $q\neq 0\ (mod\ c)$. Let $q(x)=bx^m+\cdots\ (mod\ c)$. Then $\mathrm{lt}(\overline{R}(x^\delta))=\mathrm{lt}(\prod_{l=1}^\delta q(\zeta_\delta^l x))=\prod_{l=1}^\delta b(\zeta_\delta^l x)^m=b^\delta x^{\delta m}\neq 0\ (mod\ c)$. So $c\nmid\overline{R}(x^\delta)$ and thus $\overline{R}(x^\delta)$ is primitive.

Since $\mathbb{Q}[x^\delta]$ is a PID and $\overline{R}(x^\delta)\in(q)_{\mathbb{Q}[x]}\bigcap\mathbb{Q}[x^\delta]$, there exists a primitive polynomial $\widetilde{q}\in\mathbb{Z}[x]$ such that $(\widetilde{q}(x^\delta))_{\mathbb{Q}[x^\delta]}=(q)_{\mathbb{Q}[x]}\bigcap\mathbb{Q}[x^\delta]$. Since $q(x)|\widetilde{q}(x^\delta)$ and q is irreducible, $\widetilde{q}(x)$ must be irreducible. Since both $q(x)$ and $\widetilde{q}(x)$ are primitive, we can deduce $(\widetilde{q}(x^\delta))_{\mathbb{Z}[x^\delta]}=(q)_{\mathbb{Z}[x]}\bigcap\mathbb{Z}[x^\delta]$ from $(\widetilde{q}(x^\delta))_{\mathbb{Q}[x^\delta]}=(q)_{\mathbb{Q}[x]}\bigcap\mathbb{Q}[x^\delta]$.

Since $q(x)|\widetilde{q}(x^\delta)$, $Z_\delta=\{\zeta_\delta^k z_j\mid k=1,\ldots,\delta,j=1,\ldots,n\}$ is a subset of the roots of $\widetilde{q}(x^\delta)$. Let $\overline{S}(x)$ be the square-free part of $\overline{R}(x)\in\mathbb{Z}[x]$, which is also primitive. Since Z_δ contains exactly the roots of $\overline{R}(x^\delta)$ and $\overline{S}(x^\delta)$, we have $\overline{S}(x)|\widetilde{q}(x)$. Since $\widetilde{q}(x)$ is irreducible and $\overline{S}(x)$ is the square-free part of $\overline{R}(x)$, we have $\overline{S}(x)=\widetilde{q}(x)$ and

hence $\overline{R}(x^\delta) = \widetilde{q}(x^\delta)^m$ for some $m \in \mathbb{N}[x]$. Finally, since the roots of $\widetilde{q}(x^\delta)$ are $\mathbb{Z}_\delta$, the roots of $\widetilde{q}(x)$ are $\{z^\delta \mid q(z) = 0\}$.

Corollary 4.7. *Let $\delta \in \mathbb{N}$ and $f = \prod_{j=1}^m q_j^{\alpha_j}$, where $\alpha_j \in \mathbb{N}$ and q_j are primitive irreducible polynomials in $\mathbb{Z}[x]$ with positive leading coefficients. Let $q_i^*(x^\delta)$ be the square-free part of $R_u(u^\delta - x^\delta, q_i(u))$ and $f^* \triangleq \operatorname{lcm}(\{q_j^{*\alpha_j} \mid j\})$. Then*

$$(f)_{\mathbb{Z}[x]} \bigcap \mathbb{Z}[x^\delta] = (f^*(x^\delta))_{\mathbb{Z}[x^\delta]}. \tag{8}$$

Furthermore, the roots of $f^*(x)$ are $\{z^\delta \mid f(z) = 0\}$.

