Theoretical Computer Science 755 (2019) 89–109

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

A polynomial-time algorithm to compute generalized Hermite normal forms of matrices over $\mathbb{Z}[x]$ ☆

Rui-Juan Jing, Chun-Ming Yuan, Xiao-Shan Gao *

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

ARTICLE INFO

Article history:
Received 17 March 2016
Received in revised form 25 June 2018
Accepted 5 July 2018
Available online 16 August 2018
Communicated by P. Spirakis

Keywords:
Generalized Hermite normal form
Gröbner basis
Polynomial-time algorithm
$\mathbb{Z}[x]$ module

ABSTRACT

In this paper, we give the first polynomial time algorithm 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 has polynomial bit size computational complexities and 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 sizes of coefficient matrices under consideration are nicely controlled. Second, the complexity bound of the algorithm is achieved by a nice estimation for the degree and height bounds of the polynomials in the generalized Hermite normal form. Third, fast algorithms to compute Hermite normal forms of matrices over $\mathbb{Z}$ are used as the computational tool.

© 2018 Elsevier B.V. All rights reserved.

1. Introduction

The Hermite normal form (abbr. HNF) is a standard representation for matrices over principal ideal domains such as $\mathbb{Z}$ and $\mathbb{Q}[x]$, which has many applications in algebraic group theory, integer programming, lattices, linear Diophantine equations, system theory, and analysis of cryptosystems [5,17,21]. Efficient algorithms to compute HNF have been studied extensively until recently [2,5,9,15,17,22–24]. Note that $\mathbb{Z}[x]$ is not a PID and a matrix over $\mathbb{Z}[x]$ cannot be reduced to an HNF. In [12,13], the concept of generalized Hermite normal form (abbr. GHNF) is introduced and it is shown that any matrix over $\mathbb{Z}[x]$ can be reduced to a GHNF. Furthermore, a matrix $F = [\mathbf{f}_1, \dots, \mathbf{f}_s] \in \mathbb{Z}[x]^{n\times s}$ is a GHNF if and only if the set of its column vectors $\mathbb{f} = \{\mathbf{f}_1, \dots, \mathbf{f}_s\}$ forms 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 [5], 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 binomial ideals and toric varieties [7]. For instance, the decision algorithms for some of the major properties of Laurent binomial difference ideals and toric difference varieties are based on the computation of GHNFs of the exponent matrices of the difference ideals [12,13]. This motivates the study of efficient algorithms to compute the GHNFs.

The reduced Gröbner basis for a $\mathbb{Z}[x]$-lattice can be computed with the Gröbner basis methods for modules over rings [6,16,19]. However, such general algorithms do not take advantage of the special properties of $\mathbb{Z}[x]$-modules and do not have a complexity analysis. Also note that the worst case complexity of computing Gröbner bases in $\mathbb{Q}[x_1, \dots, x_n]$ is double exponential [20].

☆ Partially supported by an NSFC grant No. 11688101.

* Corresponding author.
E-mail addresses: rjing@amss.ac.cn (R.-J. Jing), cmyuan@mmrc.iss.ac.cn (C.-M. Yuan), xgao@mmrc.iss.ac.cn (X.-S. Gao).

https://doi.org/10.1016/j.tcs.2018.07.003
0304-3975/© 2018 Elsevier B.V. All rights reserved.

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 size computational complexity. The algorithm consists of three main ingredients.

The first ingredient comes from the powerful idea in Faugère's F4 algorithm [11] and the XL algorithm [8] of Courtois et al. 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 [4]. 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 those $x^k\mathbf{f}_i$ are nicely controlled.

The second 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, which is a key factor in the complexity analysis of our algorithm. Note that the degree bound also depends on the coefficients of F. The bounds about the GHNF are obtained based on the 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. In order to find the degree and height bounds for the GHNF, we need to find solutions of 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 give better bounds than those in [1].

The third 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 matrices of those prolongations $x^k\mathbf{f}_i$ obtained in the first ingredient. The first polynomial-time algorithm to compute HNF was given by Kannan and Bachem [17] and there exist many efficient algorithms to compute HNFs for matrices over $\mathbb{Z}$ [5,9,23,24] and matrices over $\mathbb{Q}[x]$ [2,15,22]. Note that the GHNF for a matrix over $\mathbb{Z}[x]$ cannot be recovered from its HNF over $\mathbb{Q}[x]$ directly. In the complexity analysis of our algorithm, we use the HNF algorithm with the best bit size complexity bound [23].

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. In the general case, the proposed algorithm is also very efficient in that quite large problems can be solved.

The rest of this paper is organized as follows. In Section 2, we introduce several notations for Gröbner bases of $\mathbb{Z}[x]$ lattices. In Section 3, we give degree and height bounds for the GHNF of a matrix over $\mathbb{Z}[x]$. In Section 4, we give the algorithm to compute the GHNF and analyze its complexity. 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 Gröbner bases for $\mathbb{Z}[x]$ lattices will be given. For more details, please refer to [6,12,16].

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 $\{\mathbf{f}_1, \ldots, \mathbf{f}_s\} \subset \mathbb{Z}[x]^n$ and this fact is denoted as $L = (\mathbf{f}_1, \ldots, \mathbf{f}_s)_{\mathbb{Z}[x]}$. If $\mathbf{f}_i = [f_{1,i}, \ldots, f_{n,i}]^\tau$, then we call $M = [\mathbf{f}_1, \ldots, \mathbf{f}_s] = [f_{i,j}]_{n\times s}$ a *matrix representation* of $L = (\mathbf{f}_1, \ldots, \mathbf{f}_s)_{\mathbb{Z}[x]}$. If $n = 1$, M is called a *polynomial vector*.

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 in $\mathbb{Z}[x]^n$ is a product 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 $i < j$ or $i = j$ and $\alpha < \beta$. 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 $\prec$, any non-zero $\mathbf{f} \in \mathbb{Z}[x]^n$ can be written in a unique way as a $\mathbb{Z}$-linear combination of monomials,

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

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 $\mathbb{Z}[x]^n$ with $b \neq 0$, $ax^\alpha\mathbf{e}_i$ is called $\{bx^\beta\mathbf{e}_j\}$*-reduced* if one of the following conditions is valid: $i \neq j$; $i = j$ and $\alpha < \beta$; or $i = j$, $\alpha \geq \beta$, and $0 \leq a < |b|$. For any $\mathbf{f}, \mathbf{g} \in \mathbb{Z}[x]^n$ with $\mathbf{g} \neq 0$, $\mathbf{f}$ is called $\mathbf{g}$-reduced if any term of $\mathbf{f}$ is $\mathbf{LT}(\mathbf{g})$-reduced. If $\mathbf{f}$ is not $\mathbf{g}$-reduced, then by the reduction algorithm for the polynomials in $\mathbb{Z}[x]$ [19], one can compute a unique $\mathbf{r}$ and a quotient $q \in \mathbb{Z}[x]$ such that $\mathbf{r} = \mathbf{f} - q\mathbf{g}$ is $\mathbf{g}$-reduced and is denoted as $\mathbf{r} = \overrightarrow{\mathbf{f}}^{\mathbf{g}}$. If $\mathbf{f}$ is $\mathbf{g}$-reduced, then set $\overrightarrow{\mathbf{f}}^{\mathbf{g}}$ to be $\mathbf{f}$. 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 $\mathbf{g}_1 \prec \ldots \prec \mathbf{g}_m$, $\mathbf{f}$ is called G-reduced if every term of $\mathbf{f}$ is $\mathbf{LT}(\mathbf{g}_i)$-reduced for $i=1,\ldots,m$. Let $\mathbf{r}_{m+1}=\mathbf{f}$ and for $i=m,m-1,\ldots,1$, set $\mathbf{r}_i=\overline{\mathbf{r}_{i+1}}^{\mathbf{g}_i}$. Denote $\mathbf{r}_1=\overline{\mathbf{f}}^G$ and say $\mathbf{f}$ is reduced to $\mathbf{r}_1$ by G.

Definition 2.1. Let $\mathbf{f},\mathbf{g}\in\mathbb{Z}[x]^n$, $\mathbf{LT}(\mathbf{f})=ax^k\mathbf{e}_i$, $\mathbf{LT}(\mathbf{g})=bx^s\mathbf{e}_j$, $s\le k$. 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

$$S(\mathbf{f},\mathbf{g})=\begin{cases}\mathbf{f}-\frac{a}{b}x^{k-s}\mathbf{g}, & \text{if } b|a;\\ \frac{b}{a}\mathbf{f}-x^{k-s}\mathbf{g}, & \text{if } a|b;\\ u\mathbf{f}+vx^{k-s}\mathbf{g}, & \text{if } a\nmid b \text{ and } b\nmid a,\ \textit{where } \gcd(a,b)=ua+vb.\end{cases}\tag{1}$$

If $n=1$, the S-vector is called S-polynomial, which is the same with the definition in [16].

Definition 2.2. A finite set $G\subset\mathbb{Z}[x]^n$ is called a Gröbner basis for the $\mathbb{Z}[x]$ lattice L generated by G if for all $\mathbf{f}\in L$, 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 $\mathbf{g}\in G$, $\mathbf{LT}(\mathbf{g})$ is $G\setminus\{\mathbf{g}\}$-reduced.

It is easy to see that G is a Gröbner basis if and only if $\overline{\mathbf{g}}^G=0$ for any $\mathbf{g}\in(G)_{\mathbb{Z}[x]}$. The Buchberger criterion for Gröbner basis is still true: G is a Gröbner basis if and only if $\overline{S(\mathbf{f},\mathbf{g})}^G=\mathbf{0}$ for all $\mathbf{f},\mathbf{g}\in G$. 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 $\mathbf{g}_1\prec\ldots\prec\mathbf{g}_s$. To make the reduced Gröbner basis unique, we further assume that $\mathbf{LC}(\mathbf{g}_i)>0$ for any $\mathbf{g}_i\in G$.

We need the following property from [12] for Gröbner bases in $\mathbb{Z}[x]$.

Proposition 2.3. *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 $\mathbf{LT}(b_i)=c_ix^{d_i}\in\mathbb{N}[x]$. Then*

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

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

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 and $\mathrm{Primpart}(F)=\gcd(F)/\mathrm{Content}(F)$ the primitive part of F. Now, we give a refined description of Gröbner bases for ideals in $\mathbb{Z}[x]$ [18].

Proposition 2.4. *$G=\{g_1,\ldots,g_n\}$ with $\deg(g_1)<\cdots<\deg(g_n)$ is a minimal Gröbner basis of $(f_1,\ldots,f_m)$ in $\mathbb{Z}[x]$ if and only if $g_1=ab_1\cdots b_{n-1}\tilde{g}_1$, $g_n=ah_n\tilde{g}_1$, and $g_i=ab_i\cdots b_{n-1}h_i\tilde{g}_1$, $2\le i\le n-1$, 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) $b_i\in\mathbb{Z}$, $b_i\neq\pm1$, *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* $1\le i\le n-1$, *where* $h_1=1$.

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

$$\mathscr{C}=\begin{pmatrix} c_{11} & \ldots & c_{1,l_1} & c_{1,l_1+1} & \ldots & \ldots & \ldots\ \ldots & \ldots & \ldots & \ldots\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\ \ldots & \ldots & \ldots & \ldots\\ c_{r_1,1} & \ldots & c_{r_1,l_1} & c_{r_1,l_1+1} & \ldots & \ldots & \ldots\ \ldots & \ldots & \ldots & \ldots\\ 0 & \ldots & 0 & c_{r_1+1,1} & \ldots & c_{r_1+1,l_2} & \ldots\ \ldots & \ldots & \ldots & \ldots\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\ \ldots & \ldots & \ldots & \ldots\\ 0 & \ldots & 0 & c_{r_2,1} & \ldots & c_{r_2,l_2} & \ldots\ \ldots & \ldots & \ldots & \ldots\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\ \ldots & \ldots & \ldots & \ldots\\ 0 & \ldots & 0 & 0 & \ldots & 0 & \ldots\ 0 & c_{r_{t-1}+1,1} & \ldots & c_{r_{t-1}+1,l_t}\\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\ \ldots & \ldots & \ldots & \ldots\\ 0 & \ldots & 0 & 0 & \ldots & 0 & \ldots\ 0 & c_{r_t,1} & \ldots & c_{r_t,l_t} \end{pmatrix}_{n\times m}\tag{2}$$

whose elements are in $\mathbb{Z}[x]$. It is clear that $n=r_t$ and $m=\sum_{i=1}^t l_i$. Assume

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

and assume $c_{i,j,0}\ge0$. Then the leading term of $\mathbf{c}_{r_i,j}$ is $c_{r_i,j,0}x^{d_{r_i,j}}\mathbf{e}_{r_i}$, where $\mathbf{c}_{r_i,j}$ is the $(l_1+\cdots+l_{i-1}+j)$-th column of $\mathscr{C}$.

Definition 2.5. The matrix $\mathscr{C}$ is called a generalized Hermite normal form (abbr. 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) $c_{r_i,l_i,0}|\ldots|c_{r_i,2,0}|c_{r_i,1,0}$.
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 $1 \le i \le t$, $1 \le j \le l_i$.

We have the following result [12].

Theorem 2.6. *$\{\mathbf{f}_1, \ldots, \mathbf{f}_s\} \subset \mathbb{Z}[x]^n$ is a reduced Gröbner basis under the monomial order $\prec$ and $\mathbf{f}_1 \prec \mathbf{f}_2 \prec \ldots \prec \mathbf{f}_s$ if and only if the polynomial matrix $[\mathbf{f}_1, \ldots, \mathbf{f}_s]$ is a* GHNF.

3. Degree and height bounds for the GHNF

We first give some notations. 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 $F = \{f_1, \ldots, f_m\} \subset R[x]$, 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 [1,10] 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 $\widehat{\mathbb{Z}}_{(p)}[x]$ [1,10].

For any subring R of $\mathbb{C}$ or $\widehat{\mathbb{Z}}_{(p)}$ and $\mathbf{f}_1, \ldots, \mathbf{f}_s$ in $R[x]^n$, let $(\mathbf{f}_1, \ldots, \mathbf{f}_s)_{R[x]}$ be the $R[x]$ module generated by $\mathbf{f}_1, \ldots, \mathbf{f}_s$ in $R[x]^n$.

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

In this section, we give several basic degree and height bounds in $\mathbb{Z}[x]$. By the extended Euclidean algorithm, we have

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 $\gcd(f_1, \ldots, f_m) = f_1g_1 + \cdots + f_mg_m$.*

In this section, we assume $f_1, \ldots, f_m \in \mathbb{Z}[x]$, $d = \max_{1\le i\le m} \deg(f_i)$, and $h = \mathrm{height}(f_1, \ldots, f_m)$, unless specified otherwise explicitly.

