A Polynomial-time Algorithm to Compute Generalized Hermite Normal Form of Matrices over $\mathbb{Z}[x]$

Rui-Juan Jing, Chun-Ming Yuan, Xiao-Shan Gao
KLMM, Academy of Mathematics and Systems Science
Chinese Academy of Sciences, Beijing 100190, China
rjing@amss.ac.cn, {cmyuan,xgao}@mmrc.iss.ac.cn

Abstract

In this paper, a polynomial-time algorithm is given to compute the generalized Hermite normal form for a matrix F over $\mathbb{Z}[x]$, or equivalently, the reduced Gröbner basis of the $\mathbb{Z}[x]$-module generated by the column vectors of F. The algorithm is also shown to be practically more efficient than existing algorithms. The algorithm is based on three key ingredients. First, an F4 style algorithm to compute the Gröbner basis is adopted, where a novel prolongation is designed such that the coefficient matrices under consideration have polynomial sizes. Second, fast algorithms to compute Hermite normal forms of matrices over $\mathbb{Z}$ are used. Third, the complexity of the algorithm are guaranteed by a nice estimation for the degree and height bounds of the polynomials in the generalized Hermite normal form.

Keywords: $\mathbb{Z}[x]$ module, Gröbner basis, generalized Hermite normal form, Hermite normal form, polynomial-time algorithm.

1 Introduction

The Hermite normal form (abbr. HNF) is a standard representation for matrices over principal ideal domain(abbr. PID) such as $\mathbb{Z}$ and $\mathbb{Q}[x]$, which has a wide range of applications [4]. In this paper, generalized Hermite normal form (abbr. GHNF) for matrices over $\mathbb{Z}[x]$ are studied. This is motivated by the recent work on Laurent binomial difference ideals and toric difference varieties [11], where properties of Laurent binomial difference ideals and toric difference varieties are reduced to that of GHNFs for matrices over $\mathbb{Z}[x]$.

Note that $\mathbb{Z}[x]$ is not a PID and a matrix over $\mathbb{Z}[x]$ cannot be reduced to an HNF in the general case. In [11], the concept of GHNF is introduced and it is shown that any matrix over $\mathbb{Z}[x]$ can be reduced to a GHNF. Furthermore, it is shown that a matrix $F = [\mathbf{f}_1, \ldots, \mathbf{f}_s] \in \mathbb{Z}[x]^{n\times s}$ is a GHNF if and only if its columns $\mathbb{f} = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$ form a reduced Gröbner basis of the $\mathbb{Z}[x]$-module generated by $\mathbb{f}$ in $\mathbb{Z}[x]^n$ under certain monomial order. Similar to the concept of lattice [4], a $\mathbb{Z}[x]$-module in $\mathbb{Z}[x]^n$ is called a $\mathbb{Z}[x]$-lattice which plays the same role as lattice does in the study of toric varieties [6]. Therefore, computing the GHNF of matrices over $\mathbb{Z}[x]$ is equivalent to computing the reduced Gröbner basis for a $\mathbb{Z}[x]$-lattice, which can be done with the Gröbner basis methods for modules over rings [5, 14].

The main contribution of this paper is to give an algorithm to compute the GHNF of a matrix $F \in \mathbb{Z}[x]^{n\times s}$ or the reduced Gröbner basis of the $\mathbb{Z}[x]$-lattice generated by the column vectors of F, which is both practically efficient and has polynomial bit computational complexity. Note that the complexity of computing Gröbner bases in $\mathbb{Q}[x_1, \ldots, x_n]$ is double exponential [17]. As far as we know, there is no study on the complexity of Gröbner bases computation for $\mathbb{Z}[x]$-modules in $\mathbb{Z}[x]^n$. The algorithm consists of three main ingredients which will be explained below.

The first ingredient comes from the powerful idea in Faugère's F4 algorithm [10] and the XL algorithm [7] to compute Gröbner bases. To compute the Gröbner basis of the ideal generated by $p_1, \ldots, p_m \in \mathbb{Q}[x_1, \ldots, x_n]$,

these algorithms apply efficient elimination algorithms from linear algebra to the coefficient matrix of $x_j^k p_i$ for certain k. Although the F4 algorithm can not improve the worst case complexity, it is generally faster than the classical Buchberger algorithm [3]. In this paper, to compute the GHNF of $F = [\mathbf{f}_1, \ldots, \mathbf{f}_s] \in \mathbb{Z}[x]^{n\times s}$ with columns $\mathbf{f}_i$, due to the special structure of the Gröbner bases in $\mathbb{Z}[x]$, we design a novel method to do certain prolongations $x^k\mathbf{f}_i$ such that the sizes of the coefficient matrices of all those $x^j\mathbf{f}_i$ under consideration are bounded by a polynomial in n and d, where d is the degree of the polynomials in F.

The second ingredient is to use efficient algorithms to compute the HNF for matrices over $\mathbb{Z}$. The computationally dominant step of our algorithm is to compute the HNF of the coefficient matrix of those prolongations $x^j\mathbf{f}_i$ obtained in the first ingredient. Due to its importance, HNF computation is extensively studied and there exist many efficient algorithms to compute HNFs for matrices over $\mathbb{Z}$ [4, 15, 19, 20] and matrices over $\mathbb{Q}[x]$ [2, 8, 13, 18]. Note that it is difficult to recover the GHNF for a matrix over $\mathbb{Z}[x]$ from its HNF over $\mathbb{Q}[x]$. In the complexity analysis, we use the HNF algorithm with the best bit complexity bound [19].

The third ingredient is a nice estimation for the degree and height bounds of the polynomials in the GHNF $G \in \mathbb{Z}[x]^{n\times s}$ of $F \in \mathbb{Z}[x]^{n\times m}$. We show that the degrees and the heights of the key elements of G are bounded by nd and $6n^3d^2(h+1+\log(n^2d))$, respectively, where d and h are the maximal degree and maximal height of the polynomials in F, respectively. Furthermore, we show that $G = FU$ for a matrix $U \in \mathbb{Z}[x]^{m\times s}$ and the degrees of the polynomials in U are bounded by a polynomial in n, d, h. These polynomial bounds along already lead to a polynomial-time algorithm to compute the GHNF. But, in order to have an algorithm which is both polynomial-time and practically efficient, the first two ingredients are needed. The bounds about the GHNF are obtained based on powerful methods introduced by Aschenbrenner in [1], where the first double exponential algorithm for the ideal membership problem in $\mathbb{Z}[x_1, \ldots, x_n]$ is given. The key to the bound estimation for GHNF is to find solutions to linear equations over $\mathbb{Z}[x]$, whose degree and height are bounded. Due to the special structure of the Gröbner basis in $\mathbb{Z}[x]$, we can give better bounds than [1] for this problem.

The algorithm is implemented in Magma and Maple and their default HNF commands are used in our implementation. In the case of $\mathbb{Z}[x]$, our algorithm is shown to be more efficient than the Gröbner basis algorithm in Magma and Maple, which are also based on HNF. In the general case, the proposed algorithm is also very efficient in practice that quite large problems can be solved.

The rest of this paper is organized as follows. In Section 2, we introduce several notations of Gröbner bases for $\mathbb{Z}[x]$ lattices. In Section 3, we give degree and height bounds for the GHNF. In Section 4, we give the algorithm to compute the GHNFs. Experimental results are shown in Section 5. Finally, conclusions are presented in Section 6.

2 Preliminaries

In this section, some basic notations and properties about reduced Gröbner bases for $\mathbb{Z}[x]$ lattices will be given. For more details, please refer to [1, 5, 11, 14, 16].

For brevity, a $\mathbb{Z}[x]$ module in $\mathbb{Z}[x]^n$ is called a $\mathbb{Z}[x]$ *lattice*. Any $\mathbb{Z}[x]$ lattice L has a finite set of generators $\{\mathbf{f}_1, \ldots, \mathbf{f}_s\} \subseteq \mathbb{Z}[x]^n$ and this fact is denoted as

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

If $\mathbf{f}_i = [f_{1,i}, \ldots, f_{n,i}]^\tau$, then we call $M = [f_{i,j}]_{n\times s}$ a *polynomial matrix* of $L = (\mathbf{f}_1, \ldots, \mathbf{f}_s)$ or the sequence $\mathbf{f}_1, \ldots, \mathbf{f}_s$. Note that $\mathbf{f}_i$ is the i-th column of M. For convenience, we also write $M = [\mathbf{f}_1, \ldots, \mathbf{f}_s]$. If $n = 1$, M is called the *polynomial vector* of $(\mathbf{f}_1, \ldots, \mathbf{f}_s)$ or $\mathbf{f}_1, \ldots, \mathbf{f}_s$.

A monomial $\mathbf{m}$ in $\mathbb{Z}[x]^n$ is an element of the form $x^k\mathbf{e}_i \in \mathbb{Z}[x]^n$, where $k \in \mathbb{N}$, and $\mathbf{e}_i$ is the canonical i-th unit vector in $\mathbb{Z}[x]^n$. A term $\mathbf{m}$ in $\mathbb{Z}[x]^n$ is a multiplication of an integer $a \in \mathbb{Z}$ and a monomial $\mathbf{m}$, that is $a\mathbf{m}$.

The admissible order $\prec$ on monomials in $\mathbb{Z}[x]^n$ can be defined naturally: $x^\alpha \mathbf{e}_i \prec x^\beta \mathbf{e}_j$ if

$$\begin{cases} i < j, \text{ or} \\ i = j \text{ and } \alpha < \beta \end{cases} \tag{1}$$

The order $\prec$ can be naturally extended to terms: $ax^\alpha \mathbf{e}_i \prec bx^\beta \mathbf{e}_j$ if and only if $x^\alpha \mathbf{e}_i \prec x^\beta \mathbf{e}_j$ or $i = j,\ \alpha = \beta$ and $|a| < |b|$.

With the admissible order $\prec$ defined by (1), $\mathbf{f} \in \mathbb{Z}[x]^n$ can be written in a unique way as a $\mathbb{Z}$-linear combination of monomials,

$$\mathbf{f} = \textstyle\sum_{i=1}^{s} c_i \mathbf{m}_i,$$

where $c_i \neq 0$ and $\mathbf{m}_1 \prec \mathbf{m}_2 \prec \cdots \prec \mathbf{m}_s$. We define the *leading coefficient, leading monomial,* and *leading term* of $\mathbf{f}$ as $\mathbf{LC}(\mathbf{f}) = c_s$, $\mathbf{LM}(\mathbf{f}) = \mathbf{m}_s$, and $\mathbf{LT}(\mathbf{f}) = c_s\mathbf{m}_s$, respectively.

The order $\prec$ can be extended to elements of $\mathbb{Z}[x]^n$ in a natural way: for $\mathbf{f},\mathbf{g} \in \mathbb{Z}[x]^n, \mathbf{f} \prec \mathbf{g}$ if and only if $\mathbf{LT}(\mathbf{f}) \prec \mathbf{LT}(\mathbf{g})$. We will use the order $\prec$ throughout this paper.

For two terms $ax^\alpha \mathbf{e}_i$ and $bx^\beta \mathbf{e}_j$ in $\mathbb{Z}[x]^n$, if $i = j,\ \alpha \geq \beta$ and $|a| \geq |b|$, let $a = qb + r$, where $0 \leq r < |b|$. Then $rx^\alpha \mathbf{e}_i = (ax^\alpha - qx^{\alpha-\beta} \times bx^\beta)\mathbf{e}_i$ is said to be *reduced with respect to* $bx^\beta \mathbf{e}_j$ or $\{bx^\beta \mathbf{e}_j\}$*-reduced*, denoted by $rx^\alpha \mathbf{e}_i = \overline{ax^\alpha \mathbf{e}_i}^{bx^\beta \mathbf{e}_j}$. The quotient is $qx^{\alpha-\beta}$. Otherwise, $ax^\alpha \mathbf{e}_i$ is $\{bx^\beta \mathbf{e}_j\}$-reduced, and in this case we denote $ax^\alpha \mathbf{e}_i = \overline{ax^\alpha \mathbf{e}_i}^{bx^\beta \mathbf{e}_j}$ and the quotient is zero. We use $(\overline{ax^\alpha \mathbf{e}_i}^{bx^\beta \mathbf{e}_j}, qx^{\alpha-\beta}) = \text{Reduce}(ax^\alpha \mathbf{e}_i, bx^\beta \mathbf{e}_j)$ to denote this procedure.

This concept can be extended to the elements in $\mathbb{Z}[x]^n$: for any $\mathbf{f} \in \mathbb{Z}[x]^n$ and $\mathbf{g} \in \mathbb{Z}[x]^n$, let $\mathbf{h} = \mathbf{f},\ q = 0$. While there exists a term $\mathbf{m}$ of $\mathbf{h}$ which is not $\{\mathbf{LT}(\mathbf{g})\}$-reduced, let q_1 be the quotient of $\mathbf{m}$ reduced by $\mathbf{LT}(\mathbf{g})$, $\mathbf{h} = \mathbf{h} - q_1\mathbf{g},\ q = q + q_1$. This procedure will terminate in finite steps by the well-ordering given before. When the above procedure ends, $\mathbf{h}$ is $\{\mathbf{g}\}$-reduced and is denoted by $\mathbf{h} = \overline{\mathbf{f}}^{\mathbf{g}}$ and q is the corresponding quotient, denoted by $(\mathbf{h}, q) = \text{Reduce}(\mathbf{f}, \mathbf{g})$. Note that $\mathbf{h}$ and q satisfy $\mathbf{h} = \mathbf{f} - q\mathbf{g}$. Moreover, for $\mathbf{f} \in \mathbb{Z}[x]^n$ and $G = [\mathbf{g}_1, \ldots, \mathbf{g}_m] \in \mathbb{Z}[x]^{n\times m}$ with $\mathbf{g}_1 \prec \ldots \prec \mathbf{g}_m$, let $\mathbf{h}_{m+1} = \mathbf{f}$ and for $i = m, m-1, \ldots, 1$, set

$$(\mathbf{h}_i, u_i) = \text{Reduce}(\mathbf{h}_{i+1}, \mathbf{g}_i).$$

Denote $(\mathbf{h}, U) = \text{Reduce}(\mathbf{f}, G)$, where $\mathbf{h} = \mathbf{h}_1 = \overline{\mathbf{f}}^G$ and $U = [u_1, \ldots, u_m]^\tau$ the corresponding quotient vector. Then $\mathbf{h} = \mathbf{f} - GU$.

For $F = [\mathbf{f}_1, \ldots, \mathbf{f}_{m_1}] \in \mathbb{Z}[x]^{n\times m_1}, G = [\mathbf{g}_1, \ldots, \mathbf{g}_{m_2}] \in \mathbb{Z}[x]^{n\times m_2}$ with $\mathbf{g}_1 \prec \ldots \prec \mathbf{g}_{m_2}$, let $[\mathbf{h}_i, U_i] = \text{Reduce}(\mathbf{f}_i, G), i = 1, \ldots, m_1$. Then define $H = \overline{F}^G = [\mathbf{h}_1, \ldots, \mathbf{h}_{m_1}]$ and $[H, U] = \text{Reduce}(F, G)$, where $U = [U_1, \ldots, U_{m_1}] \in \mathbb{Z}[x]^{m_2\times m_1}$. We have $H = F - GU$.

Definition 2.1. *Let* $\mathbf{f},\mathbf{g} \in \mathbb{Z}[x]^n,\ \mathbf{LT}(\mathbf{f}) = ax^k\mathbf{e}_i,\ \mathbf{LT}(\mathbf{g}) = bx^s\mathbf{e}_j,\ s \leq k$. *Then the S-vector of* $\mathbf{f}$ *and* $\mathbf{g}$ *is defined as follows: if* $i \neq j$ *then* $S(\mathbf{f},\mathbf{g}) = \mathbf{0}$*; otherwise*

$$\begin{cases} \mathbf{f} - \frac{a}{b}x^{k-s}\mathbf{g}, & \text{if } b|a; \\ \frac{b}{a}\mathbf{f} - x^{k-s}\mathbf{g}, & \text{if } a|b; \\ u\mathbf{f} + vx^{k-s}\mathbf{g}, & \text{if } a \nmid b \text{ and } b \nmid a, \text{ where } \gcd(a,b) = ua + vb. \end{cases} \tag{2}$$

If $n = 1$*, the S-vector can also be called S-polynomial, which is the same with the definition in [14].*

Definition 2.2. *A finite set* $G \subseteq \mathbb{Z}[x]^n$ *is called a Gröbner basis for the* $\mathbb{Z}[x]$ *lattice* L *generated by* G *if for any* $\mathbf{f} \in L$*, there exists* $\mathbf{g} \in G$*, such that* $\mathbf{LT}(\mathbf{g})|\mathbf{LT}(\mathbf{f})$*. A Gröbner basis* G *is called reduced if for any* $\mathbf{g} \in G,\ \mathbf{g}$ *is* $G \setminus \{\mathbf{g}\}$*-reduced. A Gröbner basis* G *is called minimal if for any* $\mathbf{g} \in G,\ \mathbf{LT}(g)$ *is* $G \setminus \{\mathbf{g}\}$*-reduced. By Theorem 3.5 of [11],* G *is a Gröbner basis if and only if* $\overline{S(\mathbf{f},\mathbf{g})}^G = \mathbf{0}$ *for all* $\mathbf{f},\mathbf{g} \in G$*.*

Clearly, a reduced Gröbner basis must be a minimal one. We can obtain the reduced Gröbner basis from a minimal one by reducing the non-leading terms of every element in it with every other element.

Gröbner bases in this paper are assumed to be ranked in an increasing order with respect to the admissible order $\prec$. That is, if $G = \{\mathbf{g}_1, \ldots, \mathbf{g}_s\}$ is a Gröbner basis, then $\mathbf{g}_1 \prec \ldots \prec \mathbf{g}_s$.

We first consider Gröbner bases in $\mathbb{Z}[x]$. The following proposition shows the properties of the reduce Gröbner basis of ideals in $\mathbb{Z}[x]$.

Proposition 2.3 ([11]). *Let $B = \{b_1, \ldots, b_k\}$ be the reduced Gröbner basis of a $\mathbb{Z}[x]$ module in $\mathbb{Z}[x]$, $b_1 \prec \cdots \prec b_k$, and $\mathbf{LT}(b_i) = c_i x^{d_i} \in \mathbb{N}[x]$. Then*

1. $0 \leq d_1 < \cdots < d_k$.
2. $c_k | \cdots | c_1$ *and* $c_i \neq c_{i+1}$ *for* $1 \leq i \leq k-1$.
3. $\frac{c_i}{c_k} | b_i$ *for* $1 \leq i < k$. *Moreover if* $\widetilde{b_1}$ *is the primitive part of* b_1, *then* $\widetilde{b_1} | b_i$, *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.

This proposition also applies to the minimal Gröbner bases. Here are three Gröbner bases in $\mathbb{Z}[x]$: $\{2, x\}$, $\{12, 6x+6, 3x^2+3x, x^3+x^2\}$, $\{9x+3, 3x^2+4x+1\}$.

Now, we give a refined description of Gröbner bases for ideals in $\mathbb{Z}[x]$. For a polynomial set $F = \{f_1, \ldots, f_m\}$ in $\mathbb{Z}[x]$, we denote by $\mathrm{Content}(F)$ the GCD of the contents of f_i as a polynomial in x, $\mathrm{Primpart}(F) = \gcd(F)/\mathrm{Content}(F)$ the primitive part of F.

The following proposition is mentioned in [16]. Now we give a simple proof for it which help us to understand the structure of the Gröbner bases of ideals in $\mathbb{Z}[x]$.

Proposition 2.4 ([16]). *$G = \{g_1, \ldots, g_n\}$ with $\deg(g_1) < \cdots < \deg(g_n)$ is the minimal Gröbner basis of $(f_1, \ldots, f_m)$ in $\mathbb{Z}[x]$ if and only if*

$$\begin{aligned} &g_1 = a b_1 \ldots b_{n-1} \tilde{g}_1, \quad g_n = a h_n \tilde{g}_1, \\ &g_i = a b_i \ldots b_{n-1} h_i \tilde{g}_1, 2 \leq i \leq n-1 \end{aligned} \tag{3}$$

such that

i) $a = \mathrm{Content}(f_1, \ldots, f_m)$;

ii) $\tilde{g}_1 = \mathrm{Primpart}(f_1, \ldots, f_m)$;

iii) $h_i \in \mathbb{Z}[x]$ *is monic with degree* d_i, *and* $0 < d_2 < \cdots < d_n$;

iv) $b_i \in \mathbb{Z}, b_i \neq \pm 1$, *and* $h_{i+1} \in (h_i, b_{i-1} h_{i-1}, \ldots, b_2 \ldots b_{i-1} h_2, b_1 \ldots b_{i-1})$, *for* $1 \leq i \leq n-1$, *where* $h_1 = 1$.

Proof. By Proposition 2.3, if $G = \{g_1, \ldots, g_n\}$ is a minimal Gröbner basis, we can write G as:

$$\{a c_1 \tilde{g}, a t_2 \tilde{g}, \ldots, a t_{n-1} \tilde{g}, a t_n \tilde{g}\},$$

where $a = \mathrm{Content}(g_1, \ldots, g_n) \in \mathbb{Z}$, $\tilde{g} = \mathrm{Primpart}(g_1, \ldots, g_n) \in \mathbb{Z}[x]$,

$$t_i = c_i x^{d_i} + q_{i,d_i-1} x^{d_i-1} + \cdots + q_{i1} x + q_{i0} \in \mathbb{Z}[x], \ 2 \leq i \leq n$$

with $c_{n-1} | c_{n-2} | \ldots | c_2 | c_1$ and $0 < d_2 < d_3 < \cdots < d_n$. Since $\{f_1, \ldots, f_m\}$ and $\{g_1, \ldots, g_n\}$ are the $\mathbb{Z}[x]$ linear combinations of each other, they have the same content and primitive part. So, i) and ii) follow easily. Without loss of generality, we assume $a\tilde{g} = 1$ in the rest of the proof.