Proof: By Lemma 4.6, $(q_i)_{\mathbb{Z}[x]} \bigcap \mathbb{Z}[x^\delta] = (q_i^*(x^\delta))_{\mathbb{Z}[x^\delta]}$. Then $(f)_{\mathbb{Z}[x]} \bigcap \mathbb{Z}[x^\delta] = \bigcap_{i=0}^{s} ((q_i^{\alpha_i})_{\mathbb{Z}[x]} \bigcap \mathbb{Z}[x^\delta] = \bigcap_{i=0}^{s} (q_i^{*\alpha_i})_{\mathbb{Z}[x^\delta]} = (\operatorname{lcm}(\{q_i^{*\alpha_i} \mid i\}))_{\mathbb{Z}[x^\delta]} = (f^*(x^\delta))_{\mathbb{Z}[x^\delta]}$. From $f^* \triangleq \operatorname{lcm}(\{q_j^{*\alpha_j} \mid j\})$ and Lemma 4.6, the roots of $f^*(x)$ are $\{z^\delta \mid f(z) = 0\}$.

Theorem 4.8. *Let $f \in \mathbb{Z}[x]$ have a unique positive root x_+ and any root w of f satisfies $|w| \le x_+$. Assume that there exists a minimal $\delta \in \mathbb{N}_{>1}$ such that for all root $z \ne x_+$ of f, $|z| = x_+$ implies $z^\delta \in \mathbb{R}_{>0}$. Let $f^*(x^\delta) \in \mathbb{Z}[x^\delta]$ be the polynomial in (8). Then $f \in \Phi_1$ if and only if $\operatorname{lc}(f) = \operatorname{lc}(f^*)$ and $f^* \in \Phi_1$.*

Proof: "$\Leftarrow$" Since $\operatorname{lc}(f) = \operatorname{lc}(f^*)$ and $(f) \cap \mathbb{Z}[x^\delta] = (f^*(x^\delta))$, there exists a monic polynomial $h \in \mathbb{Z}[x]$ such that $f^*(x^\delta) = fh$. Since $f^* \in \Phi_1$, there exists a monic polynomial $g \in \mathbb{Z}[x]$ such that $f^*(x)g(x) \in \Phi_0$. Then $f^*(x^\delta)g(x^\delta) = fhg(x^\delta) \in \Phi_0$. Since $hg(x^\delta)$ is monic, we have $f \in \Phi_1$.

"$\Rightarrow$" Since $f \in \Phi_1$, there exists a primitive polynomial $h \in (f) \bigcap \Phi_0$ with $h(0) \ne 0$ and $\operatorname{lc}(h) = \operatorname{lc}(f)$. Each such h has some roots whose absolute value is x_+. Since $f \mid h$, by part 3 of Lemma 4.3 we have $\delta \mid \delta_h$, where $\delta_h = \gcd\{k \mid x^k \text{ is in } h\}$. By Lemma 4.3, $h \in \mathbb{Z}[x^{\delta_h}] \subset \mathbb{Z}[x^\delta]$. Thus $h \in (f) \bigcap \mathbb{Z}[x^\delta] = (f^*)_{\mathbb{Z}[x^\delta]}$. Since $\operatorname{lc}(f) \mid \operatorname{lc}(f^*) \mid \operatorname{lc}(h)$ and $\operatorname{lc}(f) = \operatorname{lc}(h)$, we have $\operatorname{lc}(f) = \operatorname{lc}(f^*) = \operatorname{lc}(h)$, so $f^* \in \Phi_1$.

Example 4.9. Let $f = (x^2 - 2)(x + 1)$. Then $\delta = 2$ and $f^* = (x - 2)(x - 1)$ has two positive roots and hence $f \notin \Phi_1$ by Corollary 4.4 and Theorem 4.8. Let $f_1 = x^2 - 2$, $f_2 = x^2 - 2x + 2$, and $f = f_1 f_2$. Then $\delta = 8$, $f_1^* = x - 16$, $f_2^* = x - 16$, and $f^* = x - 16$. Hence $f \in \Phi_1$.

Corollary 4.10. *Let $f^*(x)$ be defined in Theorem 4.8. Then $f^*(x)$ has only one root (may be a multiple root) whose absolute value is x_+^δ and any root $z \ne x_+^\delta$ of f^* satisfies $|z| < x_+^\delta$.*

Proof: By Corollary 4.7, the roots of $f^*(x)$ are $\{z^\delta \mid f(z) = 0\}$. Then the corollary comes from the fact that x_+ is the unique positive real root of f and $f(z) = 0, |z| = x_+$ imply $z^\delta \in \mathbb{R}_{>0}$.