Lemma 3.2. *If $1 \in (f_1, \ldots, f_m)_{\mathbb{Q}[x]}$, then $\delta = f_1g_1 + \cdots + f_mg_m$ for some $\delta \in \mathbb{Z} \setminus \{0\}$ with $\mathrm{height}(\delta) \le d(2h + \log(d+1))$ and some $g_1, \ldots, g_m \in \mathbb{Z}[x]$ with degree $< d$. In this case, the height of the* GHNF *of $[f_1, \ldots, f_m]$ is $\le d(2h + \log(d+1))$.*

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 $Ab = [1, 0, \ldots, 0]^\tau \in \mathbb{Z}^{2d}$, where $A = [A_1, \ldots, A_m]$ with

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

for $i = 1, \ldots, m$, and $b = [b_{1,0}, \ldots, b_{1,d-1}, \ldots, b_{m,0}, \ldots, b_{m,d-1}]^\tau \in \mathbb{Q}^{md}$. Let $t = \mathrm{rank}(A) \le 2d$. 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 $\mathrm{height}(\delta) \le d(2h + \log(d+1))$. In this case, $\delta \in (f_1, \ldots, f_m)_{\mathbb{Z}[x]}$. Hence, the height of GHNF of $[f_1, \ldots, f_m]$ is $\le \mathrm{height}(\delta)$. $\square$

The following lemma is given by Gel'fond [14] and a simpler proof can be found in [25, p. 178].

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 $\frac{1}{2}\log(d+1) + d\log 2 + h$.*

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

$$\begin{aligned}
\text{height}(g) &\le \text{height}(g) + \text{height}(g_i) \\
&\le \frac{1}{2}\log(d_i+1) + d_i\log 2 + \text{height}(f_i) \;\text{ for any } i \qquad (3)\\
&\le \frac{1}{2}\log(d+1) + d\log 2 + h. \qquad \square
\end{aligned}$$

Remark 3.5. By equation (3), we have $\text{height}(f_i/g) \le \frac{1}{2}\log(d+1) + d\log 2 + h$ for any i.

We now give the degree and height bounds for the GHNF in $\mathbb{Z}[x]$.

Lemma 3.6. *Let $f_1, \ldots, f_m \in \mathbb{Z}[x]$ and $[g_1, \ldots, g_s]$ the GHNF of $[f_1, \ldots, f_m]$. Then $\deg(g_i) \le d$ and $\text{height}(g_i) \le (2d+1)(h + d\log 2 + \log(d+1))$.*

Proof. Obviously, the degree bound of the GHNF in $\mathbb{Z}[x]$ is d by the procedure of the Gröbner basis computation. Let $g = \gcd(f_1, \ldots, f_m)$ in $\mathbb{Z}[x]$, then, $[g_1/g, \ldots, g_s/g]$ is the GHNF of $[f_1/g, \ldots, f_m/g]$. By Lemma 3.4 and Remark 3.5, height(g) and height(f_i/g) are both $\le \frac{1}{2}\log(d+1) + d\log 2 + h$. 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, $\text{height}(g_i) \le 2d(h + d\log 2 + \log(d+1)) + \frac{1}{2}\log(d+1) + d\log 2 + h \le (2d+1)(h + d\log 2 + \log(d+1))$. $\square$

Finally, we consider an effective Nullstellensatz in $\mathbb{Z}_{(p)}[x]$, whose proof follows that of Lemma 6.4 in [1].

Lemma 3.7. *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 $1 = f_1h_1 + \cdots + f_mh_m$.*

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

$$\delta = f_1g_1 + \cdots + f_mg_m. \qquad (4)$$

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

$$1 - (r_1f_1 + \cdots + r_mf_m) \in (p)\mathbb{Z}_{(p)}[x]$$

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

$$1 - (f_1s_1 + \cdots + f_ms_m) = s. \qquad (5)$$

We have $\deg(s_j) \le \mu(2d-1) - d$ for all j; hence $\deg(s) \le \mu(2d-1)$. By equations (4) and (5), we have

$$1 = f_1s_1 + \cdots + f_ms_m + s = f_1h_1 + \cdots + f_mh_m$$

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

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

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

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

Lemma 3.8. *If* $1 \in (f_1, \ldots, f_m)_{\mathbb{Z}[x]}$*, then there exist* $h_1, \ldots, h_m \in \mathbb{Z}[x]$ *such that* $1 = f_1h_1 + \cdots + f_mh_m$*, with* $\deg(h_i) \le 3d^2(2h + \log(d+1))$ *for* $i = 1, \ldots, m$*.*

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

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

Let $p_1, \ldots, p_k$ be all the prime factors of δ. Since $1 \in (f_1, \ldots, f_m)_{\mathbb{Z}[x]}$, we have $1 \in (f_1, \ldots, f_m)_{\mathbb{Z}_{(p_i)}[x]}$. By Lemma 3.7, there exist $h_1^{(p_i)}, \ldots, h_m^{(p_i)} \in \mathbb{Z}[x]$ 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 $a, a_1, \ldots, a_k \in \mathbb{Z}$ 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 $j = 1, \ldots, m$, 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 $i = 1, \ldots, m$. $\square$

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

Throughout this section, let $F = (f_{ij}) \in \mathbb{Z}[x]^{n\times m}$, $d = \deg(F)$ the maximal degree of entries in F, and $h = \text{height}(F)$ the maximal height of elements in F. For any subring R of $\mathbb{C}$, let

$$\text{Sol}_{R[x]}(F) = \{Y \in R[x]^m \mid FY = 0\}$$

which is an $R[x]$-module in $R[x]^m$. Let r be the rank of F and F_1 the matrix consisting of r linear independent rows of F. Then, $\text{Sol}_{R[x]}(F) = \text{Sol}_{R[x]}(F_1)$. So, we assume F is of rank n unless mentioned otherwise in the rest of this section. In this section, we will show that $\text{Sol}_{R[x]}(F)$ has a set of generators whose degrees and heights can be nicely bounded.

For a prime p, $f = \sum_{\nu=0}^{\infty} f_\nu x^\nu \in \widehat{\mathbb{Z}}_{(p)}\langle x\rangle$ 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, $\overline{f_s} \ne 0$, and $v_p(f_i) > 0$ for all $i > s$, where v_p is the p-valuation. Now we describe the Weierstrass Division Theorem for $\widehat{\mathbb{Z}}_{(p)}\langle x\rangle$ [1,3]:

Theorem 3.9. *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 3.10. $\text{Sol}_{\widehat{\mathbb{Z}}_{(p)}\langle x\rangle}(F)$ *has a set of generators in* $\mathbb{Z}[x]^m$ *with degrees* $\le nd$*.*

Proof. Since F is of rank n, we have $n \le m$. Let $\triangle$ be an $n \times n$-submatrix of F with $\delta = \det(\triangle) \ne 0$ 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 $Fy = 0$ becomes

$$\begin{pmatrix} \delta & & & c_{1,n+1} & \cdots & c_{1,m} \\ & \ddots & & \vdots & & \vdots \\ & & \delta & c_{n,n+1} & \cdots & c_{n,m} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \tag{6}$$

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

$$v^{(1)} = \begin{pmatrix} -c_{1,n+1} \\ \vdots \\ -c_{n,n+1} \\ \delta \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, v^{(m-n)} = \begin{pmatrix} -c_{1,m} \\ \vdots \\ -c_{n,m} \\ 0 \\ \vdots \\ 0 \\ \delta \end{pmatrix}. \tag{7}$$

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 $\text{Sol}_{\widehat{\mathbb{Z}}_{(p)}\langle x\rangle}(F)$. 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 $\text{Sol}_{\widehat{\mathbb{Z}}_{(p)}\langle x\rangle}(F)$. Multiplying the equation (6) 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

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

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 in a 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 the above $u^{(1)}, \ldots, u^{(m-n)}, y^{(1)}, \ldots, y^{(M')}$ 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 3.9, there exist $Q_{n+1}, \ldots, Q_m \in \widehat{\mathbb{Z}}_{(p)}\langle x\rangle$ 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 3.10, 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 3.11. *$\mathrm{Sol}_{\mathbb{Q}[x]}(F)$ can be generated by elements in $\mathbb{Z}[x]^m$ of degrees $\le nd$.*

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

Lemma 3.12. *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 Lemmas 3.10, 3.11, and 3.12, we have the following corollary:

Corollary 3.13. *$\mathrm{Sol}_{\mathbb{Z}_{(p)}[x]}(F)$ can be generated by elements in $\mathbb{Z}[x]^m$ of degrees $\le nd$.*

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

Lemma 3.14. *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 3.15. *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 $\le nd$.*

Proof. By Lemmas 3.13 and 3.14, we 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 3.16. In results 3.10, 3.11, and 3.13, 3.15, 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 Remarks of Corollary 1.5 and Lemma 5.1 in [1], we have the following result [1].

Lemma 3.17. *Let $A \in \mathbb{Z}^{n\times m}$, $r = \mathrm{rank}(A)$, and $h = \mathrm{height}(A)$. Then $\mathrm{Sol}_{\mathbb{Z}}(A)$ can be generated by $m - r$ vectors whose heights are bounded by $2r(h + \log r + 1)$.*

Let $F = (f_{ij}) \in \mathbb{Z}[x]^{n\times m}$, $d = \deg(F)$, $h = \mathrm{height}(F)$, and F is of full rank. Then, we have

Theorem 3.18. *$\mathrm{Sol}_{\mathbb{Z}[x]}(F)$ can be generated by vectors whose degrees are bounded by nd and heights are bounded by $2(n(n+1)d + n)(h + \log(n(n+1)d + n) + 1)$.*

Proof. By Corollary 3.15, $\mathrm{Sol}_{\mathbb{Z}[x]}(F)$ 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 indeterminants taking values in $\mathbb{Z}$. Then, $Fy = 0$ can be written as the following matrix equation

$$\begin{pmatrix} A_1 \\ \vdots \\ A_n \end{pmatrix} y' = 0, \tag{8}$$

$y' = [y_{10}, \ldots, y_{1,nd}, \ldots, y_{m0}, \ldots, y_{m,nd}]^\tau$, $A_i = [A_{i1}, \ldots, A_{im}]_{((n+1)d+1)\times(m(nd+1))}$, 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 3.17, we have that the equation system (8) can be generated by vectors whose heights are bounded by $2(n(n+1)d + n)(h + \log(n(n+1)d + n) + 1)$. □

Remark 3.19. Let $D = \mathbb{Z}[x_1, \ldots, x_N]$ and $A \in D^{n\times m}$. In [1], Aschenbrenner proved that $\mathrm{Sol}_D(A)$ has a set of generators whose degrees and heights are bounded by $(2nd)^{2((N+1)^N-1)}$ and $C_2(2n(d+1))^{(N+1)^{O(N)}}(h+1)$, respectively, where 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. Due to the special structure of the Gröbner basis in $\mathbb{Z}[x]$, our results are much better than that of [1] in the $\mathbb{Z}[x]$ case.

Let $F \in \mathbb{Z}[x]^{n\times m}$, $b \in \mathbb{Z}[x]^m$. Denote $d = \deg(F, b) = \max(\deg(F), \deg(b))$, $h = \max(\mathrm{height}(F), \mathrm{height}(b))$. Similar to Theorem 6.5 in [1], we have the following degree bound.

Theorem 3.20. *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 3.18, 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 $\deg(z^{(k)}) \leq nd$ and

$$\mathrm{height}(z^{(k)}) \leq 2(n(n+1)d + n)(h + \log(n(n+1)d + n) + 1) = h_2$$

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 $1 = h_1 z_{m+1}^{(1)} + \cdots + h_K z_{m+1}^{(K)}$, then $[y, 1]^\tau = h_1 z^{(1)} + \cdots + h_K z^{(K)}$ is a solution to $Fy = b$. By Lemma 3.8, we have

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

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

3.3. Degree and height bounds in $\mathbb{Z}[x]^n$

In this section, we assume $F = (f_{ij}) \in \mathbb{Z}[x]^{n\times m}$, $d = \deg(F)$, $h = \text{height}(F)$, and F is of full rank. Let $\mathscr{C}$ in (2) be the GHNF of F. We will give degree and height bounds for $\mathscr{C}$.

In our analysis of the complexity, only the degree and height bounds of c_{r_i,k_i} in the r_i-th rows of $\mathscr{C}$ will be used. So, we define $\deg(\mathscr{C}) = \max_{i,k_i} \deg(c_{r_i,k_i})$ and $\text{height}(\mathscr{C}) = \max_{i,k_i} \text{height}(c_{r_i,k_i})$. The following theorem gives the degree and height bounds for the GHNF of F.

Theorem 3.21. *We have* $\deg(c_{r_i,l_i}) \le (n-r_i+1)d$ *and* $\text{height}(c_{r_i,j}) \le 6(n-r_i+1)^3d^2(h+1+\log((n-r_i+1)^2d))$ *for any* $1 \le i \le t$, $1 \le j \le l_i$.

Proof. Without loss of generality, we need only to prove the theorem for $r_1 = 1$, in which case $\deg(c_{1j}) \le nd$ and $\text{height}(c_{1j}) \le 6n^3d^2(h+1+\log(n^2d))$ for $1 \le j \le l_1$.

For any $[a, 0, \cdots, 0]^\tau \in (F)$, which is the $\mathbb{Z}[x]$ lattice generated by the columns of F, there exists a $\mathbf{u} \in \mathbb{Z}[x]^m$, such that $[a, 0, \cdots, 0]^\tau = Fu$ and hence $\mathbf{u} \in \text{Sol}_{\mathbb{Z}[x]}(F_{n-1})$, where F_{n-1} is the last $n-1$ rows of F. By Theorem 3.18, $\text{Sol}_{\mathbb{Z}[x]}(F_{n-1})$ can be generated by polynomials of degrees $\le (n-1)d$ and heights $\le h_1 = 2(n(n-1)d+(n-1))(h+\log(n(n-1)d+(n-1))+1)$, say $\{v^{(1)}, \dots, v^{(s)}\}$. Then, $[a, 0, \dots, 0]^\tau \in (F)$ can be generated by $\{Fv^{(1)}, \dots, Fv^{(s)}\}$ and $\deg(Fv^{(j)}) \le nd$ and $\text{height}(Fv^{(j)}) \le h + h_1$. Let $Fv^{(j)} = [t_j, 0, \dots, 0]^\tau$ for some $t_j \in \mathbb{Z}[x]$, $1 \le j \le s$. Then, $[c_{1,1}, \dots, c_{1,l_1}]$ is the GHNF of $[t_1, \dots, t_s]$, and $\deg(t_j) \le nd$, $\text{height}(t_j) \le h + h_1$. By Lemma 3.6, we have $\deg(c_{1,j}) \le nd$, i.e. $\deg(c_{1,j}) \le nd$ for $1 \le j \le l_1$. Moreover,

$$\begin{aligned}
&\text{height}(c_{1j}) \\
&\le (2nd+1)(h + h_1 + nd\log 2 + \log(nd+1)) \\
&= (2nd+1)(h + 2(n(n-1)d+(n-1))(h+\log(n(n-1)d+(n-1))+1) \\
&\quad + nd\log 2 + \log(nd+1)) \\
&\le (2nd+1)(h + 2n^2d(h+\log(n^2d)+1) + nd\log 2 + \log(n^2d)) \\
&\le 6n^3d^2(h+1+\log(n^2d)). \qquad \square
\end{aligned}$$

Remark 3.22. Note that, since the last $n-r_i+1$ rows of F have rank $t-i+1$, by the above proof, we have $\deg(c_{r_i,j}) \le (t-i+1)d$ and $\text{height}(c_{r_i,j}) \le 6(t-i+1)^3d^2(h+1+\log((t-i+1)^2d))$ where $h = \text{height}(F)$, for $1 \le i \le t$, $1 \le j \le l_i$.