To prove iii), we claim $c_i|q_{ij}$ for $2 \le i \le n, 0 \le j \le d_i - 1$. We prove this claim by induction on n. If $n = 2$, $G = [c_1, t_2]$.

$$\begin{aligned} S(t_2, c_1) &= \frac{c_1}{c_2}(c_2 x^{d_2} + q_{2,d_2-1}x^{d_2-1} + \cdots + q_{21}x + q_{20}) - c_1 x^{d_2} \\ &= \frac{c_1}{c_2}q_{2,d_2-1}x^{d_2-1} + \cdots + \frac{c_1}{c_2}q_{21}x + \frac{c_1}{c_2}q_{20}. \end{aligned}$$

Since G is a Gröbner basis, $S(t_2, c_1)$ can be reduced to zero by c_1. So we obtain $c_2|q_{2j}$ for $0 \le j \le d_2 - 1$. Suppose the claim is valid for $n \le k-1$. For $n = k$ we have $G = \{c_1, t_2, \ldots, t_k\}$. Let

$$\begin{aligned} S(t_k, t_{k-1}) &= \frac{c_{k-1}}{c_k}(c_k x^{d_k} + q_{k,d_k-1}x^{d_k-1} + \cdots + q_{k0}) - x^{d_k-d_{k-1}}(c_{k-1}x^{d_{k-1}} + q_{k-1,d_{k-1}-1}x^{d_{k-1}-1} + \cdots + q_{k-1,0}) \\ &= (\frac{c_{k-1}}{c_k}q_{k,d_k-1} - q_{k-1,d_{k-1}-1})x^{d_k-1} + \cdots + (\frac{c_{k-1}}{c_k}q_{k,d_k-d_{k-1}} - q_{k-1,0})x^{d_k-d_{k-1}} + \\ &\quad \frac{c_{k-1}}{c_k}q_{k,d_k-d_{k-1}-1}x^{d_k-d_{k-1}-1} + \cdots + \frac{c_{k-1}}{c_k}q_{k,0}. \end{aligned}$$

Since $S(t_k, t_{k-1})$ can be reduced to zero by $\{c_1, t_2, \ldots, t_{k-1}\}$ and $c_k|c_{k-1}|\ldots|c_1$, c_{k-1} must divide the coefficient of every term of $S(t_k, t_{k-1})$. Considering $c_{k-1}|q_{k-1,j}$ for $0 \le j \le d_{k-1} - 1$, we can easily obtain $c_k|q_{k,j}$ for $0 \le j \le d_k - 1$. The claim is proved.

We can write G as $\{b_1 \ldots b_{n-1}, b_2 \ldots b_{n-1}h_2, \ldots, b_{n-1}h_{n-1}, h_n\}$, where $h_i = t_i/c_i$ is monic of degree d_i and $b_i = c_i/c_{i+1}$ for $1 \le i \le n-1$. Since G is minimal, we have $b_i \ne 1$ for $1 \le i \le n-1$. iii) is proved.

We prove iv) by induction on i. Since $h_1 = 1$, we have $h_2 \in (h_1) = \mathbb{Z}[x]$ and iv) is valid for $i = 1$. Suppose iv) is valid for $i < j$. $G = \{t_1, t_2, \ldots, t_n\}$, where $t_i = b_i \ldots b_{n-1}h_i$ for $1 \le i \le n-1$, $t_n = h_n$. $S(t_j, t_{j-1}) = b_{j-1} \ldots b_{n-1}(h_j - x^{d_j-d_{j-1}}h_{j-1})$. Since $S(t_j, t_{j-1})$ can be reduced to zero by

$$G = \{b_1 \ldots b_{n-1}, b_2 \ldots b_{n-1}h_2, \ldots, b_{j-1} \ldots b_{n-1}h_{j-1}\},$$

it is easy to see that

$$h_j \in (h_{j-1}, b_{j-2}h_{j-2}, \ldots, b_2 \ldots b_{j-2}h_2, b_1 \ldots b_{j-2}).$$

That is, if G is a minimal Gröebner basis, G satisfies all the above conditions.

To prove the other direction, let us assume that G has the above form and we take $G = \{c_1, c_2h_2, \ldots, c_{n-1}h_{n-1}, h_n\}$, where $c_i = b_i \ldots b_{n-1}$ for $i = 1, \ldots, n-1$. To prove G is a Gröbner basis, it suffices to prove that $S(c_jh_j, c_ih_i)$ can be reduced to zero by $\{c_1, c_2h_2, \ldots, c_{j-1}h_{j-1}\}$ for $1 \le i < j \le n$. Clearly, this is valid when $j = 2$. Suppose it is valid for $j < k$. Then $H = \{c_1, c_2h_2, \ldots, c_{k-1}h_{k-1}\}$ is a Gröbner basis for the $\mathbb{Z}[x]$ lattice (H). For any $i = 1, \ldots, k$, $S(c_kh_k, c_ih_i) = \frac{c_i}{c_k}c_kh_k - x^{d_k-d_i}c_ih_i = c_i(h_k - x^{d_k-d_i}h_i)$. Since $h_k \in (h_{k-1}, b_{k-2}h_{k-2}, \ldots, b_1 \ldots b_{k-2})$ and $c_{k-1}|c_i$,

$$S(c_kh_k, c_ih_i) \in (c_ih_{k-1}, c_ib_{k-2}h_{k-2}, \ldots, c_ib_1 \ldots b_{k-2}) \subseteq (c_1, c_2h_2, \ldots, c_{k-1}h_{k-1}).$$

So $S(c_kh_k, c_ih_i)$ can be reduced to zero by $\{c_1, c_2h_2, \ldots, c_{k-1}h_{k-1}\}$. Since $b_i \ne \pm 1$, for $1 \le i \le n-1$ and $\deg(h_2) < \cdots < \deg(h_n)$, G is also a minimal Gröbner basis. □

Next, we introduce the concept of generalized Hermite normal form. Let

$$\mathscr{C}=\begin{pmatrix} c_{11} & \dots & c_{1,l_1} & c_{1,l_1+1} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ c_{r_1,1} & \dots & c_{r_1,l_1} & c_{r_1,l_1+1} & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & c_{r_1+1,1} & \dots & c_{r_1+1,l_2} & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & c_{r_2,1} & \dots & c_{r_2,l_2} & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & 0 & \dots & 0 & c_{r_{t-1}+1,1} & \dots & c_{r_{t-1}+1,l_t} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & 0 & \dots & 0 & c_{r_t,1} & \dots & c_{r_t,l_t} \end{pmatrix}_{n\times m} \tag{4}$$

whose elements are in $\mathbb{Z}[x]$. It is clear that $n=r_t\le m$ and $m=\sum_{i=1}^{t} l_i$. We denote by $\mathbf{c}_k=\mathbf{c}_{r_i,j}$ to be the k-th column of the matrix $\mathscr{C}$, where $k=l_1+\cdots+l_{i-1}+j,\ 1\le j\le l_i$. Assume

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

Then the leading term of $\mathbf{c}_{r_i,j}$ is $c_{r_i,j,0}x^{d_{r_i,j}}\mathbf{e}_{r_i}$.

Definition 2.5. *The matrix $\mathscr{C}$ is called a generalized Hermite normal form (* GHNF *) if it satisfies the following conditions:*

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

2) $c_{r_i,l_i,0}|\dots|c_{r_i,2,0}|c_{r_i,1,0}$.

3) $S(\mathbf{c}_{r_i,j_1},\mathbf{c}_{r_i,j_2})=x^{d_{r_i,j_2}-d_{r_i,j_1}}\mathbf{c}_{r_i,j_1}-\dfrac{c_{r_i,j_1,0}}{c_{r_i,j_2,0}}\mathbf{c}_{r_i,j_2}$ *can be reduced to zero by the column vectors of the matrix for any* $1\le i\le t,\ 1\le j_1<j_2\le l_i$.

4) $\mathbf{c}_{r_i,j}$ *is reduced with respect to the column vectors of the matrix other than* $\mathbf{c}_{r_i,j}$, *for any* $1\le i\le t, 1\le j\le l_i$.

Theorem 2.6 ([11]). $\{\mathbf{f}_1,\dots,\mathbf{f}_s\}\subseteq\mathbb{Z}[x]^n$ *is a reduced Gröbner basis with order* $\prec$ *such that* $\mathbf{f}_1\prec\mathbf{f}_2\prec\dots\prec\mathbf{f}_s$ *if and only if the polynomial matrix* $[\mathbf{f}_1,\dots,\mathbf{f}_s]$ *is a* GHNF.

3 Degree and height bounds for the GHNF

In this section, we give the degree and height bounds for the GHNF.

Firstly, we give some notations which will be used in this section. Let $f\in R[x]$, where R is a subring of $\mathbb{C}$. Denote by $|f|$ the maximal absolute value of the coefficients of f. Let $\mathrm{height}(f)=\log|f|$, with $\mathrm{height}(0)=0$. For $F=\{f_1,\dots,f_m\}\subset R[x]$, let $\deg(F)=\max_{1\le i\le m}\deg(f_i)$ and $\mathrm{height}(F)=\max_{1\le i\le m}\mathrm{height}(f_i)$.

For a prime $p\in\mathbb{Z}$, let $\mathbb{Z}_{(p)}$ be the local ring of $\mathbb{Z}$ at (p). For $a=up^t\in\mathbb{Z}$ where u is a unit in $\mathbb{Z}_{(p)}$, let $v_p(a)=t$ be the p-adic valuation. Let $\widehat{\mathbb{Z}}_{(p)}$ be the completion [1, 9] of $\mathbb{Z}_{(p)}$ and $\widehat{\mathbb{Z}}_{(p)}[x]$ the polynomial ring with coefficients in $\widehat{\mathbb{Z}}_{(p)}$. Denote by $\widehat{\mathbb{Z}}_{(p)}\langle x\rangle$ the completion of $\widehat{\mathbb{Z}}_{(p)}[x]$.

3.1 Degree and height bounds in $\mathbb{Z}[x]$

In this section, we will give the degree and height bounds for several basic algorithms, such as gcd and GHNF, in $\mathbb{Z}[x]$. These results will be used to give degree and height bounds for the GHNF in $\mathbb{Z}[x]^n$.

Lemma 3.1. *Let k be a field, $f_1,\ldots,f_m \in k[x]$, and $d = \max_{1\le i\le m}\deg(f_i)$. Then there exist $g_1,\ldots,g_m \in k[x]$ with $\deg(g_i) < d$ for any i, satisfying $\gcd(f_1,\ldots,f_m) = f_1g_1+\cdots+f_mg_m$.*

Proof. The bound can be obtained easily by the extended Euclidean algorithm. □

In the following, we specialize $k = \mathbb{Q}$ and $k = \mathbb{Z}/p\mathbb{Z}$ in the above lemma, where p is a prime in $\mathbb{Z}$. The following lemma will be used to bound the height of the GHNF.

Lemma 3.2. *Suppose $f_1,\ldots,f_m \in \mathbb{Z}[x]$, $d = \max_{1\le i\le m}\deg(f_i)$. If $1 \in (f_1,\ldots,f_m)\mathbb{Q}[x]$, then $\delta = f_1g_1+\cdots+f_mg_m$ for some $g_1,\ldots,g_m \in \mathbb{Z}[x]$ with degree $< d$ and some $\delta \in \mathbb{Z}\setminus\{0\}$ with $\mathrm{height}(\delta) \le d(2h+\log(d+1))$, where $h = \mathrm{height}(f_1,\ldots,f_m)$.*

Proof. By Lemma 3.1, we have $1 = f_1u_1+\cdots+f_mu_m$, where $u_i \in \mathbb{Q}[x]$ of degree $< d$. Assume $f_i = a_{i0}+\cdots+a_{id}x^d$, $u_j = b_{j0}+\cdots+b_{j,d-1}x^{d-1}$. Then we have the matrix equation $Ab = [1,0,\ldots,0]^\tau$, where $A = [A_1,\ldots,A_m]$,

$$A_i = \begin{pmatrix} a_{i0} & & & \\ a_{i1} & a_{i0} & & \\ \vdots & & \ddots & \\ a_{i,d} & & & a_{i0} \\ & \ddots & & \vdots \\ & & & a_{i,d} \end{pmatrix}_{2d\times d} \tag{5}$$

for $i = 1,\ldots,m$, and $b = [b_{1,0},\ldots,b_{1,d-1},\ldots,b_{m,0},\ldots,b_{m,d-1}]^\tau \in \mathbb{Q}^{nd}$. Let $\mathrm{rank}(A) = t \le 2d$. By the Cramer's rule, δ can be bounded by the nonzero $t\times t$ minors of A. By the Hadamard's inequality, we have $0 < \delta \le ((d+1)a^2)^d$, where $a = \max_{i,j}|a_{ij}|$. So $\mathrm{height}(\delta) \le d(2h+\log(d+1))$. □

The following lemma is given by Gel'fond [12] and a simpler proof can be found in [22, p178].

Lemma 3.3. *Let P_1 and P_2 be two monic polynomials in $\mathbb{C}[x]$, such that $\deg(P_1)+\deg(P_2) = d$. Then $|P_1||P_2| \le (d+1)^{1/2}2^d|P_1P_2|$.*

The following lemma gives a height bound for the gcd in $\mathbb{Z}[x]$.

Lemma 3.4. *Let $f_1,\ldots,f_m \in \mathbb{Z}[x]$ and $g = \gcd(f_1,\ldots,f_m)$ in $\mathbb{Z}[x]$. Then the height of g is bounded by $\frac{1}{2}\log(d+1)+d\log 2+h$, where $d = \max_{1\le i\le m}\deg(f_i)$ and $h = \mathrm{height}(f_1,\ldots,f_m)$.*

Proof. Since $g = \gcd(f_1,\ldots,f_m)$ is in $\mathbb{Z}[x]$, for each $i = 1,\ldots,m$, there exists a $g_i \in \mathbb{Z}[x]$ such that $gg_i = f_i$. Let $g' = g/\mathbf{LC}(g)$ and $g_i' = g_i/\mathbf{LC}(g_i)$. Then $f_i' = f_i/\mathbf{LC}(f_i) = f_i/\mathbf{LC}(g)\mathbf{LC}(g_i)$ and $|f_i| = |f_i'||\mathbf{LC}(f_i)|$. Let $d_i = \deg(f_i)$. By Lemma 3.3, we have $|g'||g_i'| \le (d_i+1)^{1/2}2^{d_i}|f_i'|$ for each $1 \le i \le m$, where $d_i = \deg(f_i)$. Then $|g||g_i| = |\mathbf{LC}(g)\mathbf{LC}(g_i)||g'||g_i'| \le (d_i+1)^{1/2}2^{d_i}|\mathbf{LC}(g)\mathbf{LC}(g_i)||f_i'| = (d_i+1)^{1/2}2^{d_i}|f_i|$. We have

$$\begin{aligned} \mathrm{height}(g) &\le \mathrm{height}(g)+\mathrm{height}(g_i) \\ &\le \frac{1}{2}\log(d_i+1)+d_i\log 2+\mathrm{height}(f_i) \ \text{ for any } i \\ &\le \frac{1}{2}\log(d+1)+d\log 2+h. \end{aligned} \tag{6}$$

□

Remark 3.5. *In the proof of Lemma 3.4, by the equation (6), we have $\mathrm{height}(f_i/g) \le \frac{1}{2}\log(d+1)+d\log 2+h$ for any i.*

We now give the degree and height bounds for the GHNF in $\mathbb{Z}[x]$. Obviously, the degree bound of the GHNF in $\mathbb{Z}[x]$ is $d = \deg(F)$ by the procedure of the Gröbner basiscomputation.

Lemma 3.6. *For the polynomial vector $F = [f_1, \ldots, f_m]$ over $\mathbb{Z}[x]$, the degree of its* GHNF *can be bounded by $d = \deg(F)$.*

The height bound is given in the following lemma.

Lemma 3.7. *Let $f_1, \ldots, f_m \in \mathbb{Z}[x]$, $d = \max_{1\le i\le m} \deg(f_i)$, $h = \max_{1\le i\le m} \text{height}(f_i)$, and $[g_1, \ldots, g_s]$ the* GHNF *of $[f_1, \ldots, f_m]$. Then* $\text{height}(g_i) \le (2d+1)(h + d\log 2 + \log(d+1))$.

Proof. Let $\deg(g_1) \le \cdots \le \deg(g_s)$. By the properties of the GHNF, we have $\text{height}(g_1) = \max_{1\le i\le s} \text{height}(g_i)$. Let $g = \gcd(f_1, \ldots, f_m)$ in $\mathbb{Z}[x]$. By Lemma 3.4 and Remark 3.5, we have $\text{height}(g)$ and $\text{height}(f_i/g)$ both are $\le \frac{1}{2}\log(d+1) + d\log 2 + h$. Moreover, $1 \in (f_1/g, \ldots, f_m/g)\mathbb{Q}[x]$. By Lemma 3.2, $\text{height}(g_i/g) \le d(2(\frac{1}{2}\log(d+1) + d\log 2 + h) + \log(d+1)) = 2d(h + d\log 2 + \log(d+1))$. So, $\text{height}(g_i) \le 2d(h + d\log 2 + \log(d+1)) + \frac{1}{2}\log(d+1) + d\log 2 + h \le (2d+1)(h + d\log 2 + \log(d+1))$. □

Finally, we consider a special effective Nullstellensatz in $\mathbb{Z}[x]$, which based on the proof of Lemma 6.4 in [1].

Lemma 3.8. *If $1 \in (f_1, \ldots, f_m)\mathbb{Z}_{(p)}[x]$, then there exist $h_1, \ldots, h_n \in \mathbb{Z}_{(p)}[x]$ of degree at most $3d^2(2h + \log(d+1))/\log p$ such that*

$$1 = f_1 h_1 + \cdots + f_m h_m.$$

Proof. Suppose $1 \in (f_1, \ldots, f_m)\mathbb{Z}_{(p)}[x]$, then $1 \in (f_1, \ldots, f_m)\mathbb{Q}[x]$. By Lemma 3.2, there exist $\delta \in \mathbb{Z}\setminus\{0\}$ with height $\le d(2h + \log(d+1))$ and $g_1, \ldots, g_m \in \mathbb{Z}[x]$ with degrees $< d$ satisfying

$$\delta = f_1 g_1 + \cdots + f_m g_m. \tag{7}$$

Here and below $h = \text{height}(f_1, \ldots, f_m)$. If δ is a unit in $\mathbb{Z}_{(p)}$, then

$$1 = f_1(g_1/\delta) + \cdots + f_m(g_m/\delta).$$

Let $h_i = g_i/\delta$ for $i = 1, \ldots, m$, then we have the required properties. Suppose that δ is not a unit. Let $\mu = v_p(\delta) \ge 1$. Clearly we have $1 \in (f_1, \ldots, f_m)(\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)})[x]$. Then by the Extended Euclidean Algorithm, there exist $r_1, \ldots, r_m \in \mathbb{Z}[x]$ with

$$1 - (r_1 f_1 + \cdots + r_m f_m) \in (p)\mathbb{Z}_{(p)}[x]$$

and $\deg(r_j) < d$ for all $j = 1, \ldots, m$. So there exists $s_1, \ldots, s_m \in \mathbb{Z}_{(p)}[x]$ and $s \in (p^\mu)\mathbb{Z}_{(p)}[x]$ such that

$$1 - (f_1 s_1 + \cdots + f_m s_m) = s. \tag{8}$$

We have $\deg(s_j) \le \mu(2d-1) - d$ for all j; hence $\deg(s) \le \mu(2d-1)$. By equations (7) and (8), we have

$$1 = f_1 s_1 + \cdots + f_m s_m + s = f_1 h_1 + \cdots + f_m h_m$$

with $h_j = s_j + (s/\delta)g_j \in \mathbb{Z}_{(p)}[x]$. We have

$$\deg(s g_j) \le \mu(2d-1) + d \le 3\mu d.$$

Since $\mu \log p \le \text{height}(\delta) \le d(2h + \log(d+1))$, it follows that $\deg(h_j)$ is bounded by $3d^2(2h + \log(d+1))/\log p$. □

Then we can give the degree bound for the global case:

Lemma 3.9. *If* $1 \in (f_1,\dots,f_m)\mathbb{Z}[x]$, *then there exist* $h_1,\dots,h_m \in \mathbb{Z}[x]$ *such that* $1 = f_1h_1+\cdots+f_mh_m$, *with* $\deg(h_i) \le 3d^2(2h+\log(d+1))$ *for* $i = 1,\dots,m$.