Lemma 4.11. *If $f \in \Phi_1 \setminus \Phi_0$ has a unique positive real root x_+, then $x_+ \geqslant 1$.*

Proof: There exists a monic polynomial $g \in \mathbb{Z}[x]$ such that $fg \in \Phi_0$. Since $f \notin \Phi_0$, g is not a monomial. Without loss of generality we assume $g(0) \ne 0$, and then $\prod_{g(z)=0} |z| = |g(0)/\operatorname{lc}(g)| = |g(0)| \ge 1$ which implies $\max_{g(z)=0}(|z|) \geqslant 1$. Since x_+ is the unique positive root of fg, by Lemma 4.2, we have $x_+ \geqslant \max_{g(z)=0}(|z|) \geqslant 1$.

The following two lemmas give simple criteria to check whether $f \in \Phi_1$ in the case of $f(1) = 0$.

Lemma 4.12. *If $f(1) = 0$ and $\delta \in \mathbb{N}$ is the smallest number such that every root z of f satisfies $z^\delta = 1$, then $f \in \Phi_1$ if and only if $f^*(x) = x - 1$, where f^* is defined in (8).*

Proof: By Theorem 4.8, if $f^*(x) = x - 1$ then $f \in \Phi_1$. Suppose $f \in \Phi_1$. By Lemma 4.3, any root of f is simple and hence f is square-free. Let m_z be the minimal positive integer such that $z^{m_z} = 1$ for given root z of f, and $\delta = \operatorname{lcm}\{m_z \mid f(z) = 0\}$. Since f is primitive, $\delta \in \mathbb{N}$ is the smallest number such that $f(x) \mid x^\delta - 1$ in $\mathbb{Z}[x]$. Therefore, $f^*(x) = x - 1$.

Example 4.13. Let $f = (x - 1)(x^2 + 1)(x^3 + 1)$. Then $\delta = 12$ and $f^* = x - 1$. So, $f \in \Phi_1$. Let $f = (x - 1)(x^2 + 1)^2(x^3 + 1)$. Then $\delta = 12$ and $f^* = (x - 1)^2$. So, $f \notin \Phi_1$.

Lemma 4.14. *If $f(1) = 0$ and any other root z of f satisfies $|z| < 1$, then $f \in \Phi_1$ if and only if $f(x)/(x-1) \in \mathbb{Z}[x^\delta]$ for some $\delta \in \mathbb{N}_{>0}$ and $f(x)(x^\delta - 1)/(x - 1) \in \Phi_0$.*

Proof: The necessity is obvious. For the other direction, there exists a monic polynomial $g \in \mathbb{Z}[x]$ such that $fg \in \Phi_0$. We claim that each root z of g has absolute value 1. Since g is monic, $\prod_{g(z)=0} |z| \ge 1$. Since $fg \in \Phi_0$ and $f(1) = 0$, $\max_{g(z)=0} |z| \le 1$, and the claim is proved.

By Lemma 4.2, $fg \in \mathbb{Z}[x^\delta]$, where $\delta = \delta_{fg}$. Since $f(1) = 0$ and all other roots of f have absolute value < 1, we have $(x^\delta - 1) \mid fg$ and $((x^\delta - 1)/(x - 1)) \mid g$. By part 3 of Lemma 4.3, the roots of fg with absolute value 1 are exactly the roots of $x^\delta - 1$. Since the absolute values of all roots of g are 1 and g has no multiple roots by Lemma 4.3, $g = (x^\delta - 1)/(x - 1)$. Since $fg \in \mathbb{Z}[x^\delta]$ and $(x^\delta - 1) \mid fg$, set $fg = (x^\delta - 1)h(x^\delta)$ for $h \in \mathbb{Z}[x]$. From $g = (x^\delta - 1)/(x - 1)$, we have $f/(x - 1) = h(x^\delta) \in \mathbb{Z}[x^\delta]$.

Now, only when $f \notin \Phi_0$, f has a unique positive real root $x_+ > 1$, and any other root of f has absolute value $< x_+$, we do not know how to decide $f \in \Phi_1$. By computing many examples, we propose the following conjecture.