We have the following degree bound for the transformation matrix U, which satisfying $\mathscr{C} = FU$.

Theorem 3.23. *Let* $F \in \mathbb{Z}[x]^{n\times m}$, $\mathscr{C}$ *be its* GHNF, *and* $U \in \mathbb{Z}[x]^{m\times s}$ *the transformation matrix satisfying* $\mathscr{C} = FU$. *Then,* $\deg(U) \le D$, *where* $D = 73n^8d^5(h+1+\log(n^2d))$.

Proof. By Theorem 3.21, we have $\deg(c_{r_i,j}) \le (n-r_i+1)d$, $\text{height}(c_{r_i,j}) \le 6(n-r_i+1)^3d^2(h+1+\log((n-r_i+1)^2d))$ for $i = 1, \dots, t$, $j = 1, \dots, l_i$. Denote by $U_{r_i,j}$ the column vector of U, satisfying $FU_{r_i,j} = [*, \dots, *, c_{r_i,j}, 0, \dots, 0]^\tau$. Then $U_{r_i,j}$ can be determined by $F_{n-r_i+1}U_{r_i,j} = [c_{r_i,j}, 0, \dots, 0]^\tau$, where F_{n-r_i+1} is the last $n-r_i+1$ rows of F. In Theorem 3.20, let $\deg(F,b) = \max_{i,j}\deg(F, c_{r_i,j}) \le nd$, $\text{height}(F,b) = \max_{i,j}\text{height}(F, c_{r_i,j}) \le 6n^3d^2(h+1+\log(n^2d))$. Then we have $\deg(U) \le 3n^2d^2(h_2+\log(nd+1)) + nd$, where $h_2 = 2(n(n+1)\deg(F,b)+n)(\text{height}(F,b)+\log(n(n+1)\deg(F,b)+n)+1)$. First, we have the following inequality:

$$\begin{aligned}
h_2 &= 2(n(n+1)\deg(F,b)+n)(\text{height}(F,b)+\log(n(n+1)\deg(F,b)+n)+1) \\
&\le 2(n^2(n+1)d+n)(6n^3d^2(h+1+\log(n^2d)) + \log(n^2(n+1)d+n)+1) \\
&\le 24n^6d^3(h+1+\log n^2d) \qquad \text{for any } n \ge 2.
\end{aligned} \tag{9}$$

One can verify that the above inequality is still valid for $n = 1$, in which case $\deg(F,b) \le d$ and $\text{height}(F,b) \le d(2h+\log(d+1)) + \frac{1}{2}\log(d+1) + d\log d + h$. So we have $\deg(U) \le 3n^2d^2h_2 + 3n^2d^2\log(nd+1) + nd \le 73n^8d^5(h+1+\log n^2d)$. □

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

Example 3.24. Let $F = \begin{pmatrix} 1 & x \\ 6x^3+1 & 8x^2 \end{pmatrix}$, and $h = 3\log 2 = 3$ the height of F, where we choose the logarithm with 2 as a base.

If $a = [a_1, a_2]^\tau$ with $a_2 \neq 0$ is a column vector of $\mathscr{C}$, then a_2 is an element of the GHNF of $[6x^3+1, 8x^2]$. Thus, $\deg(a_2) \leq \max(\deg(6x^3+1), \deg(8x^2)) = 3$ and by Theorem 3.4, $\operatorname{height}(a_2) \leq 4\log 2 + h = 7$.

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

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

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 3.18, $\deg(\mathbf{g}_i) \leq 3$ and $\operatorname{height}(\mathbf{g}_i) \leq 14(h + \log 7 + 1)$. 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 $\deg(h_i) \leq 4$, and $\operatorname{height}(h_i) \leq 28(h + \log 7 + 1) < 196$. Hence, by Theorem 3.21, $\deg(b_1) \leq 4$ and $\operatorname{height}(b_1) \leq 432(h + 1 + \log 12) < 3456$. Moreover, by Theorem 3.23, we know that the degree bound for the transformation matrix is $D = 4478976(h + 1 + \log 12) < 35831808$.

Actually, the solutions to $0 = (6x^3+1)u_1 + 8x^2u_2$ can be generated by $[8x^2, -(6x^3+1)]^\tau$. Thus, b_1 is in the GHNF of $[1, x] \cdot [8x^2, -(6x^3+1)]^\tau = [-6x^4 + 8x^2 - x]$. The GHNF and the transformation matrix are

$$\mathscr{C} = \begin{pmatrix} 6x^4 - 8x^2 + x & 3x^8 - 4x^6 + 5x^5 - 6x^3 + 1 \\ 0 & 1 \end{pmatrix}, U = \begin{pmatrix} -8x^2 & -4x^6 - 6x^3 + 1 \\ 6x^3 + 1 & 3x^7 + 5x^4 \end{pmatrix}.$$

So for some examples, the bounds are far from optimal, and this is the reason we will give an incremental algorithm in the next section to compute the GHNF.

4. Algorithms to compute the GHNF

In this section, we give an algorithm to compute the GHNF of $F \in \mathbb{Z}[x]^{n\times m}$. Roughly speaking, the algorithm works as follows. We will compute the HNF $G \in \mathbb{Z}^{s\times k}$ for the coefficient matrix of F and check whether a GHNF can be retrieved from G. In the negative case, certain prolongations are done to G and the procedure is repeated. The key idea is how to do the prolongation so that the sizes of the matrices G are nicely controlled.

4.1. HNF of integer matrix

In this section, we will introduce several basic results about HNF of an integer matrix, which will be used as the main computational tool in our GHNF algorithm.

Definition 4.1. A matrix $H = (h_{i,j}) \in \mathbb{Z}^{n\times m}$ is called an (column) HNF if there exists an $r \leq m$ and a strictly increasing map f from $[r+1, m]$ to $[1, n]$ satisfying: (1) for $j \in [r+1, m]$, $h_{f(j),j} \geq 1$, $h_{i,j} = 0$ if $i > f(j)$ and $h_{f(j),j} > h_{f(j),k} \geq 0$ if $k > j$; and (2) the first r columns of H are equal to zero.

Let $A \in \mathbb{Z}^{n\times m}$ and $H^{n\times m}$ be the HNF of A. Then there exists a $U \in \mathrm{GL}_m(\mathbb{Z})$ [5] such that

$$H = AU. \tag{10}$$

Note that H is obtained from A by doing column elementary operations which are represented by the matrix U. We need the following lemma [5] on the syzygy module of A.

Lemma 4.2. *Let (10) be given and assume that the first r columns of H are the* **0** *columns of H. Then a $\mathbb{Z}$-basis for the $\mathbb{Z}$-module* $\mathbf{Syz}(A) = \{Y \in \mathbb{Z}^m \mid AY = 0\}$ *is given by the first r columns of U.*

We will measure the cost of our algorithms in numbers of bit operations. We need the function $M(k) = O(k \log k \log\log k)$ which is the cost of multiplications and quotients of two integers a and b with $|a|, |b| < 2^k$. 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 $O(n^\theta)$ arithmetic operations. The best known upper bound for θ is about 2.376.

The following result from [23] gives the complexity of computing HNF over $\mathbb{Z}$.

Theorem 4.3. *Let $A \in \mathbb{Z}^{n\times m}$ with rank r and height h, and H be the HNF of A. Then* $\operatorname{height}(H) \leq \log\beta = r(\frac{1}{2}\log r + h)$. *The bit complexity to compute H from A is $O(mnr^{\theta-2}\log\beta M(\log\log\beta)/\log\log\beta + mnB(\log\beta)\log r)$.*

4.2. The $\mathbb{Z}[x]$ case

In this section, we will show how to compute the GHNF in $\mathbb{Z}[x]$. Throughout this section, let $F = [f_1, \ldots, f_m]$ be a polynomial vector over $\mathbb{Z}[x]$, $d = \deg(F)$, and $h = \text{height}(F)$. $C \in \mathbb{Z}^{(d+1)\times m}$ is called the *coefficient matrix* of F if its columns represent the polynomials in F such that

$$F = \mathbb{X}_d C, \text{ where } \mathbb{X}_d = [1, x, \ldots, x^d].$$

Let $[\mathbf{0}, H] \in \mathbb{Z}^{(d+1)\times m}$ be the HNF of C, where $H \in \mathbb{Z}^{(d+1)\times s}$ contains no zero columns. Then, there is a unimodular matrix $U = [U_1, U_2]$ such that $[\mathbf{0}, H] = CU$, $\mathbf{0} = CU_1$, and $H = CU_2$. We call $G = \mathbb{X}_d H$ the *polynomial Hermite normal form* (abbr. PHNF) of F. For simplicity, we denote $C = \text{CMAT}(F)$ and

$$G = \text{PHNF}(F) = \mathbb{X}_d H = \mathbb{X}_d C U_2 = F U_2. \tag{11}$$

Let $G = [g_1, \ldots, g_s] \in \mathbb{Z}[x]^{1\times s}$. From the definition of HNF, we have $\deg(g_1) < \deg(g_2) < \cdots < \deg(g_s)$. We now give the algorithm.

Algorithm 1 $\text{GHNF}_1(F)$.

Require: $F = [f_1, \ldots, f_m]$, $f_i \in \mathbb{Z}[x]$ and $d = \max_i \deg(f_i)$.
Ensure: The GHNF, or the reduced Gröbner basis, of F.
1: Let $G_0 = \text{PHNF}(F)$ and $k = 0$.
2: (loop) $k = k + 1$.
$P_k = [G_{k-1}, xG_{k-1,d-1}]$, where $G_{k-1,d-1}$ is the set of polynomials in G_{k-1} with degrees $\leq d - 1$.
$G_k = \text{PHNF}(P_k)$.
If $G_k \neq G_{k-1}$, repeat Step 2.
3: Let $G_k = [g_1, \ldots, g_s]$ and $R = [g_1]$. For j from 2 to s, if $\mathbf{LC}(g_{j-1}) \neq \mathbf{LC}(g_j)$, $R = R \cup \{g_j\}$.
4: Return R.

(For $F = [f_1, \ldots, f_m]$ and $G = [g_1, \ldots, g_m]$, we use the notation $[F, G] = [f_1, \ldots, f_m, g_1, \ldots, g_m]$.)

Example 4.4. $F = [6x^3 + 3x^2 + 12, 6x^3 + 3x^2 + 6x, 6x^3 + 15x^2, 6x^3 + 3x^2]$.
Step 1: $G_0 = \text{PHNF}(F) = [12, 6x, 12x^2, 6x^3 + 3x^2]$. We have $d = 3$.
1-st loop: $P_1 = [G_0, 12x, 6x^2, 12x^3]$, $G_1 = \text{PHNF}(P_1) = [12, 6x, 6x^2, 6x^3 + 3x^2]$.
2-nd loop: $P_2 = [G_1, 12x, 6x^2, 6x^3]$, $G_2 = \text{PHNF}(P_2) = [12, 6x, 3x^2, 6x^3]$.
3-rd loop: $P_3 = [G_2, 12x, 6x^2, 3x^3]$, $G_3 = \text{PHNF}(P_3) = [12, 6x, 3x^2, 3x^3]$.
4-th loop: $P_4 = [G_3, 12x, 6x^2, 3x^3]$, $G_4 = \text{PHNF}(P_4) = [12, 6x, 3x^2, 3x^3]$. The loop is terminated.
Step 3: $R = [12, 6x, 3x^2]$ is the GHNF of F.

In the rest of this section, we will prove the correctness of the algorithm and give its complexity.

For a polynomial vector $F = [f_1, \ldots, f_m]$, we denote $(F)_{\mathbb{Z}}$ to be $\mathbb{Z}$-module generated by the elements of F. If $\deg(f_i) < \deg(f_j)$ for all $i < j$, F is called a *$\mathbb{Z}$-Gröbner basis* for the following reason: if F is a $\mathbb{Z}$-Gröbner basis and $f \in (F)_{\mathbb{Z}}$, then there exists an f_k such that $\mathbf{LT}(f_k)|\mathbf{LT}(f)$, or equivalently, f can be reduced to zero by F over $\mathbb{Z}$. Furthermore, if $\mathbf{LT}(f_i)$ is not a $\mathbb{Z}$-factor of any monomial of f_j for $j \neq i$, then F is called a *reduced $\mathbb{Z}$-Gröbner basis*. By Definition 4.1 and (10), we have

Lemma 4.5. *Let $G = \text{PHNF}(F)$. Then $(F)_{\mathbb{Z}} = (G)_{\mathbb{Z}}$ and G is a reduced $\mathbb{Z}$-Gröbner basis of $(F)_{\mathbb{Z}}$.*

In Step 2 of Algorithm GHNF_1, if using the following “full” prolongation in the k-th loop, we have

$$\widetilde{P}_k = [\widetilde{G}_{k-1}, x\widetilde{G}_{k-1}], \widetilde{G}_k = \text{PHNF}(\widetilde{P}_k), \tag{12}$$

where $\widetilde{G}_0 = G_0$. Due to (10), it is easy to check that

$$(\widetilde{P}_k)_{\mathbb{Z}} = (\widetilde{G}_k)_{\mathbb{Z}} = (F \cup \{x^i F \mid i = 1, \ldots, k\})_{\mathbb{Z}}. \tag{13}$$

Remark 4.6. Note that $\{x^i F \mid i = 1, \ldots, k\}$ in (13) are the standard prolongation used in the XL algorithm [8] or a naive F4 style algorithm. The degree of $\widetilde{G}_k$ is $d + k$ which increases with the loop number k, while the degree of G_k in Algorithm GHNF_1 is always d, and this is the main advantage of our new prolongation. A key idea in the F4 algorithm and the XL algorithm is that when k is large enough, a Gröbner basis of F can be obtained by doing Gaussian elimination to the coefficient matrix of $\widetilde{P}_k$. We will prove that this is also true for the “partial prolongation” P_k in Step 2 of the algorithm.

Let $G_{k,s}$ and $\widetilde{G}_{k,s}$ be the sets of polynomials in G_k and $\widetilde{G}_k$ with degrees $\leq s$, respectively. Denote $g_{k,j}$ and $\widetilde{g}_{k,j}$ to be the polynomials in G_k and $\widetilde{G}_k$ with degree j, respectively. If there exist no such polynomials, $g_{k,j}$ and $\widetilde{g}_{k,j}$ are set to be zero. Clearly, $g_{k,d} \neq 0$ and $\widetilde{g}_{k,d+i} \neq 0$ for $i = 0, \ldots, k$.