Proof. By Lemma 3.2, we have $g_1,\dots,g_m \in \mathbb{Z}[x]$ with degrees $< d$ and $\delta \in \mathbb{Z}$ satisfying

$$\delta = f_1g_1+\cdots+f_mg_m.$$

Let $p_1,\dots,p_k$ be all the prime factors of δ. Since $1 \in (f_1,\dots,f_m)\mathbb{Z}[x]$, $1 \in (f_1,\dots,f_m)\mathbb{Z}_{(p_i)}[x]$. By Lemma 3.8, there exist $h_1^{(p_i)},\dots,h_m^{(p_i)} \in \mathbb{Z}[x]$ with degrees $\le 3d^2(2h+\log(d+1))/\log p_i$ and $\delta^{(p_i)} \in \mathbb{Z}\setminus(p)\mathbb{Z}$ satisfying $\delta^{(p_i)} = f_1h_1^{(p_i)}+\cdots+f_mh_m^{(p_i)}$. Then there exist $a,a_1,\dots,a_k \in \mathbb{Z}$ satisfying

$$1 = a\delta + a_1\delta^{(p_1)}+\cdots+a_k\delta^{(p_k)}.$$

Hence letting $h_j = ag_j + a_1h_j^{(p_1)}+\cdots+a_kh_j^{(p_k)} \in \mathbb{Z}[x]$ for $j = 1,\dots,m$, we get

$$1 = f_1h_1+\cdots+f_mh_m.$$

From this, we can easily get $\deg(h_i) \le 3d^2(2h+\log(d+1))$ for $i = 1,\dots,m$. □

3.2 Degree and height bounds for solutions to linear equations over $\mathbb{Z}[x]$

In this section, we show that the solutions to linear equations over $\mathbb{Z}[x]$ has bases whose degree and height can be nicely bounded.

Throughout this section, let $F = (f_{ij}) \in \mathbb{Z}[x]^{n\times m}$. Denote by $d = \deg(F)$ the maximal degree of elements in F and $h = \mathrm{height}(F)$ the maximal height of elements in F. Let $\mathrm{Sol}_{R[x]}(F)$ be the solution module of the homogeneous linear system $Fy = 0$, where R is a subring of $\mathbb{C}$.

Let r be the rank of F. Without loss of generality, we may assume that the r-th principal minor of F is non-zero. Then the last $n-r$ rows of F are $\mathbb{Q}(x)$ linear combinations of the first r rows. So $Fy = 0$ is equivalent to

$$\begin{pmatrix} f_{11} & \cdots & f_{1r} & \cdots & f_{1m} \\ \vdots & & \vdots & & \vdots \\ f_{r1} & \cdots & f_{rr} & \cdots & f_{rm} \end{pmatrix}\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

So, we may assume $r = n$ unless we mention in particular.

For a prime p, $f = \sum_{v=0}^{\infty} f_v x^v \in \widehat{\mathbb{Z}}_{(p)}\langle x\rangle$ is called *regular of degree s with respect to p*, or simply, *regular of degree s* when there is no confusion, if its reduction $\overline{f} \in \widehat{\mathbb{Z}}_{(p)}\langle x\rangle/p\widehat{\mathbb{Z}}_{(p)}\langle x\rangle$ is unit-monic of degree s, that is,

(1) $\overline{f_s} \neq 0$, and

(2) $v_p(f_i) > 0$ for all $i > s$, where v_p is the p-valuation.

Now we describe the Weierstrass Division Theorem for $\widehat{\mathbb{Z}}_{(p)}\langle x\rangle$:

Theorem 3.10 ([1, 21])**.** *Let* $g \in \widehat{\mathbb{Z}}_{(p)}\langle x\rangle$ *be regular of degree s. Then for each* $f \in \widehat{\mathbb{Z}}_{(p)}\langle x\rangle$ *there are uniquely determined elements* $q \in \widehat{\mathbb{Z}}_{(p)}\langle x\rangle$ *and* $r \in \widehat{\mathbb{Z}}_{(p)}[x]$ *with* $\deg(r) < s$ *such that* $f = qg+r$.

Lemma 3.11. $\mathrm{Sol}_{\widehat{\mathbb{Z}}_{(p)}\langle x\rangle}(F)$ *has a set of generators in* $\mathbb{Z}[x]^m$ *with degrees* $\le nd$.

Proof. Let $\triangle$ be an $n\times n$-submatrix of F with $\delta = \det(\triangle) \neq 0$ having the least p-valuation among all the nonzero $n\times n$ minors of F. After permutating the unknowns of $y_1,\cdots,y_m$ in $Fy = 0$, we may assume $\triangle =$

$(f_{ij})_{1\le i,j\le n}$. Multiplying both sides of $Fy=0$ on the left by the adjoint of $\triangle$, the system $Fy=0$ turns into the system

$$\begin{pmatrix} \delta & & & c_{1,n+1} & \cdots & c_{1,m} \\ & \ddots & & \vdots & & \vdots \\ & & \delta & c_{n,n+1} & \cdots & c_{n,m} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \tag{9}$$

where δ and all the c_{ij} are in $\mathbb{Z}[x]$ with degrees $\le nd$. Note that, $v_p(c_{ij}) \ge v_p(\delta)$ for all i,j, by the choice of $\triangle$. Let

$$v^{(1)} = \begin{pmatrix} -c_{1,n+1} \\ \vdots \\ -c_{n,n+1} \\ \delta \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, v^{(m-n)} = \begin{pmatrix} -c_{1,m} \\ \vdots \\ -c_{n,m} \\ 0 \\ \vdots \\ 0 \\ \delta \end{pmatrix}. \tag{10}$$

Then, $Fv^{(i)}=0$ for $i=1,\ldots,m-n$ and $v^{(1)},\ldots,v^{(m-n)}$ are in the $\widehat{\mathbb{Z}}_{(p)}\langle x\rangle$-module $\mathrm{Sol}_{\widehat{\mathbb{Z}}_{(p)}\langle x\rangle}(F)$. Let $\mu = v_p(\delta), u^{(i)} = p^{-\mu}v^{(i)}$ for $i=1,\ldots,m-n$. Then $u^{(1)},\ldots,u^{(m-n)}$ are also in $\mathrm{Sol}_{\widehat{\mathbb{Z}}_{(p)}\langle x\rangle}(F)$. Multiplying the equation (9) by $p^{-\mu}$, we have $By=0$, where $B = \begin{pmatrix} \varepsilon & & & d_{1,n+1} & \cdots & d_{1,m} \\ & \ddots & & \vdots & & \vdots \\ & & \varepsilon & d_{n,n+1} & \cdots & d_{n,m} \end{pmatrix}$ and ε is regular of degree s for some integer $s \le nd$. Clearly, the $(n+i)$-th element of $u^{(i)}$ is ε. Moreover, ε and all the d_{ij} are in $\mathbb{Z}[x]$ with degrees $\le nd$

In the system $Fy=0$, let

$$f_{ij} = f_{ij0} + \cdots + f_{ijd}x^d,$$
$$y_j = y_{j0} + \cdots + y_{j,nd-1}x^{nd-1}$$

for $1 \le i \le n,\ 1 \le j \le m$, where $f_{ijk} \in \mathbb{Z}_{(p)}$ and y_{jk} are the new unknowns in $\widehat{\mathbb{Z}}_{(p)}\langle x\rangle$. The i-th equation in $Fy=0$ may then be written as

$$\sum_{l=0}^{k}\sum_{j=1}^{m} f_{ijl}y_{j,k-l} = 0, \qquad 0 \le k < (n+1)d,$$

where we put $f_{ijl}=0$ for $l>d$ and $y_{jl}=0$ for $l \ge nd$. Then we obtain a new system $F'y'=0$, where $F' \in \mathbb{Z}_{(p)}^{(nd(n+1))\times(mnd)}$, $y' = [y_{10},\ldots,y_{1,nd-1},\ldots,y_{m0},\ldots,y_{m,nd-1}]^\tau$, whose solutions in $\widehat{\mathbb{Z}}_{(p)}$ are one to one correspondence with the solutions of $Fy=0$ in $\widehat{\mathbb{Z}}_{(p)}[x]$ of degrees $< nd$. We have a set of finite generators for $F'y'=0$, thus we have finitely many solutions $y^{(1)},\ldots,y^{(M')} \in \mathbb{Z}_{(p)}[x]^m$ of $Fy=0$ such that each solution to $Fy=0$ of degree $< nd$ is a $\widehat{\mathbb{Z}}_{(p)}$ linear combination of $y^{(1)},\ldots,y^{(M')}$.

We claim that $u^{(1)},\ldots,u^{(m-n)},y^{(1)},\ldots,y^{(M')}$ generate the $\widehat{\mathbb{Z}}_{(p)}\langle x\rangle$-module $\mathrm{Sol}_{\widehat{\mathbb{Z}}_{(p)}\langle x\rangle}(F)$. So $\mathrm{Sol}_{\widehat{\mathbb{Z}}_{(p)}\langle x\rangle}(F)$ can be generated by elements in $\mathbb{Z}_{(p)}[x]^m$ of degrees $\le nd$.

Now we prove the claim. Let $w=[w_1,\ldots,w_m]^\tau \in \widehat{\mathbb{Z}}_{(p)}\langle x\rangle^m$ be any solution to $Fy=0$. Since ε is regular of degree s for some integer $s \le nd$, by Theorem 3.10, there exists $Q_{n+1},\ldots,Q_m \in \widehat{\mathbb{Z}}_{(p)}\langle x\rangle$ and $R_{n+1},\ldots,R_m \in \widehat{\mathbb{Z}}_{(p)}[x]$ whose degrees are less than s such that $R_j = w_j - Q_j\varepsilon$ for $j=n+1,\ldots,m$. Let $z = w - Q_{n+1}u^{(1)} - \cdots - Q_m u^{(m-n)} = [h_1,\ldots,h_n,R_{n+1},\ldots,R_m]$, which is obvious a solution to $By=0$. So we have $\varepsilon h_i = -d_{i,n+1}R_{n+1} - \cdots - d_{i,m}R_m$ for $i=1,\ldots,n$. Since ε, d_{ij} are in $\widehat{\mathbb{Z}}_{(p)}[x]$ with degrees $\le nd$ and $R_j \in \widehat{\mathbb{Z}}_{(p)}[x]$ are of degrees $< s$, we have $\deg(h_i) < nd$ for $i=1,\ldots,n$. Hence $\deg(z) < nd$, therefore it can be expressed as the $\widehat{\mathbb{Z}}_{(p)}[x]$ combination

of $y^{(1)},\ldots,y^{(M')}$. Now it is clear that w is the $\widehat{\mathbb{Z}}_{(p)}[x]$ combination of $u^{(1)},\ldots,u^{(m-n)},y^{(1)},,\ldots,y^{(M')}$. Hence $\mathrm{Sol}_{\widehat{\mathbb{Z}}_{(p)}\langle x\rangle}(F)$ as a $\widehat{\mathbb{Z}}_{(p)}\langle x\rangle$-module can be generated by $u^{(1)},\ldots,u^{(m-n)},y^{(1)},,\ldots,y^{(M')}$. □

In the proof of Lemma 3.11, if we choose $\triangle$ to be any $n\times n$-submatrix of F whose determinant is nonzero, let $\mu=0$ and do the computations in $\mathbb{Q}[x]$, we can easily give the following lemma:

Lemma 3.12. $\mathrm{Sol}_{\mathbb{Q}[x]}(F)$ *can be generated by elements in* $\mathbb{Z}[x]^m$ *of degrees* $\leq nd$.

Now we describe Corollary 2.7 of [1] in our notations:

Lemma 3.13 ([1]**).** *Let F be an $n\times m$ matrix over $\mathbb{Z}_{(p)}[x]$. If $y^{(1)},\ldots,y^{(L)}\in\mathbb{Z}_{(p)}[x]^m$ generate the $\mathbb{Q}[x]$-module $\mathrm{Sol}_{\mathbb{Q}[x]}(F)$ and $z^{(1)},\ldots,z^{(M)}\in\mathbb{Z}_{(p)}[x]^m$ generate the $\widehat{\mathbb{Z}}_{(p)}\langle x\rangle$-module $\mathrm{Sol}_{\widehat{\mathbb{Z}}_{(p)}\langle x\rangle}(F)$. Then*

$$y^{(1)},\ldots,y^{(L)},z^{(1)},\ldots,z^{(M)}$$

generate the $\mathbb{Z}_{(p)}[x]$-module $\mathrm{Sol}_{\mathbb{Z}_{(p)}[x]}(F)$.

By Lemma 3.11, 3.12 and 3.13, we have the following corollary:

Corollary 3.14. $\mathrm{Sol}_{\mathbb{Z}_{(p)}[x]}(F)$ *can be generated by elements in* $\mathbb{Z}[x]^m$ *of degrees* $\leq nd$.

We describe Lemma 4.2 of [1] in our notations as follows:

Lemma 3.15. *Let M be a $\mathbb{Z}[x]$-submodule of $\mathbb{Z}[x]^m$. For each maximal ideal (p) of $\mathbb{Z}$, let $u_p^{(1)},\ldots,u_p^{(K_p)}\in M$ generate the $\mathbb{Z}_{(p)}[x]$-submodule $M\mathbb{Z}_{(p)}[x]$ of $\mathbb{Z}_{(p)}[x]^m$. Then $u_p^{(1)},\ldots,u_p^{(K_p)}$, where (p) ranges over all maximal ideals of $\mathbb{Z}$, generate the $\mathbb{Z}[x]$-module M.*

We now give a degree bound for the solutions of linear equations over $\mathbb{Z}[x]$.

Corollary 3.16. *Let $F=(f_{ij})\in\mathbb{Z}[x]^{n\times m}$ and $d=\deg(F)$. Then $\mathrm{Sol}_{\mathbb{Z}[x]}(F)$ can be generated by a finite set of elements whose degrees are $\leq nd$.*

Proof. By Corollary 3.14 and Lemma 3.15, we can easily know that $\mathrm{Sol}_{\mathbb{Z}[x]}(F)$ can be generated by elements whose degrees are $\leq nd$. Since $\mathrm{Sol}_{\mathbb{Z}[x]}(F)\subset\mathbb{Z}[x]^m$ and $\mathbb{Z}[x]^m$ is Noetherian, the set of generators must be finite. □

Remark 3.17. *In Lemma 3.11, 3.12 and Corollary 3.14, 3.16, if F is of rank r, then the generators can be bounded by rd.*

In the rest of this section, we give height bounds for $\mathrm{Sol}_{\mathbb{Z}[x]}(F)$. By Lemma 5.1 and Remarks of Corollary 1.5 in [1], we have the following result.

Lemma 3.18 ([1]**).** *Let $A\in\mathbb{Z}^{n\times m}$, $r=\mathrm{rank}(A)$. Then $\mathrm{Sol}_{\mathbb{Z}}(A)$ can be generated by $m-r$ many vectors whose heights are bounded by $2r(h+\log r+1)$, where $h=\mathrm{height}(A)$.*

Let $F\in\mathbb{Z}[x]^{n\times m}$, $d=\deg(F)$ and F is of full rank. Then, we have the following theorem:

Theorem 3.19. $\mathrm{Sol}_{\mathbb{Z}[x]}(F)$ *can be generated by vectors whose degrees are bounded by nd and heights are bounded by $2(n(n+1)d+n)(h+\log(n(n+1)d+n)+1)$, where $h=\mathrm{height}(F)$.*

Proof. By the Corollary 3.16, $\mathrm{Sol}_{\mathbb{Z}[x]}(F)$ can be generated by elements of degrees $\leq nd$. Let $[y_1,\ldots,y_m]^\tau \in \mathrm{Sol}_{\mathbb{Z}[x]}(F)$. Assume $f_{ij} = a_{ij0} + a_{ij1}x + \cdots + a_{ijd}x^d$, $y_j = y_{j0} + y_{j1}x + \cdots + y_{j,nd}x^{nd}$, where $a_{ijk} \in \mathbb{Z}$, y_{jk} are the unknowns ranging over $\mathbb{Z}$. Then, $Fy = 0$ can be written as the following matrix equation

$$\begin{pmatrix} A_1 \\ \vdots \\ A_n \end{pmatrix} y' = 0, \tag{11}$$

where $y' = [y_{10},\ldots,y_{1d},\ldots,y_{m0},\ldots,y_{md}]^\tau$, $A_i = [A_{i1},\ldots,A_{im}]_{((n+1)d+1)\times(m(nd+1))}$, and

$$A_{ij} = \begin{pmatrix} a_{ij0} & & & \\ a_{ij1} & a_{ij0} & & \\ \vdots & & \ddots & \\ a_{ijd} & & & a_{ij0} \\ & \ddots & & \vdots \\ & & & a_{ijd} \end{pmatrix}_{((n+1)d+1)\times(nd+1)}$$

for $i = 1,\ldots,n$. So $\begin{pmatrix} A_1 \\ \vdots \\ A_n \end{pmatrix} \in \mathbb{Z}^{(n(n+1)d+n)\times(m(nd+1))}$. By Lemma 3.18, we have the equation system (11) can be generated by vectors whose heights are bounded by $2(n(n+1)d+n)(h+\log(n(n+1)d+n)+1)$, where $h = \mathrm{height}(F)$. □

Remark 3.20. *In [1], Aschenbrenner gave the following degree bound and height bound for the generators of the solutions to the equations $Ay = 0$, where A is a polynomial matrix over $D = \mathbb{Z}[x_1,\ldots,x_N]$ and $A \in D^{n\times m}$. Let $A \in D^{n\times m}$. Then $\mathrm{Sol}_D(A)$ as a D module has a set of generators with degree at most $(2nd)^{2((N+1)^N-1)}$ and height at most $C_2(2n(d+1))^{(N+1)^{O(N)}}(h+1)$. Here C_2 is a constant only depending on A, $d = \deg(A)$, $h = \mathrm{height}(A)$. Setting $N = 1$ in these bounds, we obtain the degree and height bounds $(2nd)^2$ and $C_2(2n(d+1))^{2^{O(1)}}(h+1)$, respectively, where $d = \deg(A)$, $h = \mathrm{height}(A)$. Our results are much better than that of [1] in $\mathbb{Z}[x]$ case.*

Let $F \in \mathbb{Z}[x]^{n\times m}$, $b \in \mathbb{Z}[x]^m$. We denote $\deg(F,b) = \max(\deg(F),\deg(b))$, $\mathrm{height}(F,b) = \max(\mathrm{height}(F), \mathrm{height}(b))$. Based on the proof of Theorem 6.5 in [1], we have the following degree bound:

Theorem 3.21. *Let $F \in \mathbb{Z}[x]^{n\times m}$, $b \in \mathbb{Z}[x]^n$, $d = \deg(F,b)$, and $h = \mathrm{height}(F,b)$. If the system $Fy = b$ has a solution in $\mathbb{Z}[x]^m$, then it has such a solution of degree $\leq 3n^2d^2(h_2+\log(nd+1))+nd$, where $h_2 = 2(n(n+1)d+n)(h+\log(n(n+1)d+n)+1)$.*

Proof. By Theorem 3.19, there exist generators $z^{(1)},\ldots,z^{(K)}$ for the $\mathbb{Z}[x]$-module of solutions to the system of $(F,-b)z = 0$, where $z^{(k)} = [z_1^{(k)},\ldots,z_{m+1}^{(k)}]^\tau$ is a vector of $m+1$ unknowns, with

$$\begin{aligned} \deg(z^{(k)}) &\leq nd, \\ \mathrm{height}(z^{(k)}) &\leq 2(n(n+1)d+n)(h+\log(n(n+1)d+n)+1) = h_2. \end{aligned}$$

for all $k = 1,\ldots,K$. For each k, let $z_{m+1}^{(k)} \in \mathbb{Z}[x]$ be the last component of $z^{(k)}$. Clearly, $Fy = b$ is solvable in $\mathbb{Z}[x]$ if and only if $1 \in (z_{m+1}^{(1)},\ldots,z_{m+1}^{(K)})$. Moreover, if $h_1,\ldots,h_K$ are elements of $\mathbb{Z}[x]$ such that $1 = h_1z_{m+1}^{(1)} + \cdots + h_Kz_{m+1}^{(K)}$, then $[y,1]^\tau = h_1z^{(1)} + \cdots + h_Kz^{(K)}$ is a solution to $Fy = b$. By Lemma 3.9, we have

$$\deg(h_k) \leq 3n^2d^2(2h_2+\log(nd+1)),$$

where $h_2 = 2(n(n+1)d+n)(h+\log(n(n+1)d+n)+1)$. It follows that $\deg(y) \leq 3n^2d^2(2h_2+\log(nd+1))+nd$. □

Remark 3.22. *By Theorem 6.5 of [1], if the system $Fy = b$ has a solution in $\mathbb{Z}[x_1,\ldots,x_N]$, where $F \in \mathbb{Z}[x_1,\ldots,x_N]^{n\times m}$, then it has such a solution of degree at most $2(2n\deg(F,b))^{(N+1)^{O(N)}} \cdot (\mathrm{height}(F,b)+1)$. If we specialize N to 1 in these bounds, we obtain $O((nd)^{2^{O(1)}}h)$. While our degree bound in Theorem 3.21 is equivalent to $O(n^4d^3h)$.*

3.3 Degree and height bounds for GHNF

In this section, we will give degree and height bounds for GHNF in $\mathbb{Z}[x]^n$.

In the whole section, we assume $F \in \mathbb{Z}[x]^{n\times m}$, $d = \deg(F)$, $h = \mathrm{height}(F)$, and F is of full rank. Denote by $\deg(c_{r_i,l_i})$ and $\mathrm{height}(c_{r_i,1})$ the degree and the height of the r_i-row of the GHNF $\mathscr{C}$ in (4) respectively. Note that, $\max_{1\le j\le l_i}\deg(c_{r_i,j}) = \deg(c_{r_i,l_i})$, and by Proposition 2.4, $\max_{1\le j\le l_i}\mathrm{height}(c_{r_i,j}) = \mathrm{height}(c_{r_i,1})$ for each i. The degree of the GHNF $\mathscr{C}$ can be defined as $\max_i \deg(c_{r_i,l_i})$ and the height of it is defined to be $\max_i \mathrm{height}(c_{r_i,1})$.