Conjecture 4.15. *If $f \in \mathbb{Z}[x] \setminus \Phi_0$ has a simple and unique positive real root x_+, $x_+ > 1$, and $x_+ > |z|$ for any other root z of f, then $f \in \Phi_1$.*

4.2 Algorithm for membership of Φ_1

Based on the results proved in the preceding subsection, we give an algorithm to decide whether $f \in \Phi_1$.

Algorithm 1 — MembershipΦ_1 (f)

Input: $f \in \mathbb{Z}[x]$, $\mathrm{lc}(f) > 0$, $f(0) \neq 0$, and f is primitive.
Output: Whether $f \in \Phi_1$.

1. If $\mathrm{lt}(f) = f^+$, then $f \in \Phi_0 \subset \Phi_1$.
2. If f has no positive real roots, then $f \in \Phi_1$.
3. If f has at least two positive real roots (with multiplicities counted), then $f \notin \Phi_1$.
4. Let x_+ be the simple and unique positive real root of f.
   4.1. If $x_+ < 1$, or equivalently $f(1) > 0$, then $f \notin \Phi_1$.
   4.2. If $x_+ = 1$ and all root z of f satisfies $z^\delta = 1$ for some $\delta \in \mathbb{N}$, then $f \in \Phi_1$ if and only if $f^* = x - 1$, where f^* is defined in (8).
   4.3. If $x_+ = 1$ and any other root z of f satisfies $|z| < 1$, then $f \in \Phi_1$ if and only if $f(x)/(x-1) \in \mathbb{Z}[x^\delta]$ for some $\delta \in \mathbb{N}_{>1}$ and $f(x)(x^\delta - 1)/(x-1) \in \Phi_0$.
   4.4. If f has a root z such that $|z| > x_+$, then $f \notin \Phi_1$.
   4.5. If f has a root z such that $z \neq x_+$, $|z| = x_+$, and $(\frac{z}{x_+})^\delta \neq 1$ for any $\delta \in \mathbb{N}_{>1}$, then $f \notin \Phi_1$.
   4.6. Let δ be the minimal integer such that $f(z) = 0$, $z \neq x_+$, and $|z| = x_+$ imply $(\frac{z}{x_+})^\delta = 1$. Then $f \in \Phi_1$ if and only if $\mathrm{lc}(f) = \mathrm{lc}(f^*)$ and $f^* \in \Phi_1$, where f^* is defined in (8). If $\mathrm{lc}(f) = \mathrm{lc}(f^*)$ then return **Membership**$\Phi_1(f^*)$, otherwise return false.
   4.7. If f does not satisfy all the above conditions, then it satisfies the condition of Conjecture 4.15 and $f \in \Phi_1$ assuming the conjecture is valid.

In the rest of this section, we will give the details for Algorithm 1 and prove its correctness. We will use algorithms for real root isolation and complex root isolation for univariate polynomials. Please refer to the latest work on these topics and references in these papers [1],[14].

Step 1 is trivial to check. Steps 2 and 3 can be done with any real root isolation algorithm.

Step 4.1 is trivial. For Step 4.2, there exists a $\delta \in \mathbb{N}$ such that $(z)^\delta = 1$ if and only if each irreducible factor of $f(x)$ is a cyclotomic polynomial, which can be checked with the Graeffe method in [2] and the δ can also be found. The polynomial f^* in Step 4.2 can be computed with Corollary 4.7. Step 4.3 follows from Lemma 4.14.

For Steps 4.4-4.6, we first have the following simple fact:

Lemma 4.16. *Let $p(x) = a\prod_{i=1}^{n}(x-x_i) \in \mathbb{Z}[x]$, $q(x) = b\prod_{j=1}^{m}(x-y_j) \in \mathbb{Z}[x]$, and $x_i y_j \neq 0$ for all i, j. Then the roots of $R_u(p(u), q(ux))$ are $\{y_j/x_i \mid i = 1, \cdots, n, j = 1, \cdots, m\}$ and the roots of $R_u(u^n p(x/u), q(u))$ are $\{x_i y_j \mid i = 1, \cdots, n, j = 1, \cdots, m\}$.*

In the rest of this section, we assume

$$f \quad = \quad f_0 \prod_{i=1}^{t} f_i^{e_i}, \quad r_i(x) = R_u(u^n f_i(x/u), f_i(u)) \qquad (9)$$

where f_i are primitive and irreducible polynomials with positive leading coefficients. Also assume that $f(x)$ has a unique positive root x_+ which is the root of $f_0(x)$.