Lemma 4.7. *We have* $\mathbf{LC}(\widetilde{g}_{k,d})|\mathbf{LC}(\widetilde{g}_{k,d+1})|\cdots|\mathbf{LC}(\widetilde{g}_{k,d+k})$ *and for* $f \in (\widetilde{P}_{k+1})_{\mathbb{Z}}$ *with* $l = \deg(f)$*, if* $d < l \le d+k+1$ *then* $f \in (\widetilde{G}_{k,d}, x\widetilde{G}_{k,l-1})_{\mathbb{Z}}$*; if* $l \le d$ *then* $f \in (\widetilde{G}_{k,d}, x\widetilde{G}_{k,d-1})_{\mathbb{Z}}$.

Proof. For convenience, denote $S_{i,k} = \widetilde{G}_{i,d} \cup x\widetilde{G}_{i,k}$ for $d-1 \le k \le d+i-1$. Since $\deg(S_{i,k}) = k+1$, $S_{i,k} \subset (\widetilde{G}_{i+1})_{\mathbb{Z}}$, and $\widetilde{G}_{i+1}$ is a $\mathbb{Z}$-Gröbner basis, we have $S_{i,k} \subset (\widetilde{G}_{i+1,k+1})_{\mathbb{Z}}$.

We prove the lemma by induction on the number of loops. For $k=0$, since $xg_{0,d}$ is the only element in $\widetilde{P}_1$ with degree $d+1$, we have $\mathbf{LT}(\widetilde{g}_{1,d+1}) = \mathbf{LT}(x\widetilde{g}_{0,d})$. As a consequence, if $f \in (\widetilde{P}_1)_{\mathbb{Z}}$ and $\deg(f) \le d$ then $f \in (S_{0,d-1})_{\mathbb{Z}}$. If $f \in (\widetilde{P}_1)_{\mathbb{Z}}$ and $\deg(f) = d+1$, then it is obvious that $f \in (S_{0,d})_{\mathbb{Z}} = (\widetilde{P}_1)_{\mathbb{Z}}$. The lemma is proved for $k=0$.

Suppose the lemma is valid for $k \le i$. By the induction hypothesis, since $\widetilde{g}_{i+1,j} \in \widetilde{P}_{i+1}$, we have $\widetilde{g}_{i+1,j} \in (S_{i,j-1})_{\mathbb{Z}}$ if $d < j \le d+i+1$ and $\widetilde{g}_{i+1,j} \in (S_{i,d-1})_{\mathbb{Z}}$ if $j \le d$. We first assume that $d < j \le d+i$. Since $x\widetilde{g}_{i,j-1}$ is the only polynomial with degree j in S_{j-1}, we have

$$\widetilde{g}_{i+1,j} = x\widetilde{g}_{i,j-1} + l_{i,j} \tag{14}$$

for some $l_{i,j} \in (S_{i,j-2})_{\mathbb{Z}} \subset (\widetilde{G}_{i+1,j-1})_{\mathbb{Z}}$. Then, $\mathbf{LC}(\widetilde{g}_{i+1,j}) = \mathbf{LC}(\widetilde{g}_{i,j-1})$, and thus $\mathbf{LC}(\widetilde{g}_{i+1,j})|\mathbf{LC}(\widetilde{g}_{i+1,j+1})$ for $j = d+1, \dots, d+i$ by the induction hypothesis. Moreover, since $\widetilde{g}_{i+1,d} \in (S_{i,d-1})_{\mathbb{Z}}$ and $\widetilde{g}_{i,d}$ and $x\widetilde{g}_{i,d-1}$ are the only polynomials in $S_{i,d-1}$ with degree d, we have $\mathbf{LC}(\widetilde{g}_{i+1,d})|\mathbf{LC}(\widetilde{g}_{i,d})$. Then $\mathbf{LC}(\widetilde{g}_{i+1,d})|\mathbf{LC}(\widetilde{g}_{i+1,d+1})$ follows from $\mathbf{LC}(\widetilde{g}_{i+1,d+1}) = \mathbf{LC}(\widetilde{g}_{i,d})$. The first part of the lemma is proved.

To prove the second part, we first show that if $d < q \le d+i+1$, then

$$\widetilde{g}_{i+1,q} \in (\widetilde{G}_{i+1,q-1}, x\widetilde{G}_{i+1,q-1})_{\mathbb{Z}}. \tag{15}$$

Since $\mathbf{LC}(\widetilde{g}_{i+1,q-1})|\mathbf{LC}(\widetilde{g}_{i+1,q})$, $a = \frac{\mathbf{LC}(\widetilde{g}_{i+1,q})}{\mathbf{LC}(\widetilde{g}_{i+1,q-1})}$ is in $\mathbb{Z}$. By (14), $\widetilde{g}_{i+1,q} - a x\widetilde{g}_{i+1,q-1} = x(\widetilde{g}_{i,q-1} - a x\widetilde{g}_{i,q-2}) + l_{i,q} - a x l_{i,q-1}$. Since $\deg(\widetilde{g}_{i,q-1} - a x\widetilde{g}_{i,q-2}) \le q-1$, we have $\widetilde{g}_{i,q-1} - a x\widetilde{g}_{i,q-2} \in (\widetilde{G}_{i+1,q-1})_{\mathbb{Z}}$. Also note $l_{i,j} \in (\widetilde{G}_{i+1,j-1})_{\mathbb{Z}}$. Then (15) is proved. Let $f \in (\widetilde{P}_{i+2})_{\mathbb{Z}} = (\widetilde{G}_{i+1,d+i+1}, x\widetilde{G}_{i+1,d+i+1})_{\mathbb{Z}}$ with $l = \deg(f)$. Using (15) repeatedly, we may assume $f \in (\widetilde{G}_{i+1,d}, x\widetilde{G}_{i+1,s})_{\mathbb{Z}}$ for some s. Since $\deg(\widetilde{G}_{i+1,d}) = d$ and $\deg(x\widetilde{G}_{i+1,s}) = s+1$, we have $s = l-1$ if $l > d$ and $s = d-1$ if $l \le d$, and the lemma is proved. □

Lemma 4.8. *We have* $G_k = \widetilde{G}_{k,d}$ *for any* $k \ge 0$.

Proof. This lemma is obviously valid for $k=0$. Suppose it is valid for $k = i-1$, that is, $\widetilde{G}_{i-1,d} = G_{i-1}$. Since $\deg(G_i) \le d$, $G_i \subset (\widetilde{G}_i)_{\mathbb{Z}}$, and $\widetilde{G}_i$ is a $\mathbb{Z}$-Gröbner basis, we have $(G_i)_{\mathbb{Z}} = (P_i)_{\mathbb{Z}} \subset (\widetilde{G}_{i,d})_{\mathbb{Z}}$. By Lemma 4.7 and the induction hypothesis, we have $\widetilde{G}_{i,d} \subset (\widetilde{G}_{i-1,d}, x\widetilde{G}_{i-1,d-1})_{\mathbb{Z}} = (G_{i-1}, xG_{i-1,d-1})_{\mathbb{Z}} = (P_i)_{\mathbb{Z}}$. Hence, $(G_i)_{\mathbb{Z}} = (\widetilde{G}_{i,d})_{\mathbb{Z}}$. By Lemma 4.5, G_i and $\widetilde{G}_{i,d}$ are reduced $\mathbb{Z}$-Gröbner bases. Hence $G_i = \widetilde{G}_{i,d}$. □

Lemma 4.9. *Suppose that Step 2 of Algorithm* GHNF$_1$ *terminates at the k-th loop. Then* $(\widetilde{G}_i)_{\mathbb{Z}} \subset (G_k, xg_{k,d}, \dots, x^i g_{k,d})_{\mathbb{Z}}$ *for* $i \ge 0$.

Proof. We have $G_k = G_{k+1} = \cdots$. We prove the lemma by induction on i. The lemma is valid for $i=0$, since $\widetilde{G}_0 = G_0 \subset (G_k)_{\mathbb{Z}}$. Suppose that the lemma is valid for $i=t$. From (12), $(\widetilde{G}_{t+1})_{\mathbb{Z}} = (\widetilde{G}_t, x\widetilde{G}_t)_{\mathbb{Z}}$. By the induction hypothesis, $\widetilde{G}_t \subset (G_k, xg_{k,d}, \dots, x^t g_{k,d})_{\mathbb{Z}}$. Then any $f \in \widetilde{G}_t$ can be written as $f = f_0 + \sum_{j=0}^{t} c_j x^j g_{k,d}$, where $f_0 \in G_{k,d-1}$ and $c_j \in \mathbb{Z}$. Then $xf = xf_0 + \sum_{j=0}^{t} c_i x^{i+1} g_{k,d}$. Since $xf_0 \in (xG_{k,d-1})_{\mathbb{Z}} \subset (G_{k+1})_{\mathbb{Z}} = (G_k)_{\mathbb{Z}}$, we have $xf \in (G_k, xg_{k,d}, \dots, x^{t+1} g_{k,d})_{\mathbb{Z}}$ and the lemma is proved. □

Theorem 4.10. *Algorithm* GHNF$_1$ *is correct. Furthermore, Step 2 of Algorithm* GHNF$_1$ *terminates in at most* $D+d$ *loops, where* $D = 73d^5(h + \log d + 1)$.

Proof. Suppose Step 2 of the algorithm terminates in the k-th loop. Then, $G_k = G_{k+1} = \cdots$. We will show that G_k is a Gröbner basis of $(F)_{\mathbb{Z}[x]}$. By (13), $(F)_{\mathbb{Z}[x]} = (G_k)_{\mathbb{Z}[x]} = (\widetilde{G}_k)_{\mathbb{Z}[x]}$. To show that G_k is a Gröbner basis, we will prove that any $f \in (F)_{\mathbb{Z}[x]}$ can be reduced to zero by G_k. By (13), there exists an integer l, such that $f \in (\widetilde{G}_l)_{\mathbb{Z}}$. Since $(\widetilde{G}_i)_{\mathbb{Z}} \subset (\widetilde{G}_j)_{\mathbb{Z}}$ for $i < j$, we may assume that $l \ge k$. By Lemma 4.9 $f \in (G_k, xg_{k,d}, \dots, x^l g_{k,d})_{\mathbb{Z}}$. Since $\{G_k, xg_{k,d}, \dots, x^l g_{k,d}\}$ is a $\mathbb{Z}$-Gröbner basis, we have $\overline{f}^{G_k} = 0$ and G_k is a Gröbner basis of $(F)_{\mathbb{Z}[x]}$. Step 3 of the algorithm picks a reduced Gröbner basis, or the GHNF of F, from G_k.

We now prove the termination of the algorithm. By Theorem 3.23 and (13), $\widetilde{G}_D$ contains the GHNF of F and hence a Gröbner basis of $(F)_{\mathbb{Z}[x]}$ by Theorem 2.6. By Lemma 3.6, the reduced Gröbner basis of $(F)_{\mathbb{Z}[x]}$ has degree $\le d$. By Lemma 4.8, $G_D = \widetilde{G}_{D,d}$ contains the reduced Gröbner basis of $(F)_{\mathbb{Z}[x]}$. From Example 4.4, the termination condition may not be satisfied immediately even if G_i is a Gröbner basis of $(F)_{\mathbb{Z}[x]}$. We will show that Step 2 will run at most d extra loops after G_k is a Gröbner basis. Suppose $G_k = [g_{k,s_k}, \dots, g_{k,d}]$ is already a Gröbner basis of $(F)_{\mathbb{Z}[x]}$ for some $k \le D$ and suppose $H_{k,1} = [g_{k,s_k}, \dots, g_{k,p}]$ such that p is the maximal integer satisfying $g_{k,p} = g_{k+1,p}$. Then, $H_{k,1}$ is also a Gröbner basis of $(F)_{\mathbb{Z}[x]}$. If $p = d$, then, $H_{k,1} = G_k$, clearly $G_k = G_{k+1}$ and Step 2 terminates at $(k+1)$-th loop. Otherwise, $p < d$ and $H_{k,1} \subset G_l$ for $l \ge k$.

Let $h_{k,p+1}$ be the remainder of $xg_{k,p}$ reduced by $H_{k,1}$ over $\mathbb{Z}$ and $H_{k,2}=[g_{k,s_k},\dots,g_{k,p},h_{k,p+1}]$. Then $\mathbf{LT}(h_{k,p+1})=\mathbf{LT}(xg_{k,p})$ and $\mathrm{CMAT}(H_{k,2})$ is an HNF. Since $h_{k,p+1}$ is the minimal element in (F) with degree $p+1$ and reduced w.r.t. $H_{k,1}$, we have $g_{k+l,p+1}=h_{k,p+1}$ for $l>1$, or equivalently $H_{k,2}\subset G_l$ for $l\ge k+1$. Similarly, we can prove that after each loop of Step 2, at least one more element of G_l will become stable. As a consequence, Step 2 will terminate at most $D+d$ loops. □

Theorem 4.11. *The bit size complexity of Algorithm* GHNF$_1$ *is* $O(d^{11+\theta+\varepsilon}(h+\log d)^{2+\varepsilon}+d^{7+\varepsilon}(h+\log d)B(d^6(h+\log d)))$*, where* $\varepsilon>0$ *is any sufficiently small number.*

Proof. The computationally dominant step of the algorithm is Step 2 and we will estimate the complexity of this step. In the k-th loop of Step 2, we need to compute the HNF of the coefficient matrix C_k of P_k. It is clear that C_k is of size $(d+1)\times s$ for some $s\le 2d+1$. Also note that the height of C_k is the same as that of $\mathrm{CMAT}(G_k)$. By Lemma 4.8 and (13), $\mathrm{CMAT}(G_k)$ is part of the HNF of $\mathrm{CMAT}(\cup_{i=0}^{k}x^kF)$. By Theorem 4.3, the height of C_k is $\le(k+d)(\frac{1}{2}\log(k+d)+h)\le h_1=(D+2d)(\frac{1}{2}\log(D+2d)+h)=O(d^5(h+\log d)^2)$, since the loop will terminate at most $D+d$ steps. Let $n=d+1, t=2d+1, r=d+1$, then the $\log\beta$ in Theorem 4.3 is $\log\beta=r(\frac{1}{2}\log r+h_1)=O(d^6(h+\log d))$. 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 a sufficiently small number ε. Hence, the complexity for each loop is

$$
\begin{aligned}
&O(tnr^{\theta-2}(\log\beta)M(\log\log\beta)/\log\log\beta+kn\log rB(\log\beta))\\
&\le O(d^{6+\theta+\varepsilon}(h+\log d)^{1+\varepsilon}+d^{2+\varepsilon}B(d^6(h+\log d)))\text{ for any }\varepsilon>0.
\end{aligned}
$$

By Theorem 4.10, the number of loops is bounded by $D+d$. So the worst complexity of the Algorithm GHNF$_1$ is $(D+d)O(d^{6+\theta+\varepsilon}(h+\log d)^{1+\varepsilon}+d^{2+\varepsilon}B(d^6(h+\log d)))=O(d^{11+\theta+\varepsilon}(h+\log d)^{2+\varepsilon}+d^{7+\varepsilon}(h+\log d)B(d^6(h+\log d)))$. □

In Theorem 4.11, 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 4.12. *The bit size complexity of Algorithm* GHNF$_1$ *is* $O(d^{13.38}(h+\log d)^{2.004})$.