We first give the degree bound of the GHNF. The following theorem gives the degree bound for the GHNF of F.

Theorem 3.23. *Let $F = (f_{ij}) \in \mathbb{Z}[x]^{n\times m}$ with $d = \deg(F)$, and $\mathscr{C}$, as described in (4), be the* GHNF *of F. Then $\deg(c_{r_i,l_i}) \le (n-r_i+1)d$ for $1 \le i \le t$.*

Proof. It is obvious that $\deg(c_{r_i,j}) \le \deg(c_{r_i,l_i})$ for any $i = 1,\ldots,t$, $j = 1,\ldots,l_i$. It suffices to prove the theorem for $r_1 = 1$, in which case we should prove $\deg(c_{1,l_1}) \le nd$.

For any $[a,0,\cdots,0]^\tau \in (F)$, which is the $\mathbb{Z}[x]$ lattice generated by the columns of F, there exist $u_1,\ldots,u_m \in \mathbb{Z}[x]$ such that

$$\begin{cases} a = u_1 f_{11} + \cdots + u_n f_{1,m} \\ 0 = u_1 f_{21} + \cdots + u_n f_{2,m} \\ \quad \cdots \\ 0 = u_1 f_{n1} + \cdots + u_n f_{n,m}. \end{cases} \tag{12}$$

Then, $[u_1,\ldots,u_m]^\tau$ is a solution to $\mathrm{Sol}_{\mathbb{Z}[x]}(F_{n-1})$, where F_{n-1} is the matrix formed by the last $n-1$ rows of F. By Corollary 3.16, $\mathrm{Sol}_{\mathbb{Z}[x]}(F_{n-1})$ can be generated by elements of degrees $\le (n-1)d$, say $\{v^{(1)},\ldots,v^{(s)}\}$. Then, $[u_1,\ldots,u_m]^\tau$ is a $\mathbb{Z}[x]$ linear combination of $\{v^{(1)},\ldots,v^{(s)}\} \subseteq \mathbb{Z}[x]^m$. Hence $[a,0,\ldots,0]^\tau$ is a $\mathbb{Z}[x]$ linear combination of $\{Fv^{(1)},\ldots,Fv^{(s)}\}$. Since $\deg(Fv^{(k)}) \le nd$ and $Fv^{(k)}$ has the form $[b,0,\ldots,0]^\tau$ for any $1 \le k \le s$, by Lemma 3.6, we have $\deg([c_{1,l_1},0,\ldots,0]^\tau) \le nd$, *i.e.* $\deg(c_{1,l_1}) \le nd$. □

Remark 3.24. *Note that, since the last $n-r_i+1$ rows of F have rank $t-i+1$, by the above proof, we can easily see,* $\deg(c_{r_i,l_i}) \le (t-i+1)d$ *for $1 \le i \le t$.*

Now we can give the height bounds for the GHNF of F.

Theorem 3.25. *Let $\mathscr{C}$ be the* GHNF *of F, as described in (4). Then* $\mathrm{height}(c_{r_i,j}) \le 6(n-r_i+1)^3d^2(h+1+\log((n-r_i+1)^2d))$ *for any $i = 1,\ldots,t,\ j = 1,\ldots,l_i$.*

Proof. It is obvious that $\mathrm{height}(c_{r_i,j}) \le \mathrm{height}(c_{r_i,1})$ for any $i = 1,\ldots,t,\ j = 1,\ldots,l_i$. Following the proof of Theorem 3.23, we need only to prove the theorem for $r_1 = 1$, in which case $\mathrm{height}(c_{11}) \le 6n^3d^2(h+1+\log(n^2d))$.

We know that $[a,0,\ldots,0]^\tau \in (F)$ can be generated by $\{Fv^{(1)},\ldots,Fv^{(s)}\}$, where $\deg(v^{(j)}) \le (n-1)d$ and $\mathrm{height}(v^{(j)}) \le h_1^{(1)}$ where $h_1^{(1)} = 2(n(n-1)d+(n-1))(h+\log(n(n-1)d+(n-1))+1)$. Hence $\deg(Fv^{(j)}) \le nd$ and $\mathrm{height}(Fv^{(j)}) \le h+h_1^{(1)}$. Let $(Fv^{(j)})' = Fv^{(j)}/\gcd(Fv^{(1)},\ldots,Fv^{(s)})$. By Lemma 3.4 and Remark 3.5, we have $\mathrm{height}(\gcd(Fv^{(1)},\ldots,Fv^{(s)}))$ and $\mathrm{height}((Fv^{(j)})')$ for $j = 1,\ldots,s$ are both $\le \frac{1}{2}\log(nd+1)+$

$nd\log 2 + h + h_1^{(1)}$. Moreover, the first element r of the GHNF of $\{(Fv^{(1)})', \ldots, (Fv^{(s)})'\}$ is in $\mathbb{Z}$, by Lemma 3.2, we have height$(r) \le nd(2h + 2h_1^{(1)} + 2\log(nd+1) + 2nd\log 2)$. Then, we can easily get

$$\begin{aligned}
\text{height}(c_{11}) &\le nd(2h + 2h_1^{(1)} + 2\log(nd+1) + 2nd\log 2) + \frac{1}{2}\log(nd+1) + nd\log 2 + h + h_1^{(1)} \\
&= (2nd+1)(h + h_1^{(1)}) + (2nd + \frac{1}{2})\log(nd+1) + nd(2nd+1)\log 2 \\
&\le (2nd+1)(h + 2(nd+1)(n-1)(h + \log(n-1)(nd+1)+1) + \log(nd+1) + nd) \\
&\le 2n(2nd+1)(nd+1)(h + \log(n-1)(nd+1)+1) \\
&\le 6n^3d^2(h+1+\log(n^2d)) \qquad \text{for any } n \ge 4,\ d \ge 1. \qquad (13)
\end{aligned}$$

It easily to verify height$(c_{11}) \le 6n^3d^2(h+1+\log(n^2d))$ is also valid for $n = 1,2,3$ and $d \ge 1$. □

Remark 3.26. *Note that, since the last $n - r_i + 1$ rows of F have rank $t - i + 1$, by the above proof, we have* height$(c_{r_i,1}) \le 6(t-i+1)^3d^2(h+1+\log((t-i+1)^2d))$ *where* $h = \text{height}(F)$.

Combining Theorems 3.21, 3.23, and 3.25, we have the following degree bound for the transformation matrix U, which satisfying $\mathscr{C} = FU$:

Theorem 3.27. *Let $F \in \mathbb{Z}[x]^{n\times m}$ and $\mathscr{C}$ its* GHNF. *$U \in \mathbb{Z}[x]^{m\times s}$ is the transformation matrix satisfying $\mathscr{C} = FU$. Then,* deg$(U) \le D$, *where* $D = 73n^8d^5(h+1+\log(n^2d))$.

Proof. By Theorems 3.23 and 3.25, we have deg$(c_{r_i,j}) \le (n - r_i + 1)d$, height$(c_{r_i,j}) \le 6(n-r_i+1)^3d^2(h + 1 + \log((n-r_i+1)^2d))$ for any $i = 1,\ldots,t,\ j = 1,\ldots,l_i$. Denote by $U_{r_i,j}$ the column vector of U, satisfying $FU_{r_i,j} = [*,\ldots,*,c_{r_i,j},0,\ldots,0]^\tau$. Then $U_{r_i,j}$ is determined by $F_{n-r_i+1}U_{r_i,j} = [c_{r_i,j},0,\ldots,0]^\tau$, where F_{n-r_i+1} is the last $n - r_i + 1$ rows of F. In Theorem 3.21, let deg$(F,b) = \max_{i,j}\text{deg}(F,c_{r_i,j}) \le nd$, height$(F,b) = \max_{i,j}\text{height}(F,c_{r_i,j}) \le 6n^3d^2(h+1+\log(n^2d))$. Then we have deg$(U) \le 3n^2d^2(h_2 + \log(nd+1)) + nd$, where $h_2 = 2(n(n+1)\text{deg}(F,b) + n)(\text{height}(F,b) + \log(n(n+1)\text{deg}(F,b)+n) + 1)$. First, we have the following inequality:

$$\begin{aligned}
h_2 &= 2(n(n+1)\text{deg}(F,b) + n)(\text{height}(F,b) + \log(n(n+1)\text{deg}(F,b)+n) + 1) \\
&\le 2(n^2(n+1)d + n)(6n^3d^2(h+1+\log(n^2d)) + \log(n^2(n+1)d+n) + 1) \\
&\le 24n^6d^3(h+1+\log n^2d) \qquad \text{for any } n \ge 2. \qquad (14)
\end{aligned}$$

One can verify that the above inequality is still valid for $n = 1$, in which case deg$(F,b) \le d$ and height$(F,b) \le d(2h + \log(d+1)) + \frac{1}{2}\log(d+1) + d\log d + h$. So we have

$$\begin{aligned}
\text{deg}(U) &\le 3n^2d^2h_2 + 3n^2d^2\log(nd+1) + nd \\
&\le 73n^8d^5(h+1+\log n^2d). \qquad (15)
\end{aligned}$$

□

We give an example to illustrate the main idea of the proof.

Example 3.28. *Let* $F = \begin{pmatrix} 1 & x \\ 6x^3+1 & 8x^2 \end{pmatrix}$. *Let $h = 3\log 2 = 3$ be the height of F, where we choose the logarithm with 2 as a base.*

If $a = [a_1, a_2]^\tau$ with $a_2 \ne 0$ as a column vector of G, then a_2 is an element of the GHNF *of* $[6x^3+1, 8x^2]$. *Thus,* deg$(a_2) \le \max(\text{deg}(6x^3+1), \text{deg}(8x^2)) = 3$ *and by Lemma 3.4,* height$(a_2) \le 4\log 2 + h = 7$.

If $b = [b_1, 0]^\tau$ with $b_1 \ne 0$ is a column of G, there exists a $U = [u_1, u_2]^\tau \in \mathbb{Z}[x]^2$ satisfying

$$b = FU, \quad i.e. \quad \begin{cases} b_1 = u_1 + xu_2 \\ 0 = (6x^3+1)u_1 + 8x^2u_2 \end{cases}$$

Let $\mathbf{g}_1, \ldots, \mathbf{g}_s$ *be the generators of the solutions to* $0 = (6x^3+1)u_1 + 8x^2u_2$. *By Theorem 3.19,* $\deg(\mathbf{g}_i) \le 3$ *and* $\text{height}(\mathbf{g}_i) \le 14(h + \log 7 + 1)$. *Thus,* b_1 *is an element of the* GHNF *of* $[1,x] \cdot [\mathbf{g}_1, \ldots, \mathbf{g}_s] = [h_1, \ldots, h_s]$, *where* $\deg(h_i) \le 4$, *and* $\text{height}(h_i) \le 28(h + \log 7 + 1) < 196$. *Hence, by Theorem 3.23,* $\deg(d_1) \le 4$, *by Theorem 3.25,* $\text{height}(d_1) \le 432(h + 1 + \log 12) < 3456$. *Moreover, by Theorem 3.27, we know that the degree bound for the transformation matrix is* $D = 4478976(h + 1 + \log 12) < 35831808$.

Actually, the solution to $0 = (6x^3+1)u_1 + 8x^2u_2$ *can be generated by* $[8x^2, -(6x^3+1)]^\tau$. *Thus,* b_1 *is an element of the* GHNF *of* $[1,x] \cdot [8x^2, -(6x^3+1)]^\tau = [-6x^4 + 8x^2 - x]$. *The* GHNF

$$G = \begin{pmatrix} 6x^4 - 8x^2 + x & 3x^8 - 4x^6 + 5x^5 - 6x^3 + 1 \\ 0 & 1 \end{pmatrix},$$

with transformation matrix $U = \begin{pmatrix} -8x^2 & -4x^6 - 6x^3 + 1 \\ 6x^3 + 1 & 3x^7 + 5x^4 \end{pmatrix}$.

From the above example, we can see that, although the degree bound in Theorem 3.27 is polynomial, it is far from optimal.

4 GHNF Algorithm in matrix form

There exist efficient algorithms to compute the HNF of a matrix over $\mathbb{Z}$ [4]. The main idea of our algorithm is to convert the computation of GHNF for $\mathbb{Z}[x]$ lattice into the computation of HNF over $\mathbb{Z}$. In [10], Faugère gave the famous F4 algorithm which converts the computation of Gröbner bases of polynomial systems to matrix computation of their coefficients. The F4 algorithm computes successive truncated Gröbner bases and it replaces the classical successive reduction in Buchberger algorithm by the Gauss elimination of the coefficient matrix. Our algorithm could be considered as a $\mathbb{Z}[x]$-lattice variant of the F4 algorithm, which is specifically designed so that its complexity can be estimated.

Complexity cost: In this section, we measure the cost of our algorithms in number of bit operations. To this end, we assign a function $M(k) : \mathbb{N} \mapsto \mathbb{R}_{\ge 0}$, which shows that the cost of basic operations of multiplications and quotients of two integers a and b with $|a|, |b| < 2^k$, can be computed in $O(M(k))$ bit operations. The currently fastest algorithms allows $M(k) = k \log k \log\log k$. In the sequel we will give complexity results in terms of the function $B(k) = M(k)\log k = O(k(\log k)^2(\log\log k))$. We use a parameter θ such that the multiplication of two $n \times n$ integer matrices needs $O(n^\theta)$ basic operations. The currently best known upper bound for θ is about 2.376.

4.1 HNF-based algorithm-the $\mathbb{Z}[x]$ case

Given a polynomial set $\{f_1, \ldots, f_m\} \subseteq \mathbb{Z}[x]$, with $d_i = \deg(f_i)$, $d = \max_{1 \le i \le m} d_i$. $F = [f_1, \ldots, f_m]$ is its corresponding polynomial vector. Denote by $m = \#(F)$ the number of elements in F. $H \in \mathbb{Z}^{(d+1)\times m}$ is called the *coefficient matrix* of F if its columns represent the polynomials in F satisfying $XH = F$, where $X = [1, x, \ldots, x^d]$. Let H_1 be the Hermite normal form of H and $F' = XH_1$ be the polynomial vector corresponding to H_1. We call F' the *polynomial Hermite normal form* (PHNF) of F. For simplicity, we denote by $H = M(F)$ and $F' = \text{PHNF}(F)$. Here we should notice that if H_1 has zero columns, F' will contain zero elements. By the action of PHNF, we omit all the zero elements.

For any polynomial vector $F = [f_1, \ldots, f_m]$, we also denote $\mathbf{LC}(F) = [\mathbf{LC}(f_1), \ldots, \mathbf{LC}(f_m)]$, $\mathbf{LC}_t(F) = \mathbf{LC}([f_i | \deg(f_i) = t])$, where t ranges over the degrees of F.

Example 4.1. $F=[x^2+3x+3, x^3+5x^2+4x+3]$. *The coefficient matrix of* F *is* $H=M(F)=\begin{pmatrix}3&3\\3&4\\1&5\\0&1\end{pmatrix}$.

Moreover, $H_1=\begin{pmatrix}3&3\\3&4\\1&5\\0&1\end{pmatrix}$ *is the Hermite normal form of* H*, so* $F_1=XH_1=[x^2+3x+3, x^3+5x^2+4x+3]=\mathrm{PHNF}(F)$. $\mathbf{LC}(F_1)=[1,1]$, $\mathbf{LC}_2(F_1)=1$, $\mathbf{LC}_3(F_1)=1$.

In the following of this subsection, we always assume the polynomials vector to be ranked in the increasing order *w.r.t.* $\prec$ and for the input polynomial vector set $F=[f_1,\ldots,f_m],\ f_i\in\mathbb{Z}[x]$, we always denote $d_i=\deg(f_i)$ for $i=1,\ldots,m$.

Inspired by Chapter 3, we increase the total degree by 1 in each loop of our Algorithm GHNF_1.

Algorithm 1 $\mathrm{GHNF}_1(F)$

Input: $F=[f_1,\ldots,f_m],\ f_i\in\mathbb{Z}[x]$.

Output: $G=[g_1,\ldots,g_s]$, the GHNF of F.

1: Let $G_1=\mathrm{PHNF}(F)=[g_1,\ldots,g_t]$.

2: (loop) $F_1=[G_1, xg_1,\ldots,xg_{t-1}]$, $G_2=\mathrm{PHNF}(F_1)$.
While G_1 and G_2 do not satisfy the **Termination condition T** given below, let $G_1=G_2=[g_1,\ldots,g_t]$, repeat Step 2; otherwise, we get a polynomial vector $G_1=[g_1,\ldots,g_t]$ and the condition number i satisfying **Termination condition T**, go to Step 3.

3: Let $G=[g_1]$.
For j from 2 to i, if $\mathbf{LC}(g_{j-1})\nmid\mathbf{LC}(g_j)$, $G=G\cup\{g_j\}$.

4: Return G.

Termination condition T: For two polynomial vectors $G=[g_1,\ldots,g_t]$, $H=[h_1,\ldots,h_s]$,

1. $s=t$;
2. let i be the largest integer such that $\mathbf{LC}(g_j)=\mathbf{LC}(h_j)$, $j=1,\ldots,i$, and $\mathbf{LC}(g_{i+1})\neq\mathbf{LC}(h_{i+1})$, then either $i=t$ or $\mathbf{LC}(g_k)=\mathbf{LC}(h_{k+1})$ for $k=i,\ldots,t-1$.

We call the i in the above condition *condition number*.

Now, we give two examples to illustrate our algorithm.

Example 4.2. $F=[6x^3+3x^2+12, 6x^3+3x^2+6x, 6x^3+15x^2, 6x^3+3x^2]$.

1-*th loop:* $G_1=\mathrm{PHNF}(F)=[12, 6x, 12x^2, 6x^3+3x^2]$,
$F_1=[G_1, 12x, 6x^2, 12x^3]$,
$G_2=\mathrm{PHNF}(F_1)=[12, 6x, 6x^2, 6x^3+3x^2]$.
G_1 *and* G_2 *do not satisfy the* **Termination condition T**.

2-*th loop:* $G_1=G_2$,
$F_1=[G_1, 12x, 6x^2, 6x^3]$,
$G_2=\mathrm{PHNF}(F_1)=[12, 6x, 3x^2, 6x^3]$;
G_1 *and* G_2 *do not satisfy the* **Termination condition T**.

3-*th loop:* $G_1=G_2$,
$F_1=[G_1, 12x, 6x^2, 3x^3]$,
$G_2=\mathrm{PHNF}(F_1)=[12, 6x, 3x^2, 3x^3]$;
G_1 *and* G_2 *do not satisfy the* **Termination condition T**.

4-*th loop:* $G_1 = G_2$,
$F_1 = [G_1, 12x, 6x^2, 3x^3]$,
$G_2 = \mathrm{PHNF}(F_1) = [12, 6x, 3x^2, 3x^3]$;
G_1 *and* G_2 *satisfy the* **Termination condition T**.

5-*th loop:* $G = [12, 6x, 3x^2]$ *is the* GHNF *of* F.

Example 4.3. $F = [30x^2 + 10, 30x^2 + 20x, 30x^2]$.

1-*th loop:* $G_1 = \mathrm{PHNF}(F) = [10, 20x, 30x^2]$,
$F_1 = [G_1, 10x, 20x^2]$,
$G_2 = \mathrm{PHNF}(F_1) = [10, 10x, 10x^2]$,
G_1 *and* G_2 *do not satisfy the* **Termination condition T**.

2-*th loop:* $G_1 = G_2$,
$F_1 = [G_1, 10x, 10x^2]$,
$G_2 = \mathrm{PHNF}(F_1) = [10, 10x, 10x^2]$,
G_1 *and* G_2 *satisfy the* **Termination condition T**.

3-*th loop:* $G = [10]$ *is the* GHNF *of* F.

We now show the correctness of the Algorithm GHNF_1. Firstly, we give the following lemma:

Lemma 4.4. *For any two polynomial vectors* F *and* G*, and any polynomial* $f \in \mathrm{Span}_{\mathbb{Z}}(F)$*, we have*

$$\mathbf{LC}_{\deg(f)}(\mathrm{PHNF}(F)) | \mathbf{LC}(f).$$

Moreover,

1) *if* $\mathrm{Span}_{\mathbb{Z}}(F) \subseteq \mathrm{Span}_{\mathbb{Z}}(G)$*, then* $\mathbf{LC}_t(\mathrm{PHNF}(G)) | \mathbf{LC}_t(\mathrm{PHNF}(F))$*, where* t *ranges over the degrees of* $\mathrm{PHNF}(F)$*;*

2) *if* $\mathrm{Span}_{\mathbb{Z}}(F) \subseteq \mathrm{Span}_{\mathbb{Z}}(G)$ *and* $\mathbf{LC}(\mathrm{PHNF}(F)) = \mathbf{LC}(\mathrm{PHNF}(G))$*, then* $\mathrm{PHNF}(F) = \mathrm{PHNF}(G)$*;*

3) *if* $\mathrm{Span}_{\mathbb{Z}}(F) = \mathrm{Span}_{\mathbb{Z}}(G)$*, then* $\mathrm{PHNF}(F) = \mathrm{PHNF}(G)$.

Proof. By the property of PHNF, we know that f can be written as the $\mathbb{Z}$ linear combination of the elements in $\mathrm{PHNF}(F)$, each of whom has different degree. So $\mathbf{LC}_{\deg(f)}(\mathrm{PHNF}(F)) | \mathbf{LC}(f)$.