By Lemma 4.16, the real roots of all $r_i(x)$ include x_+^2 and $z\bar{z}$, where z is a complex root of $f_i(x)$. Then the condition in Step 4.4 can be checked with the following result.

Corollary 4.17. *f has a root z such that $|z| > x_+$ if and only if some $r_i(x)$ has a positive root larger than x_+^2.*

If z is complex root of f_i such that $|z| = x_+$, then $x_+^2, x_+^2 = z \cdot \bar{z}, x_+^2 = \bar{z} \cdot z$ are all roots of r_i by Lemma 4.16. Then, we have

Corollary 4.18. *Let m_i be the multiplicity of x_+^2 as a root of r_i and n_i the multiplicity of $-x_+$ as a root of f_i (the multiplicity is set to be zero if x_+^2 or $-x_+$ is not a root). Then $\#\{z \mid f_0(z) = 0, |z| = x_+, z \notin \mathbb{R}\} = m_0 - n_0 - 1$ and $\#\{z \mid f_i(z) = 0, |z| = x_+, z \notin \mathbb{R}\} = m_i - n_i$ for $i > 0$.*

As usual, a *representation* of a complex root z is a pair (p, B) where p is an irreducible polynomial and B a box such that $p(z) = 0$ and z is the only root of p in B. A box is represented by its lower-left and upper-right vertices: $([x_l, y_l], [x_t, x_t])$.

Lemma 4.19. *Suppose f_i has s roots $z_1, \ldots, z_s$ satisfying $|z_j| = x_+$. Then, we can find representations for z_j.*

Proof: We can simultaneously refine the isolation interval $I = (a, b)$ of x_+ and the isolation boxes B_i of the roots of f_i such that the number of B_i meeting the region $a < |z| < b$ will eventually becomes s. These s boxes are the isolation boxes for $z_1, \ldots, z_s$, since f_i has exactly s such roots.

Lemma 4.20. *Let z be a root of f_k satisfying $|z| = x_+$. Then, we can find a representation for z/x_+.*

Proof: Let $H(x) = R_u(f_0(u), f_k(ux)) \in \mathbb{Z}[x]$ and $h_i(x), i = 1, \ldots, s$ the irreducible factors of H. From Lemma 4.16, $H(z/x_+) = 0$. Isolate the roots of $h_i, i = 1, \ldots, s$ and refine the isolation box $B = ([x_l, y_l], [x_t, x_t])$ of z and the isolation interval (l, r) of x_+ such that $([x_l/r, y_l/r], [x_t/l, x_t/l])$ intersects only one of the isolation boxes of $h_i, i = 1, \ldots, s$, which is the isolation box for z/x_+.

With the Graeffe method in [2], we have

Lemma 4.21. *Let z be a root of f_k satisfying $|z| = x_+$ and q the minimal polynomial for z/x_+. Then we can decide whether there exists an $m \in \mathbb{N}$ such that $(z/x_+)^m = 1$, and if such an m exists, we can compute the minimal m.*

Now, we consider Step 4.5. With Corollary 4.18 and Lemma 4.19, we can find all the roots z of f satisfying $|z| = x_+$. For each z, we can check whether there exists a δ_z such that $(z/x_+)^{\delta_z} = 1$ with Lemmas 4.20 and 4.21. Hence the conditions of Step 4.5 can be checked.

Now, we consider Step 4.6. For each root z of f satisfying $|z| = x_+$, we can find a minimal δ_z such that $(z/x_+)^{\delta_z} = 1$ with Lemma 4.21. Then $\delta = \mathrm{lcm}\{\delta_z \mid f(z) = 0, |z| = x_+, (z/x_+)^{\delta_z} = 1\}$. Now f^* can be computed with (8). From Corollary 4.7, the roots of f^* are $\{z^\delta \mid f(z) = 0\}$. Then, when running **Membership**$\Phi_1(f^*)$, only Steps 1, 3, 4.7 will be executed and no recursive calls are needed.