Remark 4.13. 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 P_k in Step 2 of the algorithm depends on d only. Only the complexity of Step 1 depends on m and by Theorem 4.3, the complexity of Step 1 is $O^{\sim}(md^{\theta+1}(h+d))$ which is comparable to the complexity bound in Theorem 4.11 only when $m=O^{\sim}(d^{10})$. We therefore omit this term.

Finally, we prove a property of the syzygy modules of $\mathbb{Z}[x]$ ideals, which will be used in the next section. In Algorithm GHNF$_1$, for any $k\ge 1$, let $v_{k-1}=\#(G_{k-1})$ be the number of columns of G_{k-1}. Then $u_k=\#(P_k)=2v_{k-1}-1$. Let

$$
X_k=\begin{pmatrix}1 & x & & & \\ & & \ddots & & \\ & & & 1 & x \\ & & & & 1\end{pmatrix}_{v_{k-1}\times u_k}.
$$

Then $P_k=G_{k-1}X_k=\mathbb{X}_dM_k$, where $M_k=\mathrm{CMAT}(P_k)$. Let $[\mathbf{0},H_k]=M_kU_k$ be the HNF of M_k, where $U_k=[U_{k,1},U_{k,2}]$ is a unimodular matrix satisfying $\mathbf{0}=M_kU_{k,1}$, $H_k=M_kU_{k,2}$. By (11),

$$
G_k=P_kU_{k,2}=FU_{0,2}X_1\cdots U_{k-1,2}X_kU_{k,2},\qquad P_k=FU_{0,2}X_1\cdots U_{k-1,2}X_k,
$$

where $G_0=\mathrm{PHNF}(F)=FU_{0,2}$. For any $k\ge 1$, we define a map

$$
\begin{aligned}
\varphi_k:\mathbb{Z}[x]^{u_k}&\to\mathbb{Z}[x]^m\\
\mathbf{u}\quad&\mapsto U_{0,2}X_1\cdots U_{k-1,2}X_k\mathbf{u}.
\end{aligned}
$$

In particular, let $\varphi_0:\mathbb{Z}[x]^m\to\mathbb{Z}[x]^m$ be the identity map. The following result shows how to find a set of generators for the syzygy module $\mathbf{Syz}(F)$.

Proposition 4.14. *For any* $\mathbf{u}\in\mathbf{Syz}(F)\subset\mathbb{Z}[x]^m$ *and* $\deg(\mathbf{u})=l$*, we have* $\mathbf{u}\in(\bigcup_{k=0}^{l}\bigcup_{j=0}^{l-k}x^j\varphi_k(U_{k,1}))_{\mathbb{Z}}$*. Moreover,* $\mathbf{Syz}(F)=(\bigcup_{k=0}^{d}\varphi_k(U_{k,1}))_{\mathbb{Z}[x]}$.

Proof. By Theorem 3.18, $\mathbf{Syz}(F)$ can be generated by elements in $\mathbb{Z}[x]^m$ with degrees $\le d$. We need only to show the first statement. Let $P_0=F$, $\mathbf{u}_0'=\mathbf{u}$.

Since $F\varphi_k(U_{k,1}) = FU_{0,2}X_1\cdots U_{k-1,2}X_kU_{k,1} = P_kU_{k,1} = \mathbb{X}_d M_k U_{k,1} = \mathbf{0}$ for any $k \geq 0$, we have $\varphi_k(U_{k,1}) \subset \mathbf{Syz}(F)$. By Lemma 4.2, the lemma is valid for $l = 0$. If $l > 0$, it suffices to show that, for any $0 \leq q \leq l$, there exists a $\mathbf{u}'_q \in \mathbb{Z}[x]^{u_q}$ with $\deg(\mathbf{u}'_q) \leq l - q$, such that $\mathbf{u} = \varphi_q(\mathbf{u}'_q) \bmod (\bigcup_{k=0}^{q-1}\bigcup_{j=0}^{l-k} x^j\varphi_k(U_{k,1}))_{\mathbb{Z}}$. In this case, $P_q\mathbf{u}'_q = FU_{0,2}X_1\cdots U_{q-1,2}X_q\mathbf{u}'_q = F\mathbf{u} = 0$. It is valid for $q = 0$. Suppose it is also valid for $q = i$. Let $\mathbf{u}'_i \in \mathbb{Z}[x]^{v'_i}$ with $\deg(\mathbf{u}'_i) \leq l - i$, such that $\mathbf{u} = \varphi_i(\mathbf{u}'_i) \bmod (\bigcup_{k=0}^{i-1}\bigcup_{j=0}^{l-k} x^j\varphi_k(U_{k,1}))_{\mathbb{Z}}$ and $P_i\mathbf{u}'_i = 0$. Let $\mathbf{u}''_i = U_i^{-1}\mathbf{u}'_i = [u_1, \ldots, u_{v'_i - v_i}, 0, \ldots, 0]^\tau + [0, \ldots, 0, u_{v'_i - v_i + 1}, \ldots, u_{v'_i}]^\tau$. Then, $\mathbf{u}'_i = U_i\mathbf{u}''_i = U_{i,1}[u_1, \ldots, u_{v'_i - v_i}]^\tau + U_{i,2}[u_{v'_i - v_i + 1}, \ldots, u_{v'_i}]^\tau$. Take $\mathbf{u}_i = [u_{v'_i - v_i + 1}, \ldots, u_{v'_i}]^\tau$. Then, $\mathbf{u}'_i = U_{i,2}\mathbf{u}_i \bmod (\bigcup_{j=0}^{l-i} x^j U_{i,1})_{\mathbb{Z}}$, $G_i\mathbf{u}_i = P_iU_{i,2}\mathbf{u}_i = P_i\mathbf{u}'_i = 0$.

For simplicity, denote $\mathbf{u}_i$ as $\mathbf{u}_i = [u_1, \ldots, u_{v_i}]^\tau$. Then $\deg(u_{v_i}) \leq l - i - 1$ and $\deg(u_j) \leq l - i$ for $1 \leq j < v_i$. Let $u_j = u_{j,0} + p_jx$ for $1 \leq j < v_i$, where $u_{j,0} \in \mathbb{Z}$ and $p_j \in \mathbb{Z}[x]$ and $\deg(p_j) \leq \deg(u_j) - 1 \leq l - i - 1$. Take $\mathbf{u}'_{i+1} = [u_{1,0}, p_1, \ldots, u_{v_i-1,0}, p_{v_i-1}, u_{v_i}]^\tau$. Then $\deg(\mathbf{u}'_{i+1}) \leq l - i - 1$ and $\mathbf{u}_i = X_{i+1}\mathbf{u}'_{i+1}$. Hence, $\mathbf{u} = \varphi_{i+1}(\mathbf{u}'_{i+1}) \bmod (\bigcup_{k=0}^{i}\bigcup_{j=0}^{l-k} x^j\varphi_k(U_{k,1}))_{\mathbb{Z}}$ and $P_{i+1}\mathbf{u}'_{i+1} = G_iX_{i+1}\mathbf{u}'_{i+1} = G_i\mathbf{u}_i = 0$. The lemma is proved. □

4.3. The $\mathbb{Z}[x]^n$ case

In this section, an algorithm will be given to compute the GHNFs for $\mathbb{Z}[x]$-lattices in $\mathbb{Z}[x]^n$, which is a generalization of Algorithm GHNF_1.

In this section, we assume $F = (f_{ij})_{n\times m} = [\mathbf{f}_1, \ldots, \mathbf{f}_m] \in \mathbb{Z}[x]^{n\times m}$ and denote by $m = \#(F)$ the number of columns of F. Let $v_i = \max_{1\leq j\leq m}(\deg(f_{ij}))$, $i = 1, \ldots, n$, and

$$\mathbb{X}_F = \begin{pmatrix} 1 & x & \ldots & x^{v_1} & & & & & & & & & \\ & & & & 1 & x & \ldots & x^{v_2} & & & & & \\ & & & & & & & & \ddots & & & & \\ & & & & & & & & & 1 & x & \ldots & x^{v_n} \end{pmatrix}_{n\times s}, \tag{16}$$

where $s = \sum_{i=1}^{n}(v_i + 1)$. Then, F can be written in the matrix form: $F = \mathbb{X}_F C$, where $C \in \mathbb{Z}^{s\times m}$ is called the *coefficient matrix* of F and is denoted by $C = \mathrm{CMAT}(F)$. Let $[\mathbf{0}, H] = C[U_1, U_2]$ be the HNF of C, where H has no zero columns and $\mathbf{0} = CU_1$ and $H = CU_2$. Then $F_1 = \mathbb{X}_F H$ is called the PHNF of F and is denoted by

$$F_1 = \mathrm{PHNF}(F) = \mathbb{X}_F H = \mathbb{X}_F CU_2 = FU_2. \tag{17}$$

For a matrix $M \in \mathbb{Z}[x]^{n\times m}$, denote $M(\cdot, i)$ to be the i-th column of M and $M(i, \cdot)$ to be the i-th row of M. For $\mathbf{f} \in \mathbb{Z}[x]^n$, denote $\mathbf{f}(t)$ to be the polynomial in the t-th row of $\mathbf{f}$. For $F = [\mathbf{f}_1, \ldots, \mathbf{f}_m] \in \mathbb{Z}[x]^{n\times m}$, define the operation Partition as follows

$$\mathrm{Partition}(F) = (Q_1, \ldots, Q_n),$$

where $Q_t = [\mathbf{f}_{k_{t,1}}, \ldots, \mathbf{f}_{k_{t,s_t}}] \in \mathbb{Z}[x]^{n\times s_t}$ is a matrix consisting of columns $\mathbf{f}_{k_{t,\ell}}$ of F, satisfying $\mathbf{f}_{k_{t,i}}(t) \neq 0$ and $\mathbf{f}_{k_{t,i}}(j) = 0$ for $i = 1, \ldots, s_t$ and $j > t$; and $Q_t = \emptyset$ if such $\mathbf{f}_{k_{t,\ell}}$ do not exist. In other words, Q_t consists of those columns $\mathbf{f}$ of F such that the t-th entry of $\mathbf{f}$ is non-zero and the j-th entry is zero for all $j > t$. Furthermore, it is always assumed that $\deg(\mathbf{f}_{k_{t,1}}(t)) \leq \cdots \leq \deg(\mathbf{f}_{k_{t,s_t}}(t))$. For $d \in \mathbb{N}$, denote

$$Q_t^{(d)} = [\mathbf{f}_{k_{t,1}}, \ldots, \mathbf{f}_{k_{t,s}}]$$

such that $\deg(\mathbf{f}_{k_{t,i}}(t)) \leq d$ for $i = 1, \ldots, s$ and $\deg(\mathbf{f}_{k_{t,j}}(t)) > d$ for $j = s + 1, \ldots, s_t$. We now give the algorithm.

Algorithm 2 $\mathrm{GHNF}_n(F)$.

Require: $F \in \mathbb{Z}[x]^{n\times m}$ and with $d = \deg(F)$.
Ensure: $G \in \mathbb{Z}[x]^{n\times s}$, which is the GHNF of F.
1: $G_0 = \mathrm{PHNF}(F)$, $k = 0$.
2: (loop) $k = k + 1$;
$(G_{k-1,1}, \ldots, G_{k-1,n}) = \mathrm{Partition}(G_{k-1})$.
$P_{k,t} = [G_{k-1,t}^{(d_t)}, xG_{k-1,t}^{(d_t-1)}]$, $t = 1, \ldots, n$, where $d_t = (n - t + 1)d$.
$P_k = [P_{k,1}, \ldots, P_{k,n}]$. $G_k = \mathrm{PHNF}(P_k)$.
If $G_k \neq G_{k-1}$, repeat Step 2.
3: For t from 1 to n, let $G_{k-1,t} = [\mathbf{g}_{k-1,1}, \ldots, \mathbf{g}_{k-1,k_t}]$, $P_t = [\mathbf{g}_{k-1,1}]$;
for j from 2 to k_t, if $\mathbf{LC}(\mathbf{g}_{k-1,j-1}(t)) \neq \mathbf{LC}(\mathbf{g}_{k-1,j}(t))$, $P_t = P_t \cup \{\overline{\mathbf{g}_{k-1,j}}^{P_t}\}$.
4: Return $G = [P_1, \ldots, P_n]$.

Note that the number d_t is from Theorem 3.21. We give the following illustrative example.

Example 4.15. Let $F = \begin{pmatrix} 6x+1 & 3x \\ 2x & 5x+1 \end{pmatrix}$. We have $d = 1$.

Step 1: $G_0 = \mathrm{PHNF}(F) = \begin{pmatrix} 24x+5 & -9x-2 \\ -2 & x+1 \end{pmatrix}$.

1-st loop: $(G_{0,1}, G_{0,2}) = \mathrm{Partition}(G_0)$, where

$$G_{0,1} = [\,],\ G_{0,2} = G_0. \text{ Also, we have } d_1 = 2, d_2 = 1.$$

$$P_{1,1} = [\,],\ P_{1,2} = \begin{pmatrix} 24x+5 & 24x^2+5x & -9x-2 \\ -2 & -2x & x+1 \end{pmatrix}.$$

$$P_1 = [P_{1,1}, P_{1,2}],\ G_1 = \mathrm{PHNF}(P_1) = \begin{pmatrix} 24x^2+11x+1 & -24x-5 & -9x-2 \\ 0 & 2 & x+1 \end{pmatrix}.$$

2-nd loop: $(G_{1,1}, G_{1,2}) = \mathrm{Partition}(G_1)$, where

$$G_{1,1} = \begin{pmatrix} 24x^2+11x+1 \\ 0 \end{pmatrix},\ G_{1,2} = \begin{pmatrix} -24x-5 & -9x-2 \\ 2 & x+1 \end{pmatrix}.$$

$$P_{2,1} = \begin{pmatrix} 24x^2+11x+1 \\ 0 \end{pmatrix},\ P_{2,2} = \begin{pmatrix} -24x-5 & -24x^2-5x & -9x-2 \\ 2 & 2x & x+1 \end{pmatrix}.$$

$$P_2 = [P_{2,1}, P_{2,2}],\ G_2 = \mathrm{PHNF}(P_2) = \begin{pmatrix} 24x^2+11x+1 & -24x-5 & -9x-2 \\ 0 & 2 & x+1 \end{pmatrix}.$$

$G_2 = G_1$ and the loop terminates.