1) For any $f \in \mathrm{PHNF}(F)$, $f \in \mathrm{Span}_{\mathbb{Z}}(F) \subseteq \mathrm{Span}_{\mathbb{Z}}(G)$. So $\mathbf{LC}_{\deg(f)}(\mathrm{PHNF}(G)) | \mathbf{LC}(f)$. Hence, we have $\mathbf{LC}_t(\mathrm{PHNF}(G)) | \mathbf{LC}_t(\mathrm{PHNF}(F))$ for t ranging over the degrees of $\mathrm{PHNF}(F)$.

2) Let $\mathrm{PHNF}(F) = [f_1, \ldots, f_t]$, $\mathrm{PHNF}(G) = [g_1, \ldots, g_s]$. Since $\mathbf{LC}(\mathrm{PHNF}(F)) = \mathbf{LC}(\mathrm{PHNF}(G))$, we have $s = t$ and $\deg(f_i) = \deg(g_i)$ for $1 \le i \le t$. Otherwise, since $\deg(f_1) < \cdots < \deg(f_t)$ and $\deg(g_1) < \ldots < \deg(g_t)$, there must be an integer $k:\ 1 \le k \le t$, such that $\deg(f_k) \ne \deg(g_j)$ for any $1 \le j \le t$. But, $f_k \notin \mathrm{Span}_{\mathbb{Z}}(\mathrm{PHNF}(G)) = \mathrm{Span}_{\mathbb{Z}}(G)$, which is contrary to the condition of 2). So $\mathbf{LT}(f_i) = \mathbf{LT}(g_i)$ for $1 \le i \le t$. Suppose k is the smallest integer, such that $g_k \ne f_k$, then $g_k - f_k \in \mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_{k-1}) = \mathrm{Span}_{\mathbb{Z}}(f_1, \ldots, f_{k-1})$. Let $g_k = f_k + \sum_{i=1}^{k-1} u_i f_i$ for some integers $u_1, \ldots, u_{k-1}$. If there exists $u_i \ne 0,\ 1 \le i \le k-1$, then g_k is not reduced *w.r.t.* $g_i = f_i$. But by the property of the Hermite normal form for the integer matrix, g_k is reduced *w.r.t.* g_i for $1 \le i \le k-1$, hence $g_k = f_k$. By induction, we have $g_i = f_i$ for $1 \le i \le t$.

3) By 1), we have $\mathbf{LC}(\mathrm{PHNF}(F)) = \mathbf{LC}(\mathrm{PHNF}(G))$. By 2), $\mathrm{PHNF}(F) = \mathrm{PHNF}(G)$. □

In the Algorithm GHNF_1, let $G^{(1)} = [g_{k_1}, \ldots, g_d]$ be the polynomial vector G_1 obtained by Step 1 of the Algorithm GHNF_1, where $\deg(g_j) = j$ for $k_1 \le j \le d$. We can explain the Step 2(loop) in the following chart:

$$\text{loop: } G^{(1)} \xrightarrow{\text{add } [xg_{k_1}, \ldots, xg_{d-1}]} F^{(1)} \xrightarrow{\text{PHNF}} G^{(2)} \xrightarrow{\text{add } [xh_{k_2}, \ldots, xh_{d-1}]} F^{(2)} \xrightarrow{\text{PHNF}} G^{(3)} \longrightarrow \cdots \tag{16}$$

where $F^{(1)} = [g_{k_1}, \ldots, g_d, xg_{k_1}, \ldots, xg_{d-1}]$, $G^{(2)} = [h_{k_2}, \ldots, h_d]$, $F^{(2)} = [h_{k_2}, \ldots, h_d, xh_{k_2}, \ldots, xh_{d-1}]$.

The original idea of this algorithm is to lift the degrees one by one, *i.e.* let $F_i = [F_{i-1}, x^i F]$, where $F_0 = F$. This process is equivalent to substitute the Step 2 of the Algorithm GHNF_1 with the following chart:

$$\text{loop}' : \; G^{(1)} \xrightarrow{\text{add } [xg_{k_1}, \ldots, xg_{d-1}, xg_d]} F^{(1)'} \xrightarrow{\text{PHNF}} G^{(2)'} \xrightarrow{\text{add } [xh'_{k_2}, \ldots, xh'_d, xh'_{d+1}]} F^{(2)'} \xrightarrow{\text{PHNF}} G^{(3)'} \longrightarrow \cdots$$

where $F^{(1)'} = [g_{k_1}, \ldots, g_d, xg_{k_1}, \ldots, xg_d]$, $G^{(2)'} = [h'_{k_2}, \ldots, h'_d, h'_{d+1}]$, $F^{(2)'} = [h'_{k_2}, \ldots, h'_{d+1}, xh'_{k_2}, \ldots, xh'_{d+1}]$.

Now, we show that the above two processes are equivalent when we compute the GHNF for $\mathbb{Z}[x]$ case.

Lemma 4.5. *Let $G^{(i)'} = [g_{k_i}, \ldots, g_{d+i}]$ and $F^{(i)'} = [g_{k_i}, \ldots, g_{d+i}, xg_{k_i}, \ldots, xg_{d+i}]$, where $k_i \le d$ and $\deg(g_j) = j$, $k_i \le j \le d+i$. Then, $\mathbf{LC}(g_d)|\mathbf{LC}(g_{d+1})|\cdots|\mathbf{LC}(g_{d+i})$ and for any $f \in \mathrm{Span}_{\mathbb{Z}}(F^{(i)'})$, if $\deg(f) \le k$, $d \le k \le d+i+1$, then, $f \in \mathrm{Span}_{\mathbb{Z}}(g_{k_i}, \ldots, g_d, xg_{k_i}, \ldots, xg_{d-1}, xg_d, \ldots, xg_{k-1})$. That is, the above two processes, loop and loop$'$, are equivalent for computing the* GHNF.

Proof. When $i = 1$, we have $G^{(1)} = [g_{k_1}, \ldots, g_d]$, $F^{(1)'} = [g_{k_1}, \ldots, g_d, xg_{k_1}, \ldots, xg_d]$. Then, $k = d$ and the lemma is valid.

Suppose it is valid for $i = 1, \ldots, s$.

When $i = s+1$, in order to distinguish $G^{(s)'}$ and $G^{(s+1)'}$, let $G^{(s)'} = [g_{k_s}, \ldots, g_{d+s}]$ and $G^{(s+1)'} = [h_{k_{s+1}}, \ldots, h_{d+s+1}]$. Then, $F^{(s)'} = [g_{k_s}, \ldots, g_{d+s}, xg_{k_s}, \ldots, xg_{d+s}]$, $F^{(s+1)'} = [h_{k_{s+1}}, \ldots, h_{d+s+1}, xh_{k_{s+1}}, \ldots, xh_{d+s+1}]$. We need to show that $\mathbf{LC}(h_d)|\mathbf{LC}(h_{d+1})|\cdots|\mathbf{LC}(h_{d+s+1})$, and for $d \le k \le d+s+2$, if $f \in \mathrm{Span}_{\mathbb{Z}}(F^{(s+1)'})$ and $\deg(f) \le k$, we have $f \in \mathrm{Span}_{\mathbb{Z}}(h_{k_{s+1}}, \ldots, h_d, xh_{k_{s+1}}, \ldots, xh_{d-1}, xh_d, \ldots, xh_{k-1})$.

By induction, we have for $d+1 \le p \le d+s+1$, $h_p = xg_{p-1} + l_p, h_{p+1} = xg_p + l_{p+1}$ for some $l_p \in \mathrm{Span}_{\mathbb{Z}}(g_{k_s}, \ldots, g_d, xg_{k_s}, \ldots, xg_{d-1}, xg_d, \ldots, xg_{p-2}) \subseteq \mathrm{Span}_{\mathbb{Z}}(h_{k_{s+1}}, \ldots, h_{p-1})$ and $l_{p+1} \in \mathrm{Span}_{\mathbb{Z}}(g_{k_s}, \ldots, g_d, xg_{k_s}, \ldots, xg_{d-1}, xg_d, \ldots, xg_{p-1}) \subseteq \mathrm{Span}_{\mathbb{Z}}(h_{k_{s+1}}, \ldots, h_p)$. Hence, $\mathbf{LC}(h_{d+1})|\cdots|\mathbf{LC}(h_{d+s+1})$. Moreover, by induction we have $h_d \in \mathrm{Span}_{\mathbb{Z}}(g_{k_s}, \ldots, g_d, xg_{k_s}, \ldots, xg_{d-1})$, and $\mathbf{LC}(h_d)|\mathbf{LC}(g_d) = \mathbf{LC}(h_{d+1})$ follows.

Let $f = \sum_{p=k_{s+1}}^{q} c_p h_p + \sum_{p=k_{s+1}}^{r} d_p x h_p$ where $c_p, d_p \in \mathbb{Z}$. If $q \le d$, then $r \le k-1$, we are done. Otherwise, we rewrite the expression of f. Since $\mathbf{LC}(h_d)|\mathbf{LC}(h_{d+1})|\cdots|\mathbf{LC}(h_{d+s+1})$, we have $h_q - axh_{q-1} = x(g_{q-1} - axg_{q-2}) + l_q - axl_{q-1}$ where $a = \frac{\mathbf{LC}(h_q)}{\mathbf{LC}(h_{q-1})}$. Then $\deg(g_{q-1} - axg_{q-2}) \le q-2$, we have $g_{q-1} - axg_{q-2} \in \mathrm{Span}_{\mathbb{Z}}(h_{k_{s+1}}, \ldots, h_{q-2})$. Hence, $h_q \in \mathrm{Span}_{\mathbb{Z}}(h_{k_{s+1}}, \ldots, h_{q-1}, xh_{k_{s+1}}, \ldots, xh_{q-2}, xh_{q-1})$, that is, $h_q = \sum_{p=k_{s+1}}^{q-1} a_p h_p + \sum_{p=k_{s+1}}^{q-1} b_p x h_p$ for some $a_p, b_p \in \mathbb{Z}$. Rewrite the expression of f by the above equation, we have $f = \sum_{p=k_{s+1}}^{q-1} c'_p h_p + \sum_{p=k_{s+1}}^{r'} d'_p x h_p$ for some $c'_p, d'_p \in \mathbb{Z}$. Inductively, we have $f = \sum_{p=k_{s+1}}^{d} c''_p h_p + \sum_{p=k_{s+1}}^{r''} d''_p x h_p$ for some $c''_p, d''_p \in \mathbb{Z}$. Since $\deg(f) \le k$, we have $r'' \le k-1$, $f \in \mathrm{Span}_{\mathbb{Z}}(h_{k_{s+1}}, \ldots, h_d, xh_{k_{s+1}}, \ldots, xh_{d-1}, xh_d, \ldots, xh_{k-1})$.

Moreover, $\mathrm{Span}_{\mathbb{Z}}(F^{(s+1)'}) = \mathrm{Span}_{\mathbb{Z}}(h_{k_{s+1}}, \ldots, h_d, xh_{k_{s+1}}, \ldots, xh_{d-1}, xh_d, \ldots, xh_{d+s+1})$, that is, loop and loop$'$ are equivalent for computing the GHNF. □

Remark 4.6. *By the way we construct F_1 in Step 2 of Algorithm* GHNF_1*, we know the maximal degree of G_1 and G_2 are always d. Then $\#(G_2) = \#(G_1)$ must be satisfied in some loop. In this case,* $\min\deg(G_1) = \min\deg(G_2)$*, $M(G_1)$ and $M(G_2)$ are upper triangulares with forms:*

$$\begin{pmatrix} * & \cdots & * \\ \vdots & \cdots & * \\ * & \cdots & * \\ a_1 & \cdots & * \\ & \ddots & \vdots \\ & & a_t \end{pmatrix}_{(d+1)\times t} \quad \textit{and} \quad \begin{pmatrix} * & \cdots & * \\ \vdots & \cdots & * \\ * & \cdots & * \\ c_1 & \cdots & * \\ & \ddots & \vdots \\ & & c_t \end{pmatrix}_{(d+1)\times t},$$

where $t = \#(G_1) \leq d+1$ *and* $a_j, c_j \neq 0$ *for* $1 \leq j \leq t$. *Note that in each loop,* $M(F_1)$ *is of size* $(d+1) \times s$ *for some integer* $s \leq 2d+1$, *and* $\deg(g_j) = \deg(g_{j-1}) + 1, 2 \leq j \leq t$.

To show the correctness and the termination of this algorithm, we need only to consider the case that G_1 and G_2 in the Step 2 of Algorithm GHNF_1 has satisfied the condition 1 of the **Termination condition T**, *i.e.* $\#(G_2) = \#(G_1)$. In the following, we assume that $G_1 = [g_1, \ldots, g_t]$ with $\mathbf{LC}(G_1) = [a_1, \ldots, a_t]$, $G_2 = [h_1, \ldots, h_t]$ with $\mathbf{LC}(G_2) = [b_1, \ldots, b_t]$. Here, $\deg(g_1) = \deg(h_1) = d - t + 1$.

Lemma 4.7. *For the above* G_1 *and* G_2, *if there exists* $i: \ 1 \leq i \leq t$ *satisfying* $a_j = b_j$ *for* $1 \leq j \leq i$, *then*

1) $a_i | a_{i-1} | \cdots | a_1$;

2) $g_j = h_j$ *for* $1 \leq j \leq i$ *and* $x^k g_l \in \mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_{l+k})$ *for any positive integers* l, k: $l + k \leq i$;

3) $\{g_1, \ldots, g_i\}$ *is a Gröbner basis for the* $\mathbb{Z}[x]$ *lattice* $(g_1, \ldots, g_i)$.

Proof. 1) Since $xg_l \in \mathrm{Span}_{\mathbb{Z}}(h_1, \ldots, h_l, h_{l+1})$, by Lemma 4.4 we have $b_{l+1} = \mathbf{LC}(h_{l+1}) | \mathbf{LC}(xg_l) = a_l$ for $1 \leq l \leq t-1$. Hence, $a_j = b_j | a_{j-1}$, $2 \leq j \leq i$ and $a_i | a_{i-1} | \cdots | a_1$ follows. The first statement is proved.

2) Since $\mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_i) \subseteq \mathrm{Span}_{\mathbb{Z}}(h_1, \ldots, h_i)$ and $a_j = b_j$ for $j: \ 1 \leq j \leq i$, by 2) of the Lemma 4.4, we have $g_j = h_j$ for $1 \leq j \leq i$.

For any positive integers l, k: $l + k \leq i$

$$\begin{aligned} xg_l &\in \mathrm{Span}_{\mathbb{Z}}(h_1, \ldots, h_{l+1}) = \mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_{l+1}) \\ x^2 g_l &\in \mathrm{Span}_{\mathbb{Z}}(xg_1, \ldots, xg_{l+1}) \subseteq \mathrm{Span}_{\mathbb{Z}}(h_1, \ldots, h_{l+2}) = \mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_{l+2}) \\ &\vdots \\ x^k g_l &\in \mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_{l+k}). \end{aligned}$$

3) For any $j, \ l: 1 \leq j < l \leq i$, $S(g_j, g_l) = \frac{a_j}{a_l} g_l - x^{l-j} g_j \in \mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_l)$. Considering that $\deg(g_1) < \cdots < \deg(g_l)$, we can easily say that $S(g_j, g_l)$ can be reduced to 0 by $\{g_1, \ldots, g_l\}$.

□

Lemma 4.8. *If* G_1 *and* G_2 *satisfy the* **Termination condition T**, *and* i *is the condition number, then*

1) $a_i | a_{i+1} | \cdots | a_t$;

2) $h_{k+1} \in \mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_i, xg_i, \ldots, xg_{k-1}, xg_k)$ *for* $i \leq k \leq t-1$

3) $\{g_1, \ldots, g_i\}$ *is a Gröbner basis for the* $\mathbb{Z}[x]$ *lattice* $(g_1, \ldots, g_t)$.

Proof. 1) Since $g_l \in \mathrm{Span}_{\mathbb{Z}}(h_1, \ldots, h_l)$, by Lemma 4.4 we have $b_l = \mathbf{LC}(h_l) | \mathbf{LC}(g_l) = a_l$ for any $l: \ 1 \leq l \leq t$. For $k: \ i \leq k < t$, $a_k = b_{k+1} | a_{k+1}$. Hence we have $a_i | a_{i+1} | \cdots | a_t$.

2) It is clear that $h_{i+1} - xg_i \in \mathrm{Span}_{\mathbb{Z}}(h_1, \ldots, h_i) = \mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_i)$. So, $h_{i+1} \in \mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_i, xg_i)$. Assume $h_l \in \mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_i, xg_i, \ldots, xg_{l-1})$ for $i+1 \leq l \leq k < t$. Since $h_{k+1} - xg_k \in \mathrm{Span}_{\mathbb{Z}}(h_1, \ldots, h_k) \subseteq \mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_i, xg_i, \ldots, xg_{k-1})$, we have $h_{k+1} \in \mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_i, xg_i, \ldots, xg_{k-1}, xg_k)$.

3) We only need to prove that for $i+1 \leq k < t$, g_k can be reduced to 0 by $\{g_1, \ldots, g_i\}$. For any $k: i+1 \leq k < t$, $g_{k+1} - \frac{a_{k+1}}{a_k} xg_k \in \mathrm{Span}_{\mathbb{Z}}(h_1, \ldots, h_k) = \mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_i, h_{i+1}, \ldots, h_k) \subseteq \mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_i, xg_i, \ldots, xg_{k-1})$. So $g_{k+1} \in \mathrm{Span}_{\mathbb{Z}}(g_1, \ldots, g_i, xg_i, \ldots, xg_k)$. It is obvious that g_{k+1} can be reduced to 0 by $\{g_1, \ldots, g_{k-1}, g_k\}$, *i.e.* g_{k+1} can be reduced to 0 by $\{g_1, \ldots, g_i\}$. Now we can say that $\{g_1, \ldots, g_i\}$ is a Gröbner basis for the $\mathbb{Z}[x]$ lattice $(g_1, \ldots, g_t)$. □

As a direct consequence of Lemma 4.7 and 4.8, we have

Theorem 4.9. *Algorithm* GHNF_1 *is correct and terminated.*

From the examples, we can see that the **Termination condition T** may not be achieved immediately when we obtain the Gröbner basis of F. The problem is that how many extra loops we need to do after we get the Gröbner basis of F.

If $\{g_1,\ldots,g_i\}$ is already the Gröbner basis of F for some $1 \le i \le t$, we have $a_i|a_{i-1}|\cdots|a_1$ and $b_j = a_j$ for $1 \le j \le i$. Moreover, $b_{i+1} = a_i$ since $b_{i+1}|a_i$. So, after one loop, we have $a_i|a_{i-1}|\cdots|a_1$ and $a_{i+1} = a_i$. After $t-i$ loops, we have $a_i|a_{i-1}|\cdots|a_1$ and $a_i = a_{i+1} = \cdots = a_t$. Until now, the **Termination condition T** holds. This is to say, our algorithm may do at most extra $t-i$ loops after we get the Gröbner basis of F. Since $\deg(g_t) = d$, we have $t \le d+1$. So we may do at most extra d loops after we get the Gröbner basis of F. By the analysis of Section 3, we can surely get the Gröbner basis after D_1-th loop, where $D_1 = 73d^5(h+\log d+1)$. Hence, the **Termination condition T** can be surely achieved in s-th loop, where $s \le D_1 + d$.

Corollary 4.10. *The Algorithm* GHNF_1 *terminates in* $D_1 + d$ *loops, where* $D_1 = 73d^5(h+\log d+1)$.

To estimate the complexity of algorithm GHNF_1, we need the complexity of computing HNF, which is given in the following theorem.

Theorem 4.11 ([19]). *Let* $A \in \mathbb{Z}^{n\times m}$ *with rank* r. *Then the complexity to compute the HNF of* H *is* $O(mnr^{\theta-2}(\log\beta)M(\log\log\beta)/\log\log\beta + mn\log rB(\log\beta))$, *where* $\beta = (\sqrt{r}\parallel A\parallel)^r$, $\parallel A\parallel$ *is the maximal absolute of* A.

Theorem 4.12. *The worst case bit size complexity of Algorithm* GHNF_1 *is* $O(d^{7+\theta+\varepsilon}(h+d)^{1+\varepsilon}(h+\log d) + d^{7+\varepsilon}(h+\log d)B(d^2(h+d)))$, *where* $h = \mathrm{height}(F)$ *and* $\varepsilon > 0$ *is any sufficiently small number.*

Proof. By Lemma 3.7, we know that the height bound for the GHNF of F is $(2d+1)(h+d\log 2+\log(d+1)) := h_1$. In each loop, we need to compute the Hermite normal form of an integer matrix with size $(d+1)\times s$ for some $s \le 2d+1$. Let $k = d+1, n = 2d+1, r = d+1$, then the $\log\beta$ in Lemma 4.11 is $\log\beta = r(\frac{1}{2}\log r + h_1) = O(d^2(h+d))$. To simplify the formula for the complexity bound, we replace $O(\log^2(s)\log\log(s)\log\log\log(s))$ by $O(s^\varepsilon)$ for an sufficiently small number ε, say $\varepsilon = 0.01$. Hence, the complexity for each loop is

$$\begin{aligned} &O(knr^{\theta-2}(\log\beta)M(\log\log\beta)/\log\log\beta + kn\log rB(\log\beta)) \\ &\le O(d^{2+\theta+\varepsilon}(h+d)^{1+\varepsilon} + d^{2+\varepsilon}B(d^2(h+d))) \text{ for any } \varepsilon > 0. \end{aligned}$$

So the worst complexity of the Algorithm GHNF_1 is $(D_1+d)O(d^{2+\theta+\varepsilon}(h+d)^{1+\varepsilon} + d^{2+\varepsilon}B(d^2(h+d))) = O(d^{7+\theta+\varepsilon}(h+d)^{1+\varepsilon}(h+\log d) + d^{7+\varepsilon}(h+\log d)B(d^2(h+d)))$. □

In Theorem 4.12, setting $\theta = 2.376$ and $\varepsilon = 0.004$ and noticing that $d^{7+\varepsilon}(h+\log d)B(d^2(h+d)))$ can be omitted now comparing to the first term, we have

Corollary 4.13. *The worst case bit size complexity of Algorithm* GHNF_1 *is* $O(d^{9.38}(h+d)^{1.004}(h+\log d))$.