4.3 Compute the finite σ-Gröbner basis

Let $f \in \Phi_1$, we will show how to compute the finite σ-Gröbner basis for $\mathcal{I}_f = \mathrm{sat}(\mathbb{P}_f)$ in (2).

Lemma 4.22. *Let $f \in \Phi_1$, $h = fg \in \Phi_0$ for a monic $g \in \mathbb{Z}[x]$, and $D = \deg(h)$. Then*

$$\mathcal{I}_D \quad = \quad \mathrm{sat}(\mathbb{P}_f) \bigcap \mathcal{F}[y, y^x, \cdots, y^{x^D}]$$

$$= \quad \mathrm{asat}(\mathbb{P}_f, \mathbb{P}_{xf}, \ldots, \mathbb{P}_{x^{D-\deg(f)}f}) \tag{10}$$

and a Gröbner basis of $\mathcal{I}_D$ is a σ-Gröbner basis of $\mathcal{I}_f$.

Proof: By the remark before Theorem 2.6, $\mathbb{P}_f$ is regular and coherent. Then $P \in \mathcal{I}_D$ if and only if $\mathrm{prem}(P, \mathbb{P}_f) = 0$ which is equivalent to $P \in \mathrm{asat}(\mathbb{P}_f, \mathbb{P}_{xf}, \ldots, \mathbb{P}_{x^{D-\deg(f)}f})$ [6], and (10) is proved. By Corollary 3.4, a Gröbner basis of $\mathcal{I}_D$ is a σ-Gröbner basis of $\mathcal{I}_f$.

The Gröbner basis of $\mathcal{I}_D$, denoted as $\mathbb{G}(f, D)$, can be computed with the following well-known fact about quotients of ideals

$$\mathrm{asat}(\mathbb{P}_f, \mathbb{P}_{xf}, \ldots, \mathbb{P}_{x^{D-\deg(f)}f}) = (z \cdot y^{\sum_{i=0}^{D-\deg(f)} x^i} - 1,$$
$$\mathbb{P}_f, \mathbb{P}_{xf}, \ldots, \mathbb{P}_{x^{D-\deg(f)}f}) \cap \mathcal{F}[y, y^x, \cdots, y^{x^D}],$$

where $I = \mathrm{init}(\mathbb{P}_f)$ and z is a new indeterminate. Therefore, in order to compute the σ-Gröbner basis of $\mathcal{I}_f$, it suffices to compute D. We thus have the following algorithm.

Algorithm 2 — FiniteGB (f)

Input: $f \in \Phi_1$ such that $f(0) \neq 0$.
Output: Return σ-Gröbner basis of $\mathcal{I}_f = \mathrm{sat}(\mathbb{P}_f)$.

1. If $\mathrm{lt}(f) = f^+$, then return $\{\mathbb{P}_f\}$.
2. If f has no positive real roots, then return $\mathbb{G}(f, N_f + \deg(f)+1)$, where N_f is defined in Lemma 3.13.
3. Let x_+ be the unique simple positive real root of f.

3.1. If $x_+ = 1$ and every root z of f satisfies $z^\delta = 1$ for some $\delta \in \mathbb{N}$, then return $\mathbb{G}(f, \delta)$.

3.2. If $x_+ = 1$ and any other root z of f satisfies $|z| < 1$, then return $\mathbb{G}(f, \deg(f) + \delta - 1)$, where δ is found in Step 4.3 of Algorithm 1.

3.3. Let δ be the minimal integer such that $f(z) = 0$, $z \neq x_+$, and $|z| = x_+$ imply $(\frac{z}{x_+})^\delta = 1$. Let the f^* be defined in (8). Return $\mathbb{G}(f, \delta\deg(f^*))$.

In the rest of this section, we will prove the correctness of Algorithm 2. Step 1 follows Lemma 3.2.

For Step 2, by Lemma 3.13, $(x+1)^{N_f} f \in \mathbb{Z}^{>0}[x]$. Following the proof of Lemma 3.5, for a sufficiently large $M \in \mathbb{N}$, $(x-M)(x+1)^{N_f} f \in \Phi_0$. Then, $D = \deg((x-M)(x+1)^{N_f} f) = N_f + \deg(f) + 1$.