In Step 3, we can easily get the GHNF of F: $G = G_2$.

Similar to GHNF_1, we consider the following "full prolongation"

$$\begin{aligned} &\widetilde{P}_{k,t} = [\widetilde{G}_{k-1,t}, x\widetilde{G}_{k-1,t}],\ t = 1, \ldots, n, \\ &\widetilde{P}_k = [\widetilde{P}_{k,1}, \ldots, \widetilde{P}_{k,n}] = [\widetilde{G}_{k-1}, x\widetilde{G}_{k-1}], \\ &\widetilde{G}_k = \mathrm{PHNF}(\widetilde{P}_k),\ \ [\widetilde{G}_{k,1}, \ldots, \widetilde{G}_{k,n}] = \mathrm{Partition}(\widetilde{G}_k), \end{aligned} \tag{18}$$

where $\widetilde{G}_0 = G_0$. Due to (10), it is easy to check that

$$(\widetilde{G}_k)_{\mathbb{Z}} = (\widetilde{P}_k)_{\mathbb{Z}} = (F \cup \{x^i F \mid i = 1, \ldots, k\})_{\mathbb{Z}}. \tag{19}$$

We define a new monomial order as follows: $x^\alpha \mathbf{e}_i \prec' x^\beta \mathbf{e}_j$ if and only if $\alpha < \beta$ or $\alpha = \beta$ and $i < j$. Similar to the order $\prec$, the order $\prec'$ can be extended to the polynomial vectors of $\mathbb{Z}[x]^n$. Moreover, the S-vector of $\mathbf{f}, \mathbf{g} \in \mathbb{Z}[x]^m$ is similar to the one described in (1). A nice 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 obtain the following result.

Lemma 4.16. *Let $F \in \mathbb{Z}[x]^{n\times m}$ and $d = \deg(F)$. Then $\mathbf{Syz}(F)$ has a Gröbner basis with degree $\le nd$ w.r.t. $\prec'$.*

Proof. Let $S = \{\mathbf{u} \mid \mathbf{u} \in \mathbf{Syz}(F),\ \ \deg(\mathbf{u}) \le nd\}$. By Theorem 3.18, S generates $\mathbf{Syz}(F)$. Then, S contains a Gröbner basis G of $\mathbf{Syz}(F)$ w.r.t. $\prec'$, since the S-vector of any $\mathbf{u}, \mathbf{v} \in S$ w.r.t. $\prec'$ is still in S. □

Let $F_{(t)} \in \mathbb{Z}[x]^{t\times m}$ be the last t rows of F and

$$S_t = \{\mathbf{u} \in \mathbb{Z}[x]^m \mid \mathbf{u} \in \mathbf{Syz}(F_{(t)}), \deg(\mathbf{u}) \le td\}. \tag{20}$$

By Lemma 4.16, S_t contains a Gröbner basis G_t with $\deg(G_t) \le td$. Then, for any $\mathbf{u} \in \mathbf{Syz}(F_{(t)})$ with $\deg(\mathbf{u}) \le k$, we have $\mathbf{u} \in (S_t, xS_t, \ldots, x^{\max(0,\ k-td)} S_t)_{\mathbb{Z}}$. Moreover, we have $(S_1)_{\mathbb{Z}[x]} \supseteq (S_2)_{\mathbb{Z}[x]} \supseteq \cdots \supseteq (S_n)_{\mathbb{Z}[x]}$.

Let $u_{k,t} = \#(G_{k,t}^{(d_t)})$, $v_{k,t} = \#(G_{k,t}^{(d_t-1)})$, $w_{k,t} = \#(G_{k,t})$, and $r_{k,t} = u_{k-1,t} + v_{k-1,t} = \#(P_{k,t})$. Define a matrix $X_{k,t} = (x_{i,j}) \in \mathbb{Z}[x]^{w_{k,t}\times r_{k,t}}$ as follows. If $G_{k,t} = [\,]$, then $X_{k,t} = [\,]$. Otherwise, $x_{i,i} = 1$ for $i = 1, \ldots, u_{k,t}$, $x_{i,u_{k,t}+i} = x$ for $i = 1, \ldots, v_{k,t}$, and all other $x_{i,j}$ are zero. Then, we have

$$P_{k,t} = G_{k-1,t} X_{k-1,t} \tag{21}$$

for any k and t. Let $M_k = \mathrm{CMAT}(P_k)$ and $[\mathbf{0}, H_k] = M_k U_k$ the HNF of M_k. From (17), we have $[\mathbf{0}, G_k] = P_k U_k$.

For each $k > 0$, let U_k be defined as above and $\widetilde{U}_{k,n}$ be the last $r_{k,n}$ rows of U_k. We rewrite $\widetilde{U}_{k,n}$ as $\widetilde{U}_{k,n} = [V_{k,1}, V_{k,2}]$, where $V_{k,1}$ consists of the column vectors of $\widetilde{U}_{k,n} \cap \mathbf{Syz}(F_{(1)})$. Let $Q_k = [P_{k,1}, \ldots, P_{k,n-1}]$ and $U_k = \begin{pmatrix} W_{k,1} & W_{k,2} \\ V_{k,1} & V_{k,2} \end{pmatrix}$. From $[\mathbf{0}, G_k] = P_k U_k$, we have

$$[\mathbf{0}, G_{k,1}, \ldots, G_{k,n-1}] = P_k \begin{pmatrix} W_{k,1} \\ V_{k,1} \end{pmatrix} = [Q_k, P_{k,n}] \begin{pmatrix} W_{k,1} \\ V_{k,1} \end{pmatrix} = Q_k W_{k,1} + P_{k,n} V_{k,1}.$$

$$G_{k,n} = P_k \begin{pmatrix} W_{k,2} \\ V_{k,2} \end{pmatrix} = [Q_k, P_{k,n}] \begin{pmatrix} W_{k,2} \\ V_{k,2} \end{pmatrix} = Q_k W_{k,2} + P_{k,n} V_{k,2}.$$

From the above equations, we have $G_{k,n}(n, \cdot) = P_{k,n}(n, \cdot) V_{k,2}$, since the elements in the last row of Q_k are all 0. Since $P_{k,n} V_{k,1} \in (P_k)_{\mathbb{Z}} = (G_k)_{\mathbb{Z}}$ and the last row of $P_{k,n} V_{k,1}$ is zero, we have

$$(P_{k,n} V_{k,1})_{\mathbb{Z}} \in (G_{k,1}, \ldots, G_{k,n-1})_{\mathbb{Z}}. \tag{22}$$

Similarly, $G_{k,n} - P_{k,n} V_{k,2} = Q_k W_{k,2} \in (G_{k,1}, \ldots, G_{k,n-1})_{\mathbb{Z}}$, that is, $G_{k,n} = P_{k,n} V_{k,2} \mod (G_{k,1}, \ldots, G_{k,n-1})_{\mathbb{Z}}$. Similar to the $\mathbb{Z}[x]$ case, for $k > 0$, we define a map ϕ_k:

$$\begin{aligned} \phi_k : \mathbb{Z}[x]^{r_{k,n}} &\to \mathbb{Z}[x]^m \\ \mathbf{u} &\mapsto V_{0,2} X_{1,n} \cdots V_{k-1,2} X_{k,n} \mathbf{u}, \end{aligned}$$

where $X_{k,n}$ is from (21). Let $P_{0,n} = F$, $r_{0,n} = m$ and $\phi_0 : \mathbb{Z}[x]^m \to \mathbb{Z}[x]^m$ be the identity map in particular. Thus, we have

$$G_{k,n}(n, \cdot) = P_{k,n}(n, \cdot) V_{k,2} = F(n, \cdot) V_{0,2} X_{1,n} \cdots V_{k-1,2} X_{k,n} V_{k,2},$$

$$P_{k,n}(n, \cdot) = G_{k-1,n}(n, \cdot) X_{k-1,n} = F(n, \cdot) V_{0,2} X_{1,n} \cdots V_{k-1,2} X_{k,n}.$$

From (22), we have

$$F\phi_k(V_{k,1}) = F V_{0,2} X_{1,n} \cdots V_{k-1,2} X_{k,n} V_{k,1} = P_{k,n} V_{k,1} \subset (G_{k,1}, \ldots, G_{k,n-1})_{\mathbb{Z}} \tag{23}$$

for each $k \geq 0$. Hence, $\phi_k(V_{k,1}) \subset \mathbf{Syz}(F_{(1)})$.

Lemma 4.17. *Let $F \in \mathbb{Z}[x]^{n \times m}$. For any $\mathbf{u} \in \mathbf{Syz}(F_{(1)})$ and $\deg(\mathbf{u}) = l > 0$, we have $\mathbf{u} \in (\bigcup_{k=0}^{l} \bigcup_{j=0}^{l-k} x^j \phi_k(V_{k,1}))_{\mathbb{Z}}$ for $k > 0$. Moreover, if $l \leq d$, we have $F\mathbf{u} \in (G_{l,1}, \ldots, G_{l,n-1})_{\mathbb{Z}}$.*

Proof. The proof of the first statement is similar to the proof of Proposition 4.14. Assume $l \leq d$. We have $x^j (G_{k,1}, \ldots, G_{k,n-1})_{\mathbb{Z}} \subset (G_{k+j,1}, \ldots, G_{k+j,n-1})_{\mathbb{Z}}$ for any $j \leq d-k$, by our prolongation. By (23), we have $F\mathbf{u} \in (\bigcup_{k=0}^{l} \bigcup_{j=0}^{l-k} x^j F\phi_k(V_{k,1}))_{\mathbb{Z}} \subset (\bigcup_{k=0}^{l} \bigcup_{j=0}^{l-k} x^j (G_{k,1}, \ldots, G_{k,n-1})_{\mathbb{Z}})_{\mathbb{Z}} \subset (G_{l,1}, \ldots, G_{l,n-1})_{\mathbb{Z}}$. □

Lemma 4.18. *For any $1 \leq s \leq n-1$, we have $G_{k,j} = \widetilde{G}_{k,j}$ for $k \leq sd$ and $1 \leq j \leq n-s$.*

Proof. First, let $s = 1$. $G_0 = \widetilde{G}_0 = FU_{0,2}$. Then, $G_{0,j} = \widetilde{G}_{0,j}$ for $1 \leq j \leq n$. This lemma is valid for $k = 0$. Suppose it is valid for $k = l < d$, i.e., $G_{l,j} = \widetilde{G}_{l,j}$ for $1 \leq j \leq n-1$. We need to show $G_{l+1,j} = \widetilde{G}_{l+1,j}$ for $1 \leq j \leq n-1$. For any $\mathbf{f} \in (\widetilde{G}_{l+1,1}, \ldots, \widetilde{G}_{l+1,n-1})_{\mathbb{Z}} \subset (\widetilde{P}_{l+1})_{\mathbb{Z}} = (F, xF, \ldots, x^{l+1}F)_{\mathbb{Z}}$, there exists a $\mathbf{u} \in \mathbb{Z}[x]^m$, such that $\mathbf{f} = F\mathbf{u}$ with $\deg(\mathbf{u}) \leq l+1$, and $\mathbf{u} \in \mathbf{Syz}(F_{(1)})$. By Lemma 4.17, we have $\mathbf{f} = F\mathbf{u} \in (G_{l+1,1}, \ldots, G_{l+1,n-1})_{\mathbb{Z}}$. Thus, we have $G_{l+1,j} = \widetilde{G}_{l+1,j}$ for $1 \leq j \leq n-1$, since $G_{l+1,j} \subset \widetilde{G}_{l+1,j}$ and both of them are reduced $\mathbb{Z}$-Gröbner bases. The lemma is valid for $s = 1$.

Suppose the lemma is valid for $s = p-1$. Then we have $G_{(p-1)d,j} = \widetilde{G}_{(p-1)d,j}$ for $1 \leq j \leq n-p+1$. By (20) and (19), $FS_{p-1} \subset (\widetilde{G}_{(p-1)d,1}, \ldots, \widetilde{G}_{(p-1)d,n-p+1})_{\mathbb{Z}} = (F')_{\mathbb{Z}}$, where $F' = [G_{(p-1)d,1}, \ldots, G_{(p-1)d,n-p+1}]$.

When $s = p$, for any $(p-1)d < k \leq pd$ and $\mathbf{f} \in (\widetilde{G}_{k,1}, \ldots, \widetilde{G}_{k,n-p})_{\mathbb{Z}} \subset (\widetilde{P}_k)_{\mathbb{Z}}$, there exists a $\mathbf{u} \in \mathbb{Z}[x]^m$ with $\deg(\mathbf{u}) \leq k$, such that $\mathbf{f} = F\mathbf{u}$ and $\mathbf{u} \in \mathbf{Syz}(F_{(p)}) \subset \mathbf{Syz}(F_{(p-1)})$. By Lemma 4.16, $\mathbf{u} \in (S_{p-1})_{\mathbb{Z}[x]}$ and $\mathbf{u} \in (S_{p-1}, \ldots, x^{k-(p-1)d} S_{p-1})_{\mathbb{Z}}$. Then, $\mathbf{f} = F\mathbf{u} \in (F', \ldots, x^{k-(p-1)d} F')_{\mathbb{Z}}$. Hence we have $\mathbf{f} = F'\mathbf{v}$ for some $\mathbf{v} \in \mathbf{Syz}(F'_{(p)})$ with $\deg(\mathbf{v}) \leq k-(p-1)d \leq d$ and $F'_{(p)}$ being the last p rows of F'. Since the last $p-1$ rows of F' are all zeros, it can be reduced to the $s = 1$ case. Considering the algorithm $\mathrm{GHNF}_n(F')$ and the analysis for the $s = 1$ case, we have $\mathbf{f} = F\mathbf{v}' \in (G_{k,1}, \ldots, G_{k,n-p})_{\mathbb{Z}}$. Thus, $G_{k,j} = \widetilde{G}_{k,j}$ for $1 \leq j \leq n-p$. □

The following lemma asserts that the last s rows of $\widetilde{P}_k$ do not contribute to the first $(n-s)$ rows of $\widetilde{G}_k$ for $k > sd$.