Remark 4.14. *The number* m *in the input of Algorithm* GHNF_1 *is not in the complexity bound. The reason is that the size of the polynomial vector* F_1 *in Step 2 of the algorithm depends on* d *only. Only the complexity of Step 1 depends on* m *and by Theorem 4.11, the complexity of this step is* $O^\sim(md^{\theta+1}(h+d))$ *which is comparable to the complexity bound given in Theorem 4.12 only when* $m = O^\sim(d^6)$. *We therefore omit this term.*

Remark 4.15. *In Algorithm* GHNF_1, *to avoid the extra loops, we can check for* $k:\ i+1 \le k \le t$, *whether or not* g_k *can be reduced to 0 by* $\{g_1,\ldots,g_i\}$, *where* i *is the largest number such that* $a_j = b_j$ *for* $1 \le j \le i$.

Next, we show some properties of the syzygy modules of the $\mathbb{Z}[x]$ ideals. In the Algorithm GHNF$_1$, for any $i \geq 1$, denote by $G^{(i)} = [g_1^{(i)}, \ldots, g_{v_i}^{(i)}]$ and $F^{(i)}$ the G_1 and F_1 used in the i-th loop of the Algorithm GHNF$_1$, respectively. Here $v_i = \#(G^{(i)})$, then $\#(F^{(i)}) = 2v_i - 1 := v_i'$. Let $X^{(i)} = \begin{pmatrix} 1 & x & & & & \\ & 1 & x & & & \\ & & \ddots & & & \\ & & & 1 & x & \\ & & & & 1 & \end{pmatrix}_{v_i \times (2v_i-1)}$,

then $F^{(i)} = G^{(i)} X^{(i)}$. Since $\deg(g_1^{(i)}) < \cdots < \deg(g_{v_i}^{(i)}) = d$, we have $\deg(F^{(i)}) \leq d$. In particular, let $F^{(0)} = F$. For any $i \geq 0$, let $M^{(i)}$ be the coefficient matrix of $F^{(i)}$ and $[\mathbf{0}, H^{(i)}] = M^{(i)} U^{(i)}$ be the HNF of $M^{(i)}$, where $U^{(i)} = [U_1^{(i)}, U_2^{(i)}]$ satisfying $\mathbf{0} = M^{(i)} U_1^{(i)}$, $H^{(i)} = M^{(i)} U_2^{(i)}$. Then, $G^{(i+1)} = \mathrm{PHNF}(F^{(i)}) = F^{(i)} U_2^{(i)}$. We can express the loop in Algorithm GHNF$_1$ in the following diagram, which is equivalent to (16): (Denote by $v_0' = m$)

$$F^{(0)} \xrightarrow[\text{remove } 0]{U^{(0)} \in \mathbb{Z}^{v_0' \times v_0'}} G^{(1)} \xrightarrow{X^{(1)} \in \mathbb{Z}[x]^{v_1 \times v_1'}} F^{(1)} \xrightarrow[\text{remove } 0]{U^{(1)} \in \mathbb{Z}^{v_1' \times v_1'}} G^{(2)} \xrightarrow{X^{(2)} \in \mathbb{Z}[x]^{v_2 \times v_2'}} \cdots \tag{17}$$

For any $i \geq 1$, we define a function

$$\begin{aligned} \varphi_i : \mathbb{Z}[x]^{v_i'} &\to \mathbb{Z}[x]^m \\ \mathbf{u} &\mapsto U_2^{(0)} X^{(1)} \cdots U_2^{(i-1)} X^{(i)} \mathbf{u}. \end{aligned}$$

In particular, let $\varphi_0 : \mathbb{Z}[x]^m \to \mathbb{Z}[x]^m$ be the identity map. Then, for any $i \geq 0$, we have $F\varphi_i(U_1^{(i)}) = F^{(0)} U_2^{(0)} X^{(1)} \cdots U_2^{(i-1)} X^{(i)} U_1^{(i)} = F^{(i)} U_1^{(i)} = \mathbf{0}$, so, $\varphi_i(U_1^{(i)}) \subseteq \mathbf{Syz}(F)$. Note that $F\varphi_i(U_2^{(i)}) = G^{(i+1)}$.

We want to see when can we find a set of generators for the syzygy module $\mathbf{Syz}(F)$. First, we have the following lemma on the $\mathbb{Z}$ matrix:

Lemma 4.16. *[4] Let A be an $m \times n$ matrix over $\mathbb{Z}$, $H = AU$ its column Hermite normal form with $U \in \mathrm{GL}_n(\mathbb{Z})$, and let r be such that the first r columns of H are equal to $\mathbf{0}$. Then a $\mathbb{Z}$-basis for the kernel of A is given by the first r columns of U.*

Based on this, we have the following lemma:

Lemma 4.17. *For any $\mathbf{u} \in \mathbf{Syz}(F)$ and $\deg(\mathbf{u}) = k$, we have $\mathbf{u} \in \mathrm{Span}_{\mathbb{Z}}(\bigcup_{i=0}^{k} \varphi_i(U_1^{(i)}))$ for any $k > 0$. Moreover, $\{\bigcup_{i=0}^{d} \varphi_i(U_1^{(i)})\}$ generates the syzygy module $\mathbf{Syz}(F)$.*

Proof. By Lemma 3.19, $\mathbf{Syz}(F)$ can be generated by elements in $\mathbb{Z}[x]^m$ with degrees $\leq d$. We only need to show the first statement.

Clearly, we have $F^{(i)} = F U_2^{(0)} X^{(1)} \cdots U_2^{(i-1)} X^{(i)}$ for any $i > 0$. In particular, let $F^{(0)} = F$, $\mathbf{u}^{(0)'} = \mathbf{u}$.

By Lemma 4.16, the lemma is valid for $k = 0$. If $\deg(\mathbf{u}) = k > 0$, it suffices to show that, for any $0 \leq i \leq k$, there exists $\mathbf{u}^{(i)'} \in \mathbb{Z}[x]^{v_i'}$ with $\deg(\mathbf{u}^{(i)'}) \leq k - i$, such that $\mathbf{u} = \varphi_i(\mathbf{u}^{(i)'})$. In which case, $F^{(i)} \mathbf{u}^{(i)'} = F U_2^{(0)} X^{(1)} \cdots U_2^{(i-1)} X^{(i)} \mathbf{u}^{(i)'} = F\mathbf{u} = 0$. It is valid for $i = 0$. Suppose it is also valid for $1, \ldots, i-1$. Let $\mathbf{u}^{(i-1)'} \in \mathbb{Z}[x]^{v_{i-1}'}$ with $\deg(\mathbf{u}^{(i-1)'}) \leq k - i + 1$, such that $\mathbf{u} = \varphi_{i-1}(\mathbf{u}^{(i-1)'})$ and $F^{(i-1)} \mathbf{u}^{(i-1)'} = 0$. Let $\mathbf{u}^{(i)} = U_2^{(i-1)} \mathbf{u}^{(i-1)'}$, then $G^{(i)} \mathbf{u}^{(i)} = F^{(i-1)} U_2^{(i-1)} \mathbf{u}^{(i-1)'} = 0$. Let $\mathbf{u}^{(i)} = [u_1, \ldots, u_{v_i}]^\tau$, with $\deg(u_{v_i}) \leq k - i$ and $\deg(u_j) \leq k - i + 1$ for $1 \leq j < v_i$. Let

$$\begin{aligned} u_1 &= u_{1,0} + p_1 x, \\ &\vdots \\ u_{v_i - 1} &= u_{v_i - 1, 0} + p_{v_i - 1} x, \end{aligned}$$

where $u_{j,0} \in \mathbb{Z}$ and $p_j \in \mathbb{Z}[x]$ and $\deg(p_j) \le \deg(u_j) - 1 \le d - i$ for $1 \le j \le v_i - 1$. Take $\mathbf{u}^{(i)'} = [u_{1,0}, p_1, \ldots, u_{v_i-1,0}, p_{v_i-1}, u_{v_i}]^\tau$, then $\deg(\mathbf{u}^{(i)'}) \le d - i$ and $\mathbf{u}^{(i)} = X^{(i)}\mathbf{u}^{(i)'}$. Clearly, we have $F^{(i)}\mathbf{u}^{(i)'} = G^{(i)}X^{(i)}\mathbf{u}^{(i)'} = G^{(i)}\mathbf{u}^{(i)} = 0$. This lemma is proved. □

4.2 HNF-based algorithm-the $\mathbb{Z}[x]^n$ case

In this subsection, the GHNF$_n$ algorithm will be given to compute the GHNFs for modules in $\mathbb{Z}[x]^n$.

Given a polynomial matrix $F = (f_{ij})_{n\times m} = [\mathbf{f}_1, \ldots, \mathbf{f}_m] \in \mathbb{Z}[x]^{n\times m}$, denote by $m = \#(F)$ be the column number of F. Let $v_i = \max_{1\le j\le n}(\deg(f_{ij}))$,

$$X = \begin{pmatrix} 1 & x & \ldots & x^{v_1} & & & & & & \\ & & & & 1 & x & \ldots & x^{v_2} & & \\ & & & & & & & & \ddots & \\ & & & & & & & & 1 & x & \ldots & x^{v_n} \end{pmatrix}_{n\times s}, \tag{18}$$

where $s = \sum_{i=1}^{n}(v_i + 1)$. Let $F = XH$, we call the $H \in \mathbb{Z}^{s\times m}$ the coefficient matrix of F. Let H' be the Hermite normal form of H and $F' = XH'$. F' is called the PHNF of F. Denote by $H = M(F)$ and $F' = \text{PHNF}(F)$.

Denote by $F(\cdot, i)$ the i-th column of F, $F(i,\cdot)$ the i-th row of F. Denote by $\mathbf{f}(t)$ the polynomial in the t-th row of $\mathbf{f}$ for any polynomial vector $\mathbf{f}$.

Define the Algorithm Divide as follows: $(H_1, \ldots, H_n)$=Divide(G), where $G = [\mathbf{g}_1, \ldots, \mathbf{g}_s]$, $\mathbf{g}_t \in \mathbb{Z}[x]^n$, $H_t = [\mathbf{g}_{k_1}, \ldots, \mathbf{g}_{k_t}]$, where $1 \le k_1 < \cdots < k_t \le s$, $\mathbf{g}_k(t) \ne 0$ and $\mathbf{g}_k(j) = 0$ for any $k = k_i,\ j > t$.

The main algorithm is as following:

Algorithm 2 GHNF$_n(F)$

Input: $F = [\mathbf{f}_1, \ldots, \mathbf{f}_m]$, $\mathbf{f}_i \in \mathbb{Z}[x]^n$.

Output: $G = [\mathbf{g}_1, \ldots, \mathbf{g}_s]$, the GHNF of F.

1: $G_1 = \text{PHNF}(F)$, $i = 0$.

2: (loop) $i = i + 1$;
$(H_1, \ldots, H_n) = \text{Divide}(G_1)$, $H_j = [\mathbf{g}_{j,k_j}, \mathbf{g}_{j,k_j+1}, \ldots, \mathbf{g}_{j,s_j}]$ with $\deg(\mathbf{g}_{j,k}(j)) = k$ for $k_j \le k \le s_j$.
If $(t-1)d < i \le td$ for some $1 \le t \le n$, for j from 1 to $n-t$, let $\overline{H_j} = [H_j, xH_j]$, for j from $n-t$ to n, let $\overline{H_j} = [\mathbf{g}_{j,k_j}, \ldots, \mathbf{g}_{j,\min(s_j,(n-j+1)d)}, x\mathbf{g}_{j,k_j}, \ldots, x\mathbf{g}_{j,\min(s_j,(n-j+1)d)-1}]$.
If $i > nd$, for j from 1 to n, let $\overline{H_j} = [\mathbf{g}_{j,k_j}, \ldots, \mathbf{g}_{j,\min(s_j,(n-j+1)d)}, x\mathbf{g}_{j,k_j}, \ldots, x\mathbf{g}_{j,\min(s_j,(n-j+1)d)-1}]$.
Let $F_1 = [\overline{H_1}, \ldots, \overline{H_n}]$, $G_2 = \text{PHNF}(F_1)$. While G_1 and G_2 do not satisfy the **Termination condition T**$_n$ given below, let $G_1 = G_2$, repeat Step 2; otherwise, we obtain a polynomial matrix G_1, $(H_1, \ldots, H_n) = \text{Divide}(G_1)$, and a condition number set $[i_1, \ldots, i_n]$.

3: For t from 1 to n, let $H_t = [\mathbf{g}_1, \ldots, \mathbf{g}_t]$, $P_t = [\mathbf{g}_1]$;
for j from 2 to i_t, if $\mathbf{LC}(\mathbf{g}_{j-1}(t)) \nmid \mathbf{LC}(\mathbf{g}_j(t))$, $P_t = P_t \cup \{\mathbf{g}_j\}$.
Let $P_t = \overline{P_t}^{(P_1,\ldots,P_{t-1})}$.

4: $G = [P_1, \ldots, P_n]$.

5: Return G

Termination condition T$_n$: For polynomial matrices F and G, let $(H_1, \ldots, H_n) = \text{Divide}(F)$, $(P_1, \ldots, P_n) = \text{Divide}(G)$, for any $1 \le t \le n$ satisfying H_t is not empty, $H_t(t,\cdot)$ and $P_t(t,\cdot)$ satisfy the **Termination condition T**. Along with the **Termination condition T**$_n$, we define the condition number set $[i_1, \ldots, i_n]$ as follows: for $t = 1, \ldots, n$,

1) if H_t is not empty, i_t is the corresponding condition number;

2) if H_t is empty, define $i_t = 0$ to be the corresponding condition number.

Remark 4.18. *One may use* $\overline{H_j} = [\mathbf{g}_{j,k_j}, \ldots, \mathbf{g}_{j,\min(s_j,(n-j+1)d)}, x\mathbf{g}_{j,1}, \ldots, x\mathbf{g}_{j,\min(s_j,(n-j+1)d)-1}]$ *to replace the* $\overline{H_j}$ *in Step* 2 *of* GHNF_n *for any* $1 \le j \le n$. *Note that if the obtained* GHNF *(Gröbner basis) is as form (4) and* $p = \deg(c_{r_i,l_i}) < (n-r_i+1)d$, *one need not to multiply x to the* $\mathbf{g}_{r_i,s_{r_i}}$ *obtained in the loop since if something new arise from the syzygy of* F_{n-r_i+1}, *the* s_j *will renew automatically. Then, the correctness of this replacement is similar to the case of* $\mathbb{Z}[x]$.

Example 4.19. $F = \begin{pmatrix} 2x+1 & 3 & 4x^2 \\ 2 & 6x & 8 \\ 0 & 1 & 1 \end{pmatrix}$.

Step 1: $G_1 = \mathrm{PHNF}(F) = \begin{pmatrix} 2x+1 & -4x^2+8x+7 & 4x^2-8x-4 \\ 2 & 6x & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Step 2: 1*-th loop:* $(H_1, H_2, H_3) = \mathrm{Divide}(G_1)$, *where*

$H_1 = [\,]$, $H_2 = \begin{pmatrix} 2x+1 & -4x^2+8x+7 \\ 2 & 6x \\ 0 & 0 \end{pmatrix}$, $H_3 = \begin{pmatrix} 4x^2-8x-4 \\ 0 \\ 1 \end{pmatrix}$;

$H_1' = [\,]$, $H_2' = \begin{pmatrix} 2x+1 & -4x^2+8x+7 & 2x^2+x \\ 2 & 6x & 2x \\ 0 & 0 & 0 \end{pmatrix}$, $H_3' = \begin{pmatrix} 4x^2-8x-4 \\ 0 \\ 1 \end{pmatrix}$;

$F_2 = [H_1', H_2', H_3']$, $G_2 = \mathrm{PHNF}(F_2) = \begin{pmatrix} 10x^2-5x-7 & 2x+1 & 2x^2+x & 4x^2-8x-4 \\ 0 & 2 & 2x & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$;

G_1 *and* G_2 *do not satisfy the* **Termination condition** $\mathbf{T}_n$, $G_1 = G_2$.

2*-th loop:* $(H_1, H_2, H_3) = \mathrm{Divide}(G_1)$, *where*

$H_1 = \begin{pmatrix} 10x^2-5x-7 \\ 0 \\ 0 \end{pmatrix}$, $H_2 = \begin{pmatrix} 2x+1 & 2x^2+x \\ 2 & 2x \\ 0 & 0 \end{pmatrix}$, $H_3 = \begin{pmatrix} 4x^2-8x-4 \\ 0 \\ 1 \end{pmatrix}$;

$H_1' = H_1$, $H_2' = H_2$, $H_3' = H_3$, $F_2 = [H_1', H_2', H_3']$, *and* $G_2 = \mathrm{PHNF}(F_2) = F_2$. *Hence,* G_1 *and* G_2 *satisfy the* **Termination condition** $\mathbf{T}_n$ *and* $[1,2,1]$ *is the condition number set.*

Step 3: $P_1 = \begin{pmatrix} 10x^2-5x-7 \\ 0 \\ 0 \end{pmatrix}$, $P_2 = \begin{pmatrix} 2x+1 \\ 2 \\ 0 \end{pmatrix}$, $P_3 = \begin{pmatrix} 4x^2-8x-4 \\ 0 \\ 1 \end{pmatrix}$.

Step 4: The GHNF *of* F *is* $G = \begin{pmatrix} 10x^2-5x-7 & 2x+1 & 4x^2-8x-4 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

In the Algorithm GHNF_n, for any $i \ge 1$, denote by $G^{(i)}$ and $F^{(i)}$ the G_1 and F_1 in the i-th loop, respectively. Let $\nu_i = \#(G^{(i)})$, $\nu_i' = \#(F^{(i)})$. For the i-th loop of the Algorithm GHNF_n, let $(H_1^{(i)}, \ldots, H_n^{(i)}) = \mathrm{Divide}(G^{(i)})$ and $H_j^{(i)} = [\mathbf{g}_{j,k_j}^{(i)}, \mathbf{g}_{j,k_j+1}^{(i)}, \ldots, \mathbf{g}_{j,s_j}^{(i)}]$ with $\deg(\mathbf{g}_{j,k}^{(i)}(k)) = k$ for $k_j \le k \le s_j$. For $1 \le j \le n$, denote by $t_j^{(i)} = \#([\mathbf{g}_{j,k_j}^{(i)}, \ldots, \mathbf{g}_{j,\min(s_j,(n-j+1)d)}^{(i)}]) \ge 0$ and $t_j^{(i)'} = \max(0, \#([\mathbf{g}_{j,(n-j+1)d+1}^{(i)}, \ldots, \mathbf{g}_{j,s_j}^{(i)}]))$. Let $X^{(i)} = \mathrm{DiagonalMatrix}(X_1^{(i)}, \ldots, X_n^{(i)})$ be the diagonal matrix with blocks $X_k^{(i)}, 1 \le k \le n$, where $X_j^{(i)} = [\,]$ if $t_j^{(i)} = 0$, otherwise,

$$X_j^{(i)} = \begin{pmatrix} \begin{pmatrix} 1 & x & & \\ & \ddots & & \\ & & 1 & x \\ & & & 1 \end{pmatrix}_{t_j^{(i)} \times (2t_j^{(i)}-1)} \\ \mathbf{0}_{t_j^{(i)'} \times (2t_j^{(i)}-1)} \end{pmatrix} \text{ when } i > (n-j)d, \tag{19}$$

and

$$X_j^{(i)} = \begin{pmatrix} 1 & x & & \\ & \ddots & & \\ & & 1 & x \end{pmatrix}_{t_j^{(i)} \times 2t_j^{(i)}} \quad \text{when } i \le (n-j)d. \tag{20}$$

In particular, let $F^{(0)} = F$. For $i \ge 0$, let $M^{(i)}$ be the coefficient matrix of $F^{(i)}$ and $[\mathbf{0}, H^{(i)}] = M^{(i)}U^{(i)}$ be the HNF of $M^{(i)}$, where $U^{(i)} = [U_1^{(i)}, U_2^{(i)}]$ satisfying $\mathbf{0} = M^{(i)}U_1^{(i)}$, $H^{(i)} = M^{(i)}U_2^{(i)}$. Then $G^{(i+1)} = \text{PHNF}(F^{(i)}) = F^{(i)}U_2^{(i)}$.