For Step 3.1, following Step 4.2 of Algorithm 1, we have $f^*(x^\delta) = f(x)g(x) = x^\delta - 1$ for some g. Then $D = \delta$. For Step 3.2, following Step 4.3 of Algorithm 1, $f(x)(x^\delta - 1)/(x-1) \in \Phi_0$. Then $D = \deg(f) + \delta - 1$.

For Step 3.3, from the proof of Step 4.6 of Algorithm 1, there exist three possibilities: $f^*(x) \in \Phi_0$, $f^*(x)$ has at least two positive roots, or f^* satisfies the conditions of Conjecture 4.15. Since we already assumed $f^* \in \Phi_1$, only one case is possible: $f^*(x) \in \Phi_0$. Since $f^*(x^\delta) = f(x)s(x) \in \Phi_0$, we have $D = \delta\deg(f)$. We have now proved the correctness of Algorithm 2.

5 CONCLUSION

In this paper, we study when a σ-ideal has a finite σ-Gröbner basis. We focused on a special class of σ-ideals: normal binomial σ-ideals which can be be described by the Gröbner basis of a $\mathbb{Z}[x]$-module. We give a criterion for a univariate normal binomial σ-ideal to have a finite σ-Gröbner basis. When the characteristic set of the σ-ideal consists of one σ-polynomial, we can give a constructive criteria for the σ-ideal to have a finite σ-Gröbner basis and an algorithm to compute the finite σ-Gröbner basis under these criteria. One case is still not solved and we summarize it as a conjecture. Also, it is desirable to extend the criteria given in this paper to the multivariate case.

REFERENCES

[1] Ruben Becker, Michael Sagraloff, Vikram Sharma, Juan Xu, and Chee Yap. 2016. Complexity analysis of root clustering for a complex polynomial. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*. ACM, 71–78.

[2] Russell J Bradford and James H Davenport. 1988. Effective tests for cyclotomic polynomials. In *International Symposium on Symbolic and Algebraic Computation*. Springer, 244–251.

[3] Richard-M Cohn. 1967. Difference algebra. (1967).

[4] David Eisenbud and Bernd Sturmfels. 1996. Binomial ideals. *Duke Mathematical Journal* 84, 1 (1996), 1–45.

[5] Xiao-Shan Gao, Zhang Huang, Jie Wang, and Chun-Ming Yuan. 2017. Toric Difference Variety. *Journal of Systems Science and Complexity* 30, 1 (2017), 173–195.

[6] Xiao-Shan Gao, Zhang Huang, and Chun-Ming Yuan. 2017. Binomial difference ideals. *Journal of Symbolic Computation* 80 (2017), 665–706.

[7] Xiao-Shan Gao, Yong Luo, and Chun-Ming Yuan. 2009. A characteristic set method for ordinary difference polynomial systems. *Journal of Symbolic Computation* 44, 3 (2009), 242–260.

[8] Vladimir P Gerdt. 2012. Consistency analysis of finite difference approximations to PDE systems. In *Mathematical Modeling and Computational Science*. Springer, 28–42.

[9] Vladimir P Gerdt and Daniel Robertz. 2012. Computation of difference Gröbner bases. *Comput. Sci. J. Mold.* 20 (2012), 203–226.

[10] Kei-ichiro Iima and Yuji Yoshino. 2009. Gröbner bases for the polynomial ring with infinite variables and their applications. *Communications in Algebra* 37, 10 (2009), 3424–3437.

[11] Viktor Levandovskyy and Bernd Martin. 2012. A Symbolic Approach to Generation and Analysis of Finite Difference Schemes of Partial Differential Equations. *Numerical and Symbolic Scientific Computing* (2012), 123–156.

[12] Alexander Levin. 2008. *Difference algebra*. Vol. 8. Springer Science & Business Media.

[13] Victoria Powers and Thorsten Wörmann. 1998. An algorithm for sums of squares of real polynomials. *Journal of pure and applied algebra* 127, 1 (1998), 99–104.

[14] Vikram Sharma and Chee K Yap. 2012. Near optimal tree size bounds on a simple real root isolation algorithm. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*. ACM, 319–326.

[15] Michael Wibmer. 2013. Algebraic difference equations. *Preprint* (2013).