Lemma 4.19. *Let $R = [G_{sd,1}, \ldots, G_{sd,n-s}]$. Then we have $\widetilde{G}_{k,n-s} \subset (R)_{\mathbb{Z}[x]}$ for $1 \leq s \leq n-1$ and $k > sd$. In particular, $\widetilde{G}_{k,n-s} \subset (R, xR, \ldots, x^{k-sd}R)_{\mathbb{Z}} \subset (\widetilde{P}_{k,1}, \ldots, \widetilde{P}_{k,n-s})_{\mathbb{Z}}$ for $1 \leq s \leq n-1$ and $k > sd$.*

Proof. Let $k > sd$. For any $\mathbf{f} \in \widetilde{G}_{k,n-s} \subset (\widetilde{P}_k)_{\mathbb{Z}}$, there exists a $\mathbf{u} \in \mathbf{Syz}(F_{(t)})$ with $\deg(\mathbf{u}) \le k$, such that $\mathbf{f} = F\mathbf{u}$. By Theorem 3.18, $\mathbf{u} \in (S_s)_{\mathbb{Z}[x]}$. By Lemma 4.16, $\mathbf{u} \in (S_s, \ldots, x^{k-sd}S_s)_{\mathbb{Z}}$. By Lemma 4.18, $G_{sd,j} = \widetilde{G}_{sd,j}$ for $1 \le j \le n-s$, $1 \le s < n$. Then, by (20) and (19), $FS_s \subset (\widetilde{G}_{sd,1}, \ldots, \widetilde{G}_{sd,n-s})_{\mathbb{Z}} = (R)_{\mathbb{Z}}$. Thus, $\mathbf{f} = F\mathbf{u} \subset (R, xR, \ldots, x^{k-sd}R)_{\mathbb{Z}} \subset (R)_{\mathbb{Z}[x]}$.

To show the second statement, first, let $k = sd+1$. We have $\mathbf{f} \in (R, xR)_{\mathbb{Z}} = (\widetilde{P}_{td+1,1}, \ldots, \widetilde{P}_{sd+1,n-s})_{\mathbb{Z}}$. The lemma is valid for $k = sd+1$. Suppose the lemma is valid for $k = l > sd$. Then, $\widetilde{G}_{l,n-s} \subset (R, xR, \ldots, x^{l-sd}R)_{\mathbb{Z}} \subset (\widetilde{P}_{l,1}, \ldots, \widetilde{P}_{l,n-s})_{\mathbb{Z}}$. We need to show $\widetilde{G}_{l+1,n-s} \subset (\widetilde{P}_{l+1,1}, \ldots, \widetilde{P}_{l+1,n-s})_{\mathbb{Z}}$. For any $\mathbf{f} \in \widetilde{G}_{l+1,n-s}$, we have $\mathbf{f} \in (R, xR, \ldots, x^{l-sd+1}R)_{\mathbb{Z}} = ((R, xR, \ldots, x^{l-sd}R) \cup x(R, xR, \ldots, x^{l-sd}R))_{\mathbb{Z}} \subset (\widetilde{G}_{l,1}, \ldots, \widetilde{G}_{l,n-s}, x\widetilde{G}_{l,1}, \ldots, x\widetilde{G}_{l,n-s})_{\mathbb{Z}} = (\widetilde{P}_{l+1,1}, \ldots, \widetilde{P}_{l+1,n-s})_{\mathbb{Z}}$. The lemma is also valid for $k = l+1$. □

Lemma 4.20. *For any $k \ge 1$ and $1 \le t \le m$, let $R_{k,t} = [\widetilde{G}^{(d_t)}_{k-1,t}, x\widetilde{G}^{(\widetilde{p}_{k-1,t}-1)}_{k-1,t}]$, where $\widetilde{p}_{k-1,t} = \max(d_t, \max_{\mathbf{g}\in\widetilde{G}_{k-1,t}} \deg(\mathbf{g}(t)))$. Then we have $\mathbf{f} \in (R_{k,1}, \ldots, R_{k,n-s})_{\mathbb{Z}}$ whenever $\mathbf{f} = [f_1, \ldots, f_{n-s}, 0, \ldots, 0]^\tau \in (\widetilde{P}_{k,1}, \ldots, \widetilde{P}_{k,n-s})_{\mathbb{Z}}$.*

Proof. First, let $s = n-1$. If $k \le (n-1)d$, by Lemma 4.18, we have $R_{k,1} = \widetilde{P}_{k,1}$. Then, $\mathbf{f} \in (\widetilde{P}_{k,1})_{\mathbb{Z}} = (R_{k,1})_{\mathbb{Z}}$. Otherwise, $k > (n-1)d$, by Lemma 4.19, $\mathbf{f} \in (\widetilde{P}_{k,1})_{\mathbb{Z}} \subset (G_{(n-1)d,1})_{\mathbb{Z}[x]}$. By Lemma 4.7, $(\widetilde{P}_{k,1})_{\mathbb{Z}} = (R_{k,1})_{\mathbb{Z}}$. The lemma is valid for $s = n-1$.

Suppose the lemma is valid for $s = l+1 \le n-1$, i.e. for any $k > 0$ and $\mathbf{f} \in (\widetilde{P}_{k,1}, \ldots, \widetilde{P}_{k,n-l-1})_{\mathbb{Z}}$, $\mathbf{f} \in (R_{k,1}, \ldots, R_{k,n-l-1})_{\mathbb{Z}}$. Let $s = l$, $\mathbf{f} = [f_1, \ldots, f_{n-l}, 0, \ldots, 0]^\tau \in (\widetilde{P}_{k,1}, \ldots, \widetilde{P}_{k,n-l})_{\mathbb{Z}}$. If $k \le ld$, then, $R_{k,j} = \widetilde{P}_{k,j}$ for $1 \le j \le n-l$. Thus, $\mathbf{f} \in (R_{k,1}, \ldots, R_{k,n-l})_{\mathbb{Z}}$. Otherwise, $k > ld$. If $f_{n-l} = 0$, $\mathbf{f} \in (\widetilde{G}_{k,1}, \ldots, \widetilde{G}_{k,n-l-1})_{\mathbb{Z}}$. In this case, if $k \le (l+1)d$, $R_{k,j} = \widetilde{P}_{k,j} = P_{k,j}$ for $1 \le j \le n-l-1$ by Lemma 4.18. $\mathbf{f} \in (\widetilde{P}_{k,1}, \ldots, \widetilde{P}_{k,n-l})_{\mathbb{Z}} = (R_{k,1}, \ldots, R_{k,n-l-1}, \widetilde{P}_{k,n-l})_{\mathbb{Z}} \subset (R_{k,1}, \ldots, R_{k,n-l})_{\mathbb{Z}}$ by Lemmas 4.7 and 4.17. If $k > (l+1)d$, by Lemma 4.19, $\mathbf{f} \in (\widetilde{P}_{k,1}, \ldots, \widetilde{P}_{k,n-l-1})_{\mathbb{Z}}$. By the induction hypothesis, $\mathbf{f} \in (R_{k,1}, \ldots, R_{k,n-l-1})_{\mathbb{Z}}$. If $f_{n-l} \ne 0$, by Lemma 4.19 we have $\mathbf{f} \in (\widetilde{P}_{k,1}, \ldots, \widetilde{P}_{k,n-l})_{\mathbb{Z}} \subset (G_{ld,1}, \ldots, G_{ld,n-l})_{\mathbb{Z}[x]}$. Then, for $k > ld$ we have $\mathbf{f} \in (\widetilde{P}_{k,1}, \ldots, \widetilde{P}_{k,n-l-1}, R_{k,n-l})_{\mathbb{Z}}$ by Lemmas 4.7 and 4.17. Thus, by induction, $\mathbf{f} \in (R_{k,1}, \ldots, R_{k,n-l})_{\mathbb{Z}}$. The lemma is proved. □

Lemma 4.21. *We have $G^{(d_t)}_{k,t}(t,\cdot) = \widetilde{G}^{(d_t)}_{k,t}(t,\cdot)$ for any $k \ge 0$, $1 \le t \le n$.*

Proof. Note that $d_n = d$ and for the n-th row of F, Algorithm GHNF$_n$ and Algorithm GHNF$_1$ are exactly the same. Hence, by Lemma 4.8, we have $G^{(d_n)}_{k,n}(n,\cdot) = \widetilde{G}^{(d_n)}_{k,n}(n,\cdot)$ for any $k \ge 0$. Set $s = n-t$ in Lemma 4.18, we have $G_{k,j} = \widetilde{G}_{k,j}$ for any $1 \le t \le n-1$, $k \le (n-t)d$, and $1 \le j \le t$. We thus proved the lemma when $k \le (n-t)d$. Set $s = n-t$ in Lemmas 4.19 and 4.20, we have $\widetilde{G}_{k,t} \subset (\widetilde{P}_{k,1}, \ldots, \widetilde{P}_{k,t})_{\mathbb{Z}} \subset (R_{k,1}, \ldots, R_{k,t})_{\mathbb{Z}}$ for $1 \le t \le n-1$ and $k > (n-t)d$. Note that Lemma 4.20 is the analog of Lemma 4.7 in the case of $n > 1$. Thus, similar to Lemma 4.8, we can prove $G^{(d_t)}_{k,t}(t,\cdot) = \widetilde{G}^{(d_t)}_{k,t}(t,\cdot)$ for $k > (n-t)d$. The lemma is proved. □

Lemma 4.22. *Suppose Step 2 of Algorithm GHNF$_n$ terminates at the k-th loop and let $\mathbf{g}_{k,t,d_t}$ be the last column vector of $G^{(d_t)}_{k,t}$. Then $\deg(\mathbf{g}_{k,t,d_t}) = d_t$ and for any $i \ge 0$, $(\widetilde{G}_i)_{\mathbb{Z}} \subset (H_{i,1}, \ldots, H_{i,n})_{\mathbb{Z}}$, where $H_{i,t} = (G^{(d_t)}_{k,t}, x\mathbf{g}_{k,t,d_t}, \ldots, x^{\max(i,k)-(n-t)d}\mathbf{g}_{k,t,d_t})$.*

Proof. It is sufficient to show $\widetilde{G}_{i,t} \subset (H_{i,1}, \ldots, H_{i,t})_{\mathbb{Z}}$ for any $i \ge 0$ and $1 \le t \le n$. If $\deg(G_{k-1,t}) < d_t$, then $\deg(G_{k,t}) \ge \deg(P_{k,t}) > \deg(G_{k-1,t})$ and the algorithm does not terminate. Therefore, if $G_{k,t} \ne \emptyset$, then we have $k \ge d_t - d = (n-t)d$ and hence $\deg(\mathbf{g}_{k,t,d_t}) = d_t$.

First, let $t = 1$. Clearly, for any $i \le (n-1)d$, $\widetilde{G}_{i,1} = G_{i,1} \subset (G^{(d_1)}_{k,1})_{\mathbb{Z}}$, where $=$ is based on Lemma 4.18 and $\subset$ is valid because $(G^{(d_1)}_{j,1})_{\mathbb{Z}} \subset (G^{(d_1)}_{j+1,1})_{\mathbb{Z}}$ for any $j \ge 0$. Thus, we have $\widetilde{G}_{(n-1)d,1} = G_{(n-1)d,1} \subset (G^{(d_1)}_{k,1})_{\mathbb{Z}} \subset (H_{(n-1)d,1})_{\mathbb{Z}}$. Suppose it is valid for $i = j > (n-1)d$. From (18) and Lemma 4.19, $(\widetilde{G}_{j+1,1})_{\mathbb{Z}} = (\widetilde{G}_{j,1}, x\widetilde{G}_{j,1})_{\mathbb{Z}}$. By induction hypothesis, $\widetilde{G}_{j,1} \subset (H_{j,1})_{\mathbb{Z}}$ where $H_{j,1} = (G^{(d_1)}_{k,1}, x\mathbf{g}_{k,1,d_1}, \ldots, x^{\max(j,k)-(n-1)d}\mathbf{g}_{k,1,d_1})_{\mathbb{Z}}$. Then, any $\mathbf{g} \in \widetilde{G}_{j,1}$ can be written as $\mathbf{g} = \mathbf{g}_0 + \sum_{l=0}^{\max(j,k)-(n-1)d} c_l x^l \mathbf{g}_{k,1,d_1}$, where $\mathbf{g}_0 \in G^{(d_1-1)}_{k,1}$ and $c_l \in \mathbb{Z}$. Since $x\mathbf{g}_0 \in (xG^{(d_1-1)}_{k,1})_{\mathbb{Z}} \subset (G^{(d_1)}_{k+1,1})_{\mathbb{Z}} = (G^{(d_1)}_{k,1})_{\mathbb{Z}}$, we have $(\widetilde{G}_{j+1,1})_{\mathbb{Z}} \subset (G^{(d_1)}_{k,1}, x\mathbf{g}_{k,1,d_1}, \ldots, x^{\max(j+1,k)-(n-1)d}\mathbf{g}_{k,1,d_1})_{\mathbb{Z}}$. The lemma is valid for any $i \ge 0$ and $t = 1$.

Suppose the lemma is valid for any $i \ge 0$ and $t \le s < n$. Then $(G_{j,1}, \ldots, G_{j,s})_{\mathbb{Z}} \subset (\widetilde{G}_{j,1}, \ldots, \widetilde{G}_{j,s})_{\mathbb{Z}} \subset (H_{j,1}, \ldots, H_{j,s})_{\mathbb{Z}}$ for any $j \ge 0$.

By induction, $(\widetilde{G}_{i,1}, \ldots, \widetilde{G}_{i,s+1})_{\mathbb{Z}} = (G_{i,1}, \ldots, G_{i,s+1})_{\mathbb{Z}} \subset (H_{i,1}, \ldots, H_{i,s}, G_{i,s+1})_{\mathbb{Z}}$ for $i \le (n-s-1)d$. Moreover, $(G^{(d_{s+1})}_{i,s+1})_{\mathbb{Z}} \subset (G_{i+1,1}, \ldots, G_{i+1,s}, G^{(d_{s+1})}_{i+1,s+1})_{\mathbb{Z}} \subset (H_{i+1,1}, \ldots, H_{i+1,s}, G^{(d_{s+1})}_{i+1,s+1})_{\mathbb{Z}}$ for any $i \ge 0$. Since $d+i \le d_{s+1}$ and $H_{j,t} = H_{k,t}$ for any $j \le k$ and $1 \le t \le n$, we have $(\widetilde{G}_{i,1}, \ldots, \widetilde{G}_{i,s+1})_{\mathbb{Z}} \subset (H_{k,1}, \ldots, H_{k,s}, G^{(d_{s+1})}_{k,s+1})_{\mathbb{Z}} \subset (H_{i,1}, \ldots, H_{i,s}, H_{i,s+1})_{\mathbb{Z}}$ and the lemma is valid for $i \le (n-s-1)d$.