The loop can be expressed as the following diagram:

$$\text{loop}_n : F \xrightarrow[\text{remove } \mathbf{0}]{U^{(0)} \in \mathbb{Z}^{\nu_0' \times \nu_0'}} G^{(1)} \xrightarrow{X^{(1)} \in \mathbb{Z}[x]^{\nu_1 \times \nu_1'}} F^{(1)} \xrightarrow[\text{remove } \mathbf{0}]{U^{(1)} \in \mathbb{Z}^{\nu_1' \times \nu_1'}} G^{(2)} \xrightarrow{X^{(2)} \in \mathbb{Z}[x]^{\nu_2 \times \nu_2'}} \cdots$$

Similar to the above loop$'$, we give the following loop$'_n$:

$$\text{loop}'_n : F \xrightarrow[\text{remove } \mathbf{0}]{U^{(0)}} G^{(1)} \xrightarrow{\text{add } xG^{(1)}} F^{(1)'} \xrightarrow[\text{remove } \mathbf{0}]{U^{(1)'}} G^{(2)'} \xrightarrow{\text{add } xG^{(2)'}} \cdots$$

Let $(H_1^{(i)}, \ldots, H_n^{(i)}) = \text{Divide}(G^{(i)})$, and $(H_1^{(i)'}, \ldots, H_n^{(i)'}) = \text{Divide}(G^{(i)'})$. Without loss of generality, we assume $t_j^{(i)} > 0$ for $1 \le j \le n$. For simplicity, denote by $H_j^{(i)} = [\mathbf{g}_{j,k_j}^{(i)}, \mathbf{g}_{j,k_j+1}^{(i)}, \ldots, \mathbf{g}_{j,s_j}^{(i)}]$, $H_j^{(i)'} = [\mathbf{g}_{j,k_j'}^{(i)'}, \mathbf{g}_{j,k_j'+1}^{(i)'}, \ldots, \mathbf{g}_{j,s_j'}^{(i)'}]$ for $1 \le j \le n$, where $\deg(\mathbf{g}_{j,k}^{(i)}(j)) = \deg(\mathbf{g}_{j,k}^{(i)'}(j)) = k$. Then, $F^{(i)} = [\overline{H_1^{(i)}}, \ldots, \overline{H_n^{(i)}}]$, where $\overline{H_j^{(i)}} = H_j^{(i)}X_j^{(i)} = [H_j^{(i)}, xH_j^{(i)}]$ if $i \le (n-j)d$, $\overline{H_j^{(i)}} = H_j^{(i)}X_j^{(i)} = [\mathbf{g}_{j,k_j}^{(i)}, \ldots, \mathbf{g}_{j,s_j}^{(i)}, x\mathbf{g}_{j,k_j}^{(i)}, \ldots, x\mathbf{g}_{j,s_j-1}^{(i)}]$ if $i > (n-j)d$. And $F^{(i)'} = [\overline{H_1^{(i)'}}, \ldots, \overline{H_n^{(i)'}}]$, where $\overline{H_j^{(i)'}} = [H_j^{(i)'}, xH_j^{(i)'}]$ for $1 \le j \le n$. Let $P_j^{(i)'} = [\mathbf{g}_{j,k_j'}^{(i)'}, \ldots, \mathbf{g}_{j,\min(s_j', (n-j+1)d)}^{(i)'}, x\mathbf{g}_{j,k_j'}^{(i)'}, \ldots, x\mathbf{g}_{j,s_j'}^{(i)'}]$ for $1 \le j \le n$.

In order to show the the equivalence of loop$_n$ and loop$'_n$ for computing the GHNF, we define another order as followings: $x^\alpha \mathbf{e}_i \prec' x^\beta \mathbf{e}_j$ if and only if $\alpha < \beta$ or $\alpha = \beta$, $i < j$. Similar to the order $\prec$, the order $\prec'$ can be extended to the polynomial vectors of $\mathbb{Z}[x]^n$. Moreover, let $\mathbf{f}, \mathbf{g} \in \mathbb{Z}[x]^m$, the S-vector of $\mathbf{f}, \mathbf{g}$ is the same with the order $\prec$. A good property of the order $\prec'$ is: if $\max(\deg(\mathbf{f}), \deg(\mathbf{g})) \le d$, then $\deg(S_{\prec'}(\mathbf{f}, \mathbf{g})) \le d$. We can easily get the following lemma:

Lemma 4.20. *Let $F \in \mathbb{Z}[x]^{n \times m}$, $d = \deg(F)$, then $\mathbf{Syz}(F)$ has a Gröbner basis G with degree $\le nd$ w.r.t. $\prec'$.*

Proof. Let $S = \{\mathbf{u} | \mathbf{u} \in \mathbf{Syz}(F),\ \deg(\mathbf{u}) \le nd\}$, then, S has a Gröbner basis $G \subseteq S$ since the S-vector of any $\mathbf{u}, \mathbf{v} \in S$ *w.r.t.* $\prec'$ is also in S. By Lemma 3.19, S generates $\mathbf{Syz}(F)$. The lemma is proved. □

Let F_t be the last t rows of F, $S_t = \{\mathbf{u} \in \mathbb{Z}[x]^m | \mathbf{u} \in \mathbf{Syz}(F_t), \deg(\mathbf{u}) \le td\}$. By Lemma 4.20, S_t has a Gröbner basis $G_t \subseteq S_t$ and $\deg(G_t) \le td$. For any $\mathbf{u} \in \mathbf{Syz}(F_t)$ with $\deg(\mathbf{u}) \le k$, $\mathbf{u} \in \text{Span}_{\mathbb{Z}}(S_t, xS_t, \ldots, x^{\max(0,\ k-td)}S_t)$. Moreover, we have $(S_1) \supseteq (S_2) \supseteq \cdots \supseteq (S_n)$.

Similar to the $\mathbb{Z}[x]$ case, for the loop$_n$, we define a sequence of maps ϕ_i:

For each $i > 0$, let $U^{(i)} = [V_1^{(i)}, V_2^{(i)}]$, where $V_1^{(i)}$ consists of column vectors of $U^{(i)} \cap \mathbf{Syz}(F_1)$, $\overline{H_n^{(i)}}V_2^{(i)} = H_n^{(i)}X_n^{(i)}V_2^{(i)} = H_n^{(i+1)}$. Let

$$\begin{aligned} \phi_i : \mathbb{Z}[x]^{\#(X_n^{(i)})} &\to \mathbb{Z}[x]^m \\ \mathbf{u} &\mapsto V_2^{(0)}X_n^{(1)} \cdots V_2^{(i-1)}X_n^{(i)}\mathbf{u}. \end{aligned}$$

In particular, let $\phi_0 : \mathbb{Z}[x]^m \to \mathbb{Z}[x]^m$ be the identity map. Thus, $FV_2^{(0)}X_n^{(1)} \cdots V_2^{(i-1)}X_n^{(i)}V_2^{(i)} = H_n^{(i+1)}$ and $F\phi_i(V_1^{(i)}) = FV_2^{(0)}X_n^{(1)} \cdots V_2^{(i-1)}X_n^{(i)}V_1^{(i)} \subseteq \text{Span}_{\mathbb{Z}}(H_1^{(i+1)}, \ldots, H_{n-1}^{(i+1)})$ for each $0 \le i \le d$.

Lemma 4.21. *Let $F \in \mathbb{Z}[x]^{n\times m}$. For any $\mathbf{u} \in \mathbf{Syz}(F_1)$ and $\deg(\mathbf{u}) = k$, we have $\mathbf{u} \in \mathrm{Span}_{\mathbb{Z}}(\bigcup_{i=0}^{l} \phi_i(V_1^{(i)}))$ for any $k > 0$.*

Proof. This is similar to the proof of Lemma 4.17. □

Lemma 4.22. *For any $1 \le t \le n$ and $k \le td+1$, we have $H_j^{(k)} = H_j^{(k)'}$ for $1 \le j \le n-t$.*

Proof. First, let $t = 1$. In the loop$_n$ and loop$'_n$, $G^{(1)} = G^{(1)'} = FU_2^{(0)}$. Then, $H_j^{(1)} = H_j^{(1)'}$ for $1 \le j \le n$. This lemma is valid for $k = 1$. Suppose it is valid for $k = l \le d$, *i.e.*, $H_j^{(l)} = H_j^{(l)'}$ for $1 \le j \le n-1$. We need to show $H_j^{(l+1)} = H_j^{(l+1)'}$ for $1 \le j \le n-1$. For any $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(H_1^{(l+1)'}, \ldots, H_{n-1}^{(l+1)'}) \subset \mathrm{Span}_{\mathbb{Z}}(F^{(l)'}) = \mathrm{Span}_{\mathbb{Z}}(F, xF, \ldots, x^lF)$, there exists a $\mathbf{u} \in \mathbb{Z}[x]^m$, such that $\mathbf{f} = F\mathbf{u}$ with $\deg(\mathbf{u}) \le l$, and $\mathbf{u} \in \mathbf{Syz}(F_1)$. By Lemma 4.21, we have $\mathbf{u} \in \mathrm{Span}_{\mathbb{Z}}(\bigcup_{i=0}^{l} \phi_i(V_1^{(i)}))$. Then, $\mathbf{f} = F\mathbf{u} \in \mathrm{Span}_{\mathbb{Z}}(H_1^{(l+1)}, \ldots, H_{n-1}^{(l+1)})$. Thus, we have $H_j^{(l+1)} = H_j^{(l+1)'}$ for $1 \le j \le n-1$. The lemma is valid for $t = 1$.

Suppose the lemma is valid for $t = p-1$. Then we have $H_j^{((p-1)d+1)} = H_j^{((p-1)d+1)'}$ for $1 \le j \le n-p+1$. $FS_{p-1} \subseteq \mathrm{Span}_{\mathbb{Z}}(H_1^{((p-1)d+1)'}, \ldots, H_{n-p+1}^{((p-1)d+1)'}) = \mathrm{Span}_{\mathbb{Z}}(Q)$, where $Q = [H_1^{((p-1)d+1)}, \ldots, H_{n-p+1}^{((p-1)d+1)}]$.

When $t = p$, for any $(p-1)d+1 < k \le pd+1$ and $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(H_1^{(k)'}, \ldots, H_{n-p}^{(k)'}) \subseteq \mathrm{Span}_{\mathbb{Z}}(F^{(k-1)'})$, there exists a $\mathbf{u} \in \mathbb{Z}[x]^m$ with $\deg(\mathbf{u}) \le k-1$, such that $\mathbf{f} = F\mathbf{u}$ and $\mathbf{u} \in \mathbf{Syz}(F_p) \subseteq \mathbf{Syz}(F_{p-1})$. By Lemma 4.20, $\mathbf{u} \in \mathbf{Syz}(F_p) = (S_{p-1})$, hence we have $u \in \mathrm{Span}_{\mathbb{Z}}(S_{p-1}, \ldots, x^{k-(p-1)d-1}S_p)$. Then, $\mathbf{f} = F\mathbf{u} \in \mathrm{Span}_{\mathbb{Z}}(Q, \ldots, x^{k-(p-1)d-1}Q)$. Hence we have $\mathbf{f} = Q\mathbf{v}$ for some $v \in \mathbf{Syz}(Q_p)$ with $\deg(\mathbf{v}) \le k-(p-1)d-1$ and Q_p being the last p rows of Q. Consider the algorithm GHNF$_n(Q)$, we have $\mathrm{Span}_{\mathbb{Z}}(Q^{(i)}) \subseteq \mathrm{Span}_{\mathbb{Z}}(H_1^{((p-1)d+1+i)}, \ldots, H_{n-p+1}^{((p-1)d+1+i)})$ for $i \le d$. Then, $\mathrm{Span}_{\mathbb{Z}}(Q^{(k-(p-1)d-1)}) \subset \mathrm{Span}_{\mathbb{Z}}(H_1^{(k)}, \ldots, H_{n-p+1}^{(k)})$. Since the last $p-1$ rows of Q are all zeros, it can be reduced to the $t = 1$ case. Hence, we have $\mathbf{f} = Q\mathbf{v} \in \mathrm{Span}_{\mathbb{Z}}(Q^{(k-(p-1)d-1)})$. Thus, $H_j^{(k)} = H_j^{(k)'}$ for $1 \le j \le n-p$. □

Lemma 4.23. *Let $H = [H_1^{(td+1)}, \ldots, H_{n-t}^{(td+1)}]$. For $k > td+1$, $0 \le t \le n-1$, we have $H_{n-t}^{(k)'} \subseteq (H_1^{(td+1)}, \ldots, H_{n-t}^{(td+1)})$. In particular, for $k > td+1$, $0 \le t \le n-1$, $H_{n-t}^{(k)'} \subseteq \mathrm{Span}_{\mathbb{Z}}(H, xH, \ldots, x^{k-td-1}H) \subseteq \mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(k-1)'}}, \ldots, \overline{H_{n-t}^{(k-1)'}})$.*

Proof. Let $k > td+1$. For any $\mathbf{f} \in H_{n-t}^{(k)'} \subseteq \mathrm{Span}_{\mathbb{Z}}(F^{(k-1)'})$, there exists a $\mathbf{u} \in \mathbf{Syz}(F_t)$ with $\deg(\mathbf{u}) \le k-1$, such that $\mathbf{f} = F\mathbf{u}$. By Lemma 3.19, $\mathbf{u} \in (S_t)$. By Lemma 4.20, $\mathbf{u} \in \mathrm{Span}_{\mathbb{Z}}(S_t, \ldots, x^{k-td-1}S_t)$. By Lemma 4.22, $H_j^{(td+1)} = H_j^{(td+1)'}$ for $1 \le j \le n-t$, $1 \le t \le n$. Then, $FS_t \subseteq \mathrm{Span}_{\mathbb{Z}}(H_1^{(td+1)'}, \ldots, H_{n-t}^{(td+1)'})) = \mathrm{Span}_{\mathbb{Z}}(H)$. Thus, $\mathbf{f} = F\mathbf{u} \subseteq \mathrm{Span}_{\mathbb{Z}}(H, xH, \ldots, x^{k-td-1}H) \subseteq (H)$.

To show the second statement, first, let $k = td+2$. Then, $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(H, xH) = \mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(td+1)'}}, \ldots, \overline{H_{n-t}^{(td+1)'}}))$. The, lemma is valid for $k = td+2$. Suppose the lemma is valid for $k = l > td+2$. Then, $H_{n-t}^{(l)'} \subseteq \mathrm{Span}_{\mathbb{Z}}(H, xH, \ldots, x^{l-td-1}H) \subseteq \mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(l-1)'}}, \ldots, \overline{H_{n-t}^{(l-1)'}}) \subseteq \mathrm{Span}_{\mathbb{Z}}(H_1^{(l)'}, \ldots, H_{n-t}^{(l)'})$. We need to show $H_{n-t}^{(l+1)'} \subseteq \mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(l)'}}, \ldots, \overline{H_{n-t}^{(l)'}})$. For any $\mathbf{f} \in H_{n-t}^{(l+1)'}$, $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(H, xH, \ldots, x^{l-td}H) = \mathrm{Span}_{\mathbb{Z}}(\mathrm{Span}_{\mathbb{Z}}(H, xH, \ldots, x^{l-td-1}H) \cup x\mathrm{Span}_{\mathbb{Z}}(H, xH, x^{l-td-1}H)) \subseteq \mathrm{Span}_{\mathbb{Z}}(H_1^{(l)'}, \ldots, H_{n-t}^{(l)'}, xH_1^{(l)'}, \ldots, xH_{n-t}^{(l)'}) = \mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(l)'}}, \ldots, \overline{H_{n-t}^{(l)'}})$. The lemma is also valid for $k = l+1$. □

Lemma 4.24. $\mathrm{Span}_{\mathbb{Z}}(G^{(k+1)'}) = \mathrm{Span}_{\mathbb{Z}}(F^{(k)'}) = \mathrm{Span}_{\mathbb{Z}}(P_1^{(k)'}, \ldots, P_n^{(k)'})$ *for any $k > 0$.*

Proof. We claim that $\mathbf{f} = [f_1, \ldots, f_{n-t}, 0, \ldots, 0]^\tau \in \mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(k)'}}, \ldots, \overline{H_{n-t}^{(k)'}})$, implies $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(P_1^{(k)'}, \ldots, P_{n-t}^{(k)'})$.

First, let $t = n-1$. If $k \le (n-1)d$, we have $P_1^{(k)'} = \overline{H_1^{(k)'}}$.Then, $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(k)'}}) = \mathrm{Span}_{\mathbb{Z}}(P_1^{(k)'})$. Otherwise, $k > (n-1)d$, by Lemma 4.23, $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(k)'}}) \subseteq (H_1^{((n-1)d+1)})$. By Lemma 4.5, $\mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(k)'}}) = \mathrm{Span}_{\mathbb{Z}}(P_1^{(k)'})$. The lemma is valid for $t = n-1$.

Suppose the claim is valid for $t = l+1 \le n-1$, *i.e.* for any $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(k)'}}, \ldots, \overline{H_{n-l-1}^{(k)'}})$ and $k > 0$, $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(P_1^{(k)'}, \ldots, P_{n-l-1}^{(k)'})$.

Let $t = l$, $\mathbf{f} = [f_1, \ldots, f_{n-l}, 0, \ldots, 0]^\tau \in \mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(k)'}}, \ldots, \overline{H_{n-l}^{(k)'}})$. If $k \le ld$, then, $P_j^{(k)'} = \overline{H_j^{(k)'}}$ for $1 \le j \le n-l$. Thus, $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(P_1^{(k)'}, \ldots, P_{n-l}^{(k)'})$. Otherwise, $k > ld$. If $f_{n-l} = 0$, $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(H_1^{(k+1)'}, \ldots, H_{n-l-1}^{(k+1)'})$. If $k \le (l+1)d$, $P_j^{(k)'} = \overline{H_j^{(k)'}} = \overline{H_j^{(k)}}$ for $1 \le j \le n-l-1$ be Lemma 4.22. $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(k)'}}, \ldots, \overline{H_{n-l}^{(k)'}}) = \mathrm{Span}_{\mathbb{Z}}(P_1^{(k)'}, \ldots, P_{n-l-1}^{(k)'}, \overline{H_{n-l}^{(k)'}}) \subseteq \mathrm{Span}_{\mathbb{Z}}(P_1^{(k)'}, \ldots, P_{n-l}^{(k)'})$ by Lemma 4.21. If $k > (l+1)d$, by Lemma 4.23, $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(k)'}}, \ldots, \overline{H_{n-l-1}^{(k)'}})$. By induction, $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(P_1^{(k)'}, \ldots, P_{n-l-1}^{(k)'})$. If $f_{n-l} \ne 0$, $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(k)'}}, \ldots, \overline{H_{n-l}^{(k)'}}) \subseteq (H_1^{(ld+1)}, \ldots, H_{n-l}^{(ld+1)})$ be Lemma 4.23. Then, $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(k)'}}, \ldots, \overline{H_{n-l-1}^{(k)'}}, P_{n-l}^{(k)'})$ for $k > ld$, by Lemma 4.21. Thus, by induction, $\mathbf{f} \in \mathrm{Span}_{\mathbb{Z}}(P_1^{(k+1)'}, \ldots, P_{n-l}^{(k+1)'})$. The claim is proved. We have $\mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(k)'}}, \ldots, \overline{H_n^{(k)'}}) \subseteq \mathrm{Span}_{\mathbb{Z}}(P_1^{(k)'}, \ldots, P_n^{(k)'})$. Since $\mathrm{Span}_{\mathbb{Z}}(P_1^{(k)'}, \ldots, P_n^{(k)'}) \subseteq \mathrm{Span}_{\mathbb{Z}}(\overline{H_1^{(k)'}}, \ldots, \overline{H_n^{(k)'}}) = \mathrm{Span}_{\mathbb{Z}}(G^{(k+1)'}) = \mathrm{Span}_{\mathbb{Z}}(F^{(k)'})$. The lemma is valid. □

Lemma 4.25. *loop$_n$ and loop$'_n$ are equivalent for computing the* GHNF.

Proof. By Lemma 4.24, $[\mathbf{g} \in H_t^{(i)'} : \deg(\mathbf{g}(t)) \le (n-t)d] = H_t^{(i)}$ for any t and i. When we check the **Termination condition $\mathbf{T}_n$** in two different procedures loop$_n$ and loop$'_n$, they terminate at the same time. □

From now on, let G_1 and G_2 be the outputs of the Step 2, $(H_1, \ldots, H_n) = \mathrm{Divide}(G_1)$, $(H'_1, \ldots, H'_n) = \mathrm{Divide}(G_2)$. Similar to the $\mathbb{Z}[x]$ case, to prove the correctness of this algorithm, we assume $\#H_t = \#H'_t$. Denote by $H_t = [\mathbf{g}_{t,1}, \ldots, \mathbf{g}_{t,k_t}]$, $H'_t = [\mathbf{h}_{t,1}, \ldots, \mathbf{h}_{t,k_t}]$ and $\mathbf{LC}(H_t(t,\cdot)) = [a_{t,1}, \ldots, a_{t,k_t}]$, $\mathbf{LC}(H'_t(t,\cdot)) = [b_{t,1}, \ldots, b_{t,k_t}]$. Let $L_t = \{\mathbf{g}_{t,1}, \ldots, \mathbf{g}_{t,k_t}\}$, $L'_t = \{\mathbf{h}_{t,1}, \ldots, \mathbf{h}_{t,k_t}\}$ for $1 \le t \le n$.

Lemma 4.26. *For the above G_1 and G_2, if there exists a set of number $[i_1, \ldots, i_n]$, such that $a_{t,j} = b_{t,j}$ for $1 \le j \le i_t$, $1 \le t \le n$, then*

1) $a_{t,i_t} | a_{t,i_t-1} | \cdots | a_{t,1}$ *for* $1 \le t \le n$;

2) $\mathbf{g}_{t,j} = \mathbf{h}_{t,j} \mod \mathrm{Span}_{\mathbb{Z}}(L'_1, \ldots, L'_{t-1})$ *for* $1 \le j \le i_t$, $2 \le t \le n$.
Moreover, $x^k \mathbf{g}_{t,l} \in \mathrm{Span}_{\mathbb{Z}}(\bigcup_{j=1}^{t-1} L'_j, x\bigcup_{j=1}^{t-1} L'_j, \ldots, x^{k-1}\bigcup_{j=1}^{t-1} L'_j, \mathbf{g}_{t,1}, \ldots, \mathbf{g}_{t,l+k})$ *for any positive integers* $k, l:\ k+l \le i_t$, $1 \le t \le n$;

Proof. 1) By Lemma 4.7, 1) is valid for $1 \le t \le n$.

2) For $1 \le t \le n$, $1 \le j \le i_t$, let $g_{t,j}$, $h_{t,j}$ be the t-th elements of $\mathbf{g}_{t,j}$, $\mathbf{h}_{t,j}$ respectively. Then, we have $\mathrm{Span}_{\mathbb{Z}}(g_{t,1}, \ldots, g_{t,i_t}) \subseteq \mathrm{Span}_{\mathbb{Z}}(h_{t,1}, \ldots, h_{t,i_t})$ and $\mathbf{LC}([g_{t,1}, \ldots, g_{t,i_t}]) = \mathbf{LC}([h_{t,1}, \ldots, h_{t,i_t}])$ for $1 \le t \le n$. By Lemma 4.4, we have $g_{t,j} = h_{t,j}$ for $1 \le j \le i_t$, $1 \le t \le n$. So, $\mathbf{h}_{t,j} - \mathbf{g}_{t,j} \in \mathrm{Span}_{\mathbb{Z}}(L'_1, \ldots, L'_{t-1})$, *i.e.* $\mathbf{g}_{t,j} = \mathbf{h}_{t,j} \mod \mathrm{Span}_{\mathbb{Z}}(L'_1, \ldots, L'_{t-1})$ for $1 \le j \le i_t$, $2 \le t \le n$.

For any t, such that L_t is not empty, we have

$$
\begin{aligned}
x\mathbf{g}_{t,l} &\in \mathrm{Span}_{\mathbb{Z}}(\bigcup_{t=1}^{r-1} L'_t, \mathbf{h}_{t,1}, \ldots, \mathbf{h}_{t,l+1}) = \mathrm{Span}_{\mathbb{Z}}(\bigcup_{t=1}^{r-1} L'_t, \mathbf{g}_{t,1}, \ldots, \mathbf{g}_{t,l+1}), \text{ for } 1 \le l \le i_t - 1;\\
x^2\mathbf{g}_{t,l} &\in \mathrm{Span}_{\mathbb{Z}}(x\bigcup_{t=1}^{r-1} L'_t, x\mathbf{g}_{t,1}, \ldots, x\mathbf{g}_{t,l+1}) \subseteq \mathrm{Span}_{\mathbb{Z}}(\bigcup_{t=1}^{r-1} L'_t, x\bigcup_{t=1}^{r-1} L'_t, \mathbf{g}_{t,1}, \ldots, \mathbf{g}_{t,l+2}), \text{ for } 1 \le l \le i_t - 2;\\
&\vdots\\
x^k\mathbf{g}_{t,l} &\in \mathrm{Span}_{\mathbb{Z}}(\bigcup_{t=1}^{r-1} L'_t, x\bigcup_{t=1}^{r-1} L'_t, \ldots, x^{k-1}\bigcup_{t=1}^{r-1} L'_t, \mathbf{g}_{t,1}, \ldots, \mathbf{g}_{t,l+k}), \text{ for } 1 \le l \le i_t - k;.
\end{aligned}
$$

□

Lemma 4.27. *When the* **Termination condition** $\mathbf{T}_n$ *holds and* $[i_1,\ldots,i_n]$ *is the condition number set, then,*

1) $a_{t,i_t}|a_{t,i_t+1}|\cdots|a_{t,k_t}$ *for* $1\le t\le n$*;*

2) $\mathbf{h}_{t,l}\in \mathrm{Span}_{\mathbb{Z}}(L'_1,\ldots,L'_{t-1},\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t},x\mathbf{g}_{t,i_t},x\mathbf{g}_{t,i_t+1},\ldots,x\mathbf{g}_{t,l-1})$ *for* $i_t<l\le k_t$, $1\le t\le n$*;*

3) $\bigcup_{t=1}^n\{\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t}\}$ *is a Gröbner basis for the* $\mathbb{Z}[x]$ *lattice* $(\bigcup_{t=1}^n L_t)$.

Proof. 1) By Lemma 4.8, 1) is valid for $1\le t\le n$.

2) For any t, $\mathbf{h}_{t,i_t+1}-x\mathbf{g}_{t,i_t}\in \mathrm{Span}_{\mathbb{Z}}(L'_1,\ldots,L'_{t-1},\mathbf{h}_{t,1},\ldots,\mathbf{h}_{t,i_t})=\mathrm{Span}_{\mathbb{Z}}(L'_1,\ldots,L'_{t-1},\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t})$. So, $\mathbf{h}_{t,i_t+1}\in \mathrm{Span}_{\mathbb{Z}}(L'_1,\ldots,L'_{t-1},\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t},x\mathbf{g}_{t,i_t})$. Suppose 2) is valid for $i_t<j\le l-1$. Then, $\mathbf{h}_{t,l}-x\mathbf{g}_{t,l-1}\in \mathrm{Span}_{\mathbb{Z}}(L'_1,\ldots,L'_{t-1},\mathbf{h}_{t,1},\ldots,\mathbf{h}_{t,l-1})\subseteq \mathrm{Span}_{\mathbb{Z}}(L'_1\ldots,L'_{t-1},\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t},x\mathbf{g}_{t,i_t},\ldots,x\mathbf{g}_{t,l-2})$. So, we have $\mathbf{h}_{t,l}\in \mathrm{Span}_{\mathbb{Z}}(L'_1\ldots,L'_{t-1},\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t},x\mathbf{g}_{t,i_t},\ldots,x\mathbf{g}_{t,l-2},x\mathbf{g}_{t,l-1})$, which is valid for $i_t<l\le k_t$, $1\le t\le n$.

3) We prove this by induction. Without loss of generality, we assume L_1 is not empty. By Lemma 4.8, $\{\mathbf{g}_{1,1},\ldots,\mathbf{g}_{1,i_1}\}$ is a Gröbner basis for the $\mathbb{Z}[x]$ lattice (L_1). Suppose $\bigcup_{t=1}^{r-1}\{\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t}\}$ is a Gröbner basis for the $\mathbb{Z}[x]$ lattice of $(\bigcup_{t=1}^{r-1}L_t)$. We need to show that $\bigcup_{t=1}^{r}\{\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t}\}$ is a Gröbner basis for the $\mathbb{Z}[x]$ lattice of $(\bigcup_{t=1}^{r}\{\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t}\})$ and $\mathbf{g}_{r,l}$ can be reduced to $\mathbf{0}$ by $\bigcup_{t=1}^{r}\{\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t}\}$ for $i_r<l\le k_r$.

By Lemma 4.26, $S(\mathbf{g}_{r,k},\mathbf{g}_{r,l})=\frac{a_{r,k}}{a_{r,l}}\mathbf{g}_{r,l}-x^{l-k}\mathbf{g}_{r,k}\in \mathrm{Span}_{\mathbb{Z}}(\bigcup_{t=1}^{r-1}L'_t,x\bigcup_{t=1}^{r-1}L'_t,\ldots,x^{l-k-1}\bigcup_{t=1}^{r-1}L'_t,\mathbf{g}_{r,1},\ldots,\mathbf{g}_{r,l})$ for any $1\le k<l\le i_r$. So, there exists a sequence of integers $u_1,\ldots,u_l$, such that

$$S(\mathbf{g}_{r,k},\mathbf{g}_{r,l})-(u_1\mathbf{g}_{r,1}+\cdots+u_l\mathbf{g}_{r,l})\in \mathrm{Span}_{\mathbb{Z}}(\bigcup_{t=1}^{r-1}L'_t,x\bigcup_{t=1}^{r-1}L'_t,\ldots,x^{l-k-1}\bigcup_{t=1}^{r-1}L'_t)\subseteq(\bigcup_{t=1}^{r-1}L_t).$$

By assumption, $\bigcup_{t=1}^{r-1}\{\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t}\}$ is a Gröbner basis for the $\mathbb{Z}[x]$ lattice of $(\bigcup_{t=1}^{r-1}L_t)$. So $S(\mathbf{g}_{r,k},\mathbf{g}_{r,l})-(u_1\mathbf{g}_{r,1}+\cdots+u_l\mathbf{g}_{r,l})$ can be reduced to $\mathbf{0}$ by $\bigcup_{t=1}^{r-1}\{\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t}\}$. Hence, we have $\bigcup_{t=1}^{r}\{\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t}\}$ is a Gröbner basis for the $\mathbb{Z}[x]$ lattice $(\bigcup_{t=1}^{r}\{\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t}\})$.

By 2),

$$\mathbf{g}_{r,l}-\frac{a_{r,l}}{a_{r,l-1}}x\mathbf{g}_{r,l-1}\in \mathrm{Span}_{\mathbb{Z}}(L'_1,\ldots,L'_{r-1},\mathbf{h}_{r,1},\ldots,\mathbf{h}_{r,l})\subseteq \mathrm{Span}_{\mathbb{Z}}(L'_1,\ldots,L'_{r-1},\mathbf{g}_{r,1},\ldots,\mathbf{g}_{r,i_r},x\mathbf{g}_{r,i_r},\ldots,x\mathbf{g}_{r,l-1})$$

for $i_r<l\le k_r$. So there exists a sequence of integers $u_1,\ldots,u_{i_r},v_{i_r},\ldots,v_{l-1}$, such that $\mathbf{g}_{r,l}-\frac{a_{r,l}}{a_{r,l-1}}x\mathbf{g}_{r,l-1}-\sum_{k=1}^{i_r}u_k\mathbf{g}_{r,k}-\sum_{k=i_r}^{l-1}v_kx\mathbf{g}_{r,k}\in \mathrm{Span}_{\mathbb{Z}}(L'_1,\ldots,L'_{r-1})\subseteq(\bigcup_{t=1}^{r-1}L_t)=(\bigcup_{t=1}^{r-1}\{\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t}\})$. Hence, $\mathbf{g}_{r,l}$ can be reduced to $\mathbf{0}$ by $\bigcup_{t=1}^{r}\{\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t}\}$. Then, $\bigcup_{t=1}^{r}\{\mathbf{g}_{t,1},\ldots,\mathbf{g}_{t,i_t}\}$ is a Gröbner basis for the $\mathbb{Z}[x]$ lattice of $(\bigcup_{t=1}^{r}L_t)$. □

Theorem 4.28. *Algorithm* GHNF_n *is correct and terminated.*

Proof. It is a direct consequence by Lemma 4.26 and 4.27. □

Similar to Corollary 4.10, we have

Corollary 4.29. *The Algorithm* GHNF_n *ends in at most* $D+nd$ *loops, where* $D=73n^8d^5(h+(\log n^2d)+1)$.

Theorem 4.30. *The worst case bit size complexity of Algorithm* GHNF_n *is* $O(n^{20+2\theta+\varepsilon}d^{12+\theta+\varepsilon}(h+\log(n^2d))^{2+\varepsilon}+n^{19}d^{11}(\log n^2d)B(n^5d^3(h+\log n^2d)))$*, where* $h=\mathrm{height}(F)$ *and* $\varepsilon>0$ *is a sufficiently small number.*

Proof. By Lemma 3.25, the height bound for the GHNF of F is $6n^3d^2(h+(\log n^2d)+1):=h_2$. Consider the Step 2 of the Algorithm GHNF_n, we know that in the k-th loop, we need to compute the HNF of an integer matrix with size at most $n(d+k+1)\times(n(n+1)d+n)$, whose rank is no more that $(n(n+1)d+n)$. The $\log\beta$ in Lemma 4.11 can be taken as $\log\beta=(n(n+1)d+n)(\frac{1}{2}\log(n(n+1)d+n)+h_2)=O(n^5d^3(h+\log n^2d))$.

The complexity in the k-th loop is $O(n(d+k+1)\cdot(n(n+1)d+n)^{\theta-1}(\log\beta)M(\log\log\beta)/(\log\log\beta)+n(d+k+1)\cdot(n(n+1)d+n)\log(n(n+1)d+n)B(\log\beta))=(d+k+1)O(n^{4+2\theta+\varepsilon}d^{2+\theta+\varepsilon}(h+\log n^2d)^{1+\varepsilon}+n^3d(\log n^2d)B(n^5d^3(h+\log n^2d)))$, for any $\varepsilon>0$. Hence, the total complexity is,

$$\begin{aligned}&\sum_{k=0}^{D+nd}(d+k+1)O(n^{4+2\theta+\varepsilon}d^{2+\theta+\varepsilon}(h+\log n^2d)^{1+\varepsilon}+n^3d(\log n^2d)B(n^5d^3(h+\log n^2d)))\\&=O(n^{20+2\theta+\varepsilon}d^{12+\theta+\varepsilon}(h+\log n^2d)^{2+\varepsilon}+n^{19}d^{11}(\log n^2d)B(n^5d^3(h+\log n^2d))),\ \text{for any } \varepsilon>0.\end{aligned}$$

□

Similar to Corollary 4.13, by setting $\theta=2.376$ and $\varepsilon=0.001$, we have

Corollary 4.31. *The worst case bit size complexity of Algorithm* GHNF_n *is* $O(n^{24.753}d^{14.377}(h+\log n^2d)^{2.001})$.

Similar to Remark 4.14, the number m in the input is omitted in the complexity bound.

5 Experimental results

The algorithms presented in Section 4 have been implemented in both Maple 18 and Magma 2.21-7. The timings given in this section are collected on a PC with Intel(R) Xeon(R) CPU E7-4809 with 1.90GHz. For each set of inpute parameters, we use the average timing of ten experiments for random polynomials with coefficients between $[-100,100]$.

Figure 1 shows the timings of the Algorithm GHNF_1 in Magma 2.21-7 and Maple 18, and that of the GröbnerBasis command in Magma 2.21-7. From Theorem 4.12, the degree of the input polynomials is the the dominant factor in the computational complexity of the algorithm. In the experiments, the length of the input polynomial vectors is fixed to be 3. The degrees are in the range $[45,80]$.

From the figure, we see that our algorithm is much more efficient than the GröbnerBasis algorithm in Magma. As far as we know, the GröbnerBasis algorithm in Magma also uses an F4 style algorithm to compute the Gröbner basis and is also based on the computation of HNF of the coefficient matrices. In other words, the GröbnerBasis algorithm in Magma is quite similar to our algorithm and the comparison is fair. The reason for Algorithm GHNF_1 to be more efficient is due to the way how the prolongation is done in Step 2 of algorithm GHNF_1. By prolonging $g_1,\ldots,g_{t-1}$ instead of the original polynomials and not g_t, the size of the coefficient matrices is nice controlled. This fact is more important in algorithm GHN_n.

The difference for the timings of Algorithm GHNF_1 in Magma and Maple is mainly due to the different implementations of the HNF algorithms.

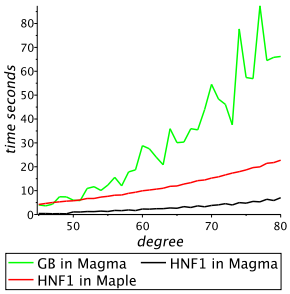

Figure 1: Comparison of GHNF_1 and GröbnerBasis in Magma and Maple: the $\mathbb{Z}[x]$ case

In Table 1, we give the timings for several input where the polynomials have larger degrees. Other parameters are the same. We see that for input polynomials with degree larger than 150, the GröbnerBasis algorithm in Magma cannot compute in the GHNF in reasonable time.

d	GHNF_1 in Maple 18	GHNF_1 in Magma 2.21-7	GB in Magma 2.21-7
100	50.5932	19.048	214.91
150	202.8135	104.827	>1000
200	590.7763	384.946	>1000

Table 1: Comparison of GHNF_1 and GröbnerBasis in Magma and Maple: the $\mathbb{Z}[x]$ case

Figure 2 plots the timings of Algorithm GHNF_n implemented in Magma 2.21-7 and Maple 18, where the input random polynomial matrices are of size 3×3 with degrees in $[2, 30]$. There is no implementation of Gröbner bases methods in Magma for $\mathbb{Z}[x]$-modules, so we cannot make a comparison with Magma in this case. In line with our complexity analysis given in Section 4, algorithm GHNF_n slows down rapidly when $n > 1$.

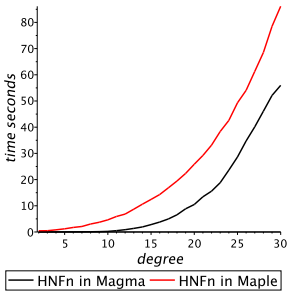

Figure 2: Timings of GHNF_n in Magma and Maple

In Table 2, we list the timings of Algorithm GHNF_n for several examples with larger degrees. This shows the polynomial-time natural of the algorithm, because the algorithm works for quite large d. Also, for large d, the Maple implementation becomes faster.

d	GHNF_n in Maple 18	GHNF_n in Magma 2.21-7
40	245.689	236.029
50	554.452	637.05

Table 2: Timings of GHNF_n in Magma and Maple

6 Conclusion

In this paper, a polynomial-time algorithm is given to compute the GHNFs of matrices over $\mathbb{Z}[x]$, or equivalently, the reduced Gröbner basis of a $\mathbb{Z}[x]$-lattice. The algorithm adopts the F4 strategy to compute Gröbner bases, where a novel prolongation is designed so that the coefficient matrices under consideration have polynomial sizes. Existing efficient algorithms are used to compute the HNF for these coefficient matrices. Finally, nice degree and height bounds of elements of the reduced Gröbner basis are given. The algorithm is implemented and is shown to be more efficient than existing algorithms.

Acknowledgement. We would like to thank Dr. Jianwei Li for provide us information on the complexity of computing Hermite normal forms.

References

[1] M. Aschenbrenner, *Ideal membership in polynomial rings over the integers*, Journal of the American Mathematical Society. **17**, 2, pp. 407-441 (2004).

[2] B. Beckermann, G. Labahn, and G. Villard, *Normal forms for general polynomial matrices*, Journal of Symbolic Computation. **41**, 6, pp. 708-737 (2006).

[3] B. Buchberger, *Bruno buchberger's phd thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal*, Journal of Symbolic Computation, **41**, 3, pp. 475-511 (2006).

[4] H. Cohen, *A course in computational algebraic number theory*, Springer. **138** (1993).

[5] D. Cox, J. Little, and D. O'shea, *Using algebraic geometry*, Springer-Verlag, New York. (2005).

[6] D. Cox, J. Little, H. Schenck, *Toric Varieties*, Springer-Verlag, New York. (2010).

[7] N. Courtois, A. Klimov, J. Patarin, et al., *Efficient algorithms for solving over-determined systems of multivariate polynomial equations*, EUROCRYPT, Bruges, Belgium, pp. 392-407 (2000).

[8] P.D. Domich, R. Kannan, and L.E. Trotter Jr, *Hermite normal form computation using modulo determinant arithmetic*, Mathematics of Operations Research. **12**, 1, pp. 50-59 (1987).

[9] D. Eisenbud, *Commutative Algebra: with a view toward algebraic geometry*, Springer. (1995).

[10] J.C. Faugere, *A new efficient algorithm for computing Gröbner bases (F4)*, Journal of pure and applied algebra. **139**, 1, pp. 61-88 (1999).

[11] X.S. Gao, Z. Huang, and C.M. Yuan, *Binomial difference ideal and toric difference variety*, arXiv preprint arXiv:1404.7580 v2. (2015).

[12] A.O. Gelfond, *Transcendental and Algebraic Numbers*, Dover, New York. (1960).

[13] E. Kaltofen, M.S. Krishnamoorthy, and B.D. Saunders, *Fast parallel computation of Hermite and Smith forms of polynomial matrices*, SIAM Journal on Algebraic Discrete Methods. **8**, 4, pp. 683-690 (1987).

[14] Ä. Kandri-Rody and D. Kapur, *Computing a Gröbner basis of a polynomial ideal over a Euclidean domain*, Journal of Symbolic Computation. **6**, 1, pp. 37-57 (1988).

[15] R. Kannan and A. Bachem, *Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix*, SIAM Journal on Computing. **8**, 4, pp. 499-507 (1979).

[16] D. Lazard, *Gröbner bases, gaussian elimination and resolution of systems of algebraic equations*, Computer Algebra. pp. 146-156 (1983).

[17] E. Mayr and A. Meyer, *The complexity of the word problems for commutative semigroups and polynomial ideals*, Advance of Mathematics. **46**, pp. 305-329 (1982).

[18] T. Mulders and A. Storjohann, *On lattice reduction for polynomial matrices*, Journal of Symbolic Computation. **35**, 4, pp. 377-401 (2003).

[19] A. Storjohann, *Algorithms for matrix canonical forms[D]*. PhD Thesis, Swiss Federal Institute of Technology Zurich, 2013.

[20] A. Storjohann and G. Labahn, *Asymptotically fast computation of Hermite normal forms of integer matrices*, *Proc. ISSAC'96*, pp. 259-266. ACM Press, (1996).

[21] S. Bosch, and U. Güntzer, and R. Remmert, *Non-Archimedean analysis. A systematic approach to rigid analytic geometry*, Journal of Grundlehren der Math. Wissen, Springer-Verlag (1984).

[22] R. Zippel, *Effective Polynomial Computation*, Kluwer Academic Publishers, Boston (1993).