Suppose the lemma is valid for $i = j > (n-s-1)d$. From (18), $(\widetilde{G}_{j+1,s+1})_{\mathbb{Z}} = (\widetilde{G}_{j,s+1}, x\widetilde{G}_{j,s+1})_{\mathbb{Z}}$. By the induction hypothesis, $\widetilde{G}_{j,s+1} \subset (H_{j,1}, \ldots, H_{j,s+1})_{\mathbb{Z}}$. Then, any $\mathbf{g} \in \widetilde{G}_{j,s+1}$ can be written as $\mathbf{g} = \sum_{t=1}^{s+1}(\mathbf{g}_{t,0} + \sum_{l=0}^{\max(j,k)-(n-t)d} c_{t,l}x^l\mathbf{g}_{k,t,d_t})$, where $\mathbf{g}_{t,0} \in G^{(d_t-1)}_{k,t}$, and $c_{t,l} \in \mathbb{Z}$. Moreover, since for any $i \ge 0$ and $t \le s+1$, $(G^{(d_t)}_{i,t})_{\mathbb{Z}} \subset (G_{i+1,1}, \ldots, G_{i+1,t-1}, G^{(d_t)}_{i+1,t})_{\mathbb{Z}} \subset$

$(H_{i+1,1}, \dots, H_{i+1,t-1}, G^{(d_t)}_{i+1,t})_{\mathbb{Z}}$, we have $x\mathbf{g}_{t,0} \in (G_{k+1,1}, \dots, G_{k+1,t-1}, G^{(d_t)}_{k+1,t})_{\mathbb{Z}} \subset (H_{k+1,1}, \dots, H_{k+1,t-1}, G^{(d_t)}_{k+1,t})_{\mathbb{Z}} = (H_{k+1,1}, \dots, H_{k+1,t-1}, G^{(d_t)}_{k,t})_{\mathbb{Z}}$. Then, $(\widetilde{G}_{j+1,s+1})_{\mathbb{Z}} \subset (H_{k+1,1}, \dots, H_{k+1,s+1})_{\mathbb{Z}}$. Since $\deg(\widetilde{G}_{j+1,s+1}) \le d + j + 1$, we have $(\widetilde{G}_{j+1,s+1})_{\mathbb{Z}} \subset (H_{j+1,1}, \dots, H_{j+1,s+1})_{\mathbb{Z}}$. □

Notice that in the proof of Lemma 4.22, we need only $G^{(d_t)}_{k,t} = G^{(d_t)}_{k+1,t}$ for $1 \le t \le n$. Then, we have the following corollary.

Corollary 4.23. *In the Algorithm* GHNF$_n$*, if $G^{(d_t)}_{k,t} = G^{(d_t)}_{k+1,t}$ for $1 \le t \le s$ for some positive integer $s \le n$, then $(\widetilde{G}_{i,s})_{\mathbb{Z}} \in (H_{i,1}, \dots, H_{i,s})_{\mathbb{Z}}$, where $H_{i,t} = (G^{(d_t)}_{k,t}, x\mathbf{g}_{k,t,d_t}, \dots, x^{\max(i,k)-(n-t)d}\mathbf{g}_{k,t,d_t})_{\mathbb{Z}}$ for any $i \ge 0$, $1 \le t \le s$.*

By this result, we obtain an equivalent termination condition for the Algorithm GHNF$_n$:

Lemma 4.24. *In the Algorithm* GHNF$_n$*, $G_k = G_{k+1}$ is equivalent to $G_{k,t}(t,\cdot) = G_{k+1,t}(t,\cdot)$ for $1 \le t \le n$.*

Proof. Clearly, if $G_k = G_{k+1}$, we have $G_{k,t}(t,\cdot) = G_{k+1,t}(t,\cdot)$ for $1 \le t \le n$. We just need to show the opposite direction. In this condition, we prove $G_{k,t} = G_{k+1,t}$ by induction on t. Since $G_{j,1}(1,\cdot) = G_{j,1}$ for any j, the lemma is valid for $t = 1$. Suppose $G_{k,t} = G_{k+1,t}$ for $1 \le t \le s < n$. Since $G_{k,t}(t,\cdot) = G_{k+1,t}(t,\cdot)$ for $1 \le t \le n$, for any $\mathbf{g}' \in G_{k+1,s+1}$, there exists a $\mathbf{g} \in G_{k,s+1}$ satisfying $\mathbf{g}(s+1) = \mathbf{g}'(s+1)$. If $\mathbf{g} \in G^{(d_{s+1})}_{k,s+1}$, we have $\mathbf{g} \in (G_{k+1})_{\mathbb{Z}}$. Then, $\mathbf{g} - \mathbf{g}' \in (G_{k+1})_{\mathbb{Z}}$. Since $(\mathbf{g} - \mathbf{g}')(t) = 0$ for $s+1 \le t \le n$, we have $\mathbf{g} - \mathbf{g}' \in (G_{k+1,1}, \dots, G_{k+1,s})_{\mathbb{Z}} = (G_{k,1}, \dots, G_{k,s})_{\mathbb{Z}}$. Thus, $\mathbf{g}' \in (G_{k,1}, \dots, G^{(d_{s+1})}_{k,s+1})_{\mathbb{Z}}$ and $(G_{k+1,1}, \dots, G_{k+1,s}, G^{(d_{s+1})}_{k+1,s+1})_{\mathbb{Z}} = (G_{k,1}, \dots, G_{k,s}, G^{(d_{s+1})}_{k,s+1})_{\mathbb{Z}}$. Then, $G^{(d_{s+1})}_{k,s+1} = G^{(d_{s+1})}_{k+1,s+1}$ since both of them are reduced $\mathbb{Z}$-Gröbner bases. If $\mathbf{g} \notin G^{(d_{s+1})}_{k,s+1}$, we have $\mathbf{g} \in (G_{k,1}, \dots, G_{k,s}, G^{(d_{s+1})}_{k,s+1}, x\mathbf{g}_{k,s+1,d_{s+1}}, \dots, x^l\mathbf{g}_{k,s+1,d_{s+1}})_{\mathbb{Z}}$ for some $l \ge 0$ by Corollary 4.23. So is $\mathbf{g}'$ since $G^{(d_{s+1})}_{k,s+1} = G^{(d_{s+1})}_{k+1,s+1}$. Thus we have $\mathbf{g} - \mathbf{g}' \in (G_{k,1}, \dots, G_{k,s})$ since $(G_{k,1}, \dots, G_{k,s}, G^{(d_{s+1})}_{k,s+1}, x\mathbf{g}_{k,s+1,d_{s+1}}, \dots, x^l\mathbf{g}_{k,s+1,d_{s+1}})_{\mathbb{Z}}$ is a $\mathbb{Z}$-Gröbner basis. Then $(G_{k,1}, \dots, G_{k,s+1})_{\mathbb{Z}} = (G_{k+1,1}, \dots, G_{k+1,s+1})_{\mathbb{Z}}$. Since both of them are reduced $\mathbb{Z}$-Gröbner bases, we have $G_{k,s+1} = G_{k+1,s+1}$. □

We now show the correctness of the algorithm.

Theorem 4.25. *Algorithm* GHNF$_n$ *is correct. Furthermore, Step 2 of Algorithm* GHNF$_n$ *terminates in at most $D + nd$ loops, where $D = 73n^8d^5(h + \log(n^2d) + 1)$.*

Proof. Suppose Step 2 of the algorithm terminates in the k-th loop. The fact that G_k is a Gröbner basis of $(F)_{\mathbb{Z}[x]}$ can be proved similarly to that of Theorem 4.10, where instead of Lemma 4.9, we use Lemma 4.22.

We now prove the termination of the algorithm. By Theorem 3.23 and (19), $\widetilde{G}_D$ contains the GHNF of F and hence a Gröbner basis of $(F)_{\mathbb{Z}[x]}$ by Theorem 2.6. By Lemma 3.6, if $\mathscr{C}$ is the GHNF of F and has form (2), then $\deg(\mathscr{C}(r_i,\cdot)) \le d_{r_i} = (n - r_i + 1)d$, $i = 1, \dots, t$. Hence, G_D also contains a Gröbner basis of $(F)_{\mathbb{Z}[x]}$ by Lemma 4.21. Similar to the $\mathbb{Z}[x]$ case, the termination condition may not be satisfied immediately even if G_i is a Gröbner basis of $(F)_{\mathbb{Z}[x]}$. By Lemma 4.24, Algorithm GHNF$_n$ terminates at the $(k+1)$-th loop if and only if $G_{k,t}(t,\cdot) = G_{k+1,t}(t,\cdot)$ for $1 \le t \le n$. By Lemma 4.19 and Lemma 4.21, after the nd-th loop, $\deg(G_{i,t}(t,\cdot)) = d_t$ and the computation of $G_{i,t}(t,\cdot)$ only depends on $G_{i,t}(t,\cdot)$ for $1 \le t \le n$. Also note that if G_i is a Gröbner basis, then $G_{i,t}$ is either empty or a Gröbner basis. Then, similar to the proof of Theorem 4.10, we can show that after D-loop, $G_{i,t}(t,\cdot)$ are Gröbner bases for $t = 1, \dots, n$ and after that the loop terminates for at most $d_1 = dn$ extra steps. □

Theorem 4.26. *The worst bit size complexity of Algorithm* GHNF$_n$ *is*

$$O(n^{26+2\theta+\varepsilon}d^{15+\theta+\varepsilon}(h + \log(n^2d))^{4+\varepsilon} + n^{19}d^{11}(h + \log(n^2d))^2\log(n^2d)B(n^{11}d^6(h + \log(n^2d))^2)),$$

where $h = \mathrm{height}(F)$ and $\varepsilon > 0$ is a sufficiently small number.

Proof. In the k-th loop in Step 2, we need to compute the HNF of an integer matrix M_k whose size is $n(d + k + 1) \times s$, where $s \le (2d+1) + (4d+1) + \cdots + (2nd+1) = n(n+1)d + n$. By Theorems 4.3, 4.25, and (19), the height of $M_k \le n(D + nd + 1)(\frac{1}{2}\log(n(D + nd + 1)) + h) = O(n^9d^5(h + \log(n^2d))^2) := h_2$. The $\log\beta$ in Theorem 4.3 can be taken as $\log\beta = (n(n+1)d + n)(\frac{1}{2}\log(n(n+1)d + n) + h_2) = O(n^{11}d^6(h + \log(n^2d))^2)$. 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 a sufficiently small number ε. The complexity in the k-th loop is

$$\begin{aligned}
&O(n(d + k + 1) \cdot (n(n+1)d + n)^{\theta-1}(\log\beta)M(\log\log\beta)/(\log\log\beta)\\
&+ n(d + k + 1) \cdot (n(n+1)d + n)\log(n(n+1)d + n)B(\log\beta))\\
&= (d + k + 1)O(n^{10+2\theta+\varepsilon}d^{5+\theta+\varepsilon}(h + \log(n^2d))^{2+\varepsilon} + n^3d\log(n^2d)B(n^{11}d^6(h + \log(n^2d))^2)),
\end{aligned}$$

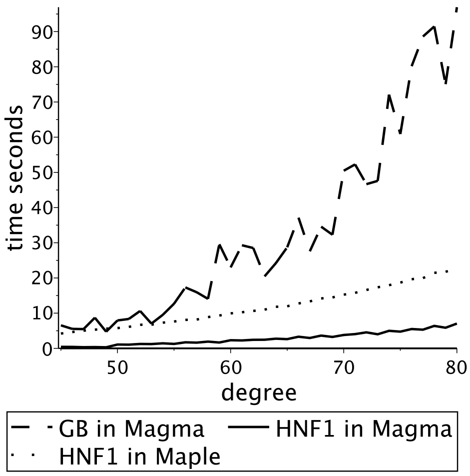

Fig. 1. Comparison of GHNF_1 and GröbnerBasis in Magma and Maple: the $\mathbb{Z}[x]$ case.

for any $\varepsilon > 0$. Hence the total complexity is

$$\sum_{k=0}^{D+nd}(d+k+1)\,O\left(n^{10+2\theta+\varepsilon}d^{5+\theta+\varepsilon}(h+\log(n^2d))^{2+\varepsilon}+n^3d\log(n^2d)B(n^{11}d^6(h+\log(n^2d))^2)\right)$$
$$= O\left(n^{26+2\theta+\varepsilon}d^{15+\theta+\varepsilon}(h+\log(n^2d))^{4+\varepsilon}+n^{19}d^{11}(h+\log(n^2d))^2\log(n^2d)B(n^{11}d^6(h+\log n^2d)^2)\right). \qquad \square$$

Similar to Corollary 4.12, by setting $\theta = 2.376$ and $\varepsilon = 0.001$, we have

Corollary 4.27. *The worst bit size complexity of Algorithm* GHNF_n *is* $O(n^{30.753}d^{17.377}(h+\log(n^2d))^{4.001})$.

Similar to Remark 4.13, 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 1.90 GHz. For each set of input parameters, we use the average timing of ten experiments for random polynomials with coefficients between $[-100, 100]$.

Fig. 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 4.11, the degree of the input polynomials is 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 have the following observations. The new 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 $xg_1, \ldots, xg_{t-1}$ instead of $xg_1, \ldots, xg_t$, the size of the coefficient matrices is nicely controlled. This fact is more important in Algorithm GHNF_n. Our second observation is that the complexity bound $O(d^{13.38}h^{2.004})$ in Corollary 4.12 is not reached in most cases and the algorithm terminates in a much smaller number of loops. So a further problem is to find a better complexity bound or the average complexity for the algorithm.

In Table 1, we give the timings for several inputs 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. The difference for the timings of Algorithm GHNF_1 in Magma and Maple is mainly due to the different implementations of the HNF algorithms.

Fig. 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 $n > 1$.

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

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

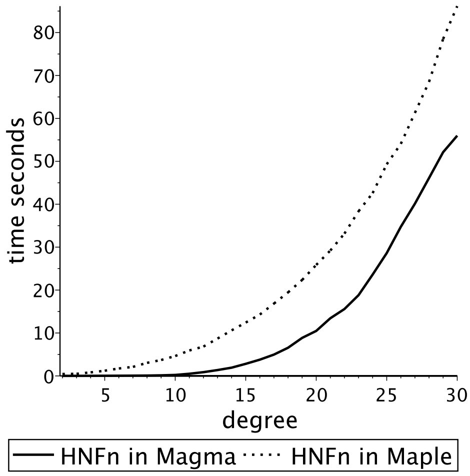

Fig. 2. Timings of $GHNF_n$ in Magma and Maple.

Table 2
Timings of $GHNF_n$ in Magma and Maple.

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

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

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 well-known F4 strategy to compute Gröbner bases, where a novel prolongation is designed so that the coefficient matrices under consideration have smaller sizes than existing methods. 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 and the complexity of the algorithm is obtained from these bounds. The algorithm is implemented in Maple and Magma and is shown to be more efficient than existing algorithms.

Acknowledgement

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

References

[1] M. Aschenbrenner, Ideal membership in polynomial rings over the integers, J. Amer. Math. Soc. 17 (2004) 407–441.
[2] B. Beckermann, G. Labahn, G. Villard, Normal forms for general polynomial matrices, J. Symbolic Comput. 41 (2006) 708–737.
[3] S. Bosch, U. Güntzer, R. Remmert, Non-Archimedean Analysis. A Systematic Approach to Rigid Analytic Geometry, Grundlehren Math. Wiss., Springer, Berlin, Heidelberg, 1984.
[4] 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, J. Symbolic Comput. 41 (2006) 475–511.
[5] H. Cohen, A Course in Computational Algebraic Number Theory, vol. 138, Springer Science & Business Media, 1993.
[6] D. Cox, J. Little, D. O'shea, Using Algebraic Geometry, Springer-Verlag, New York, 2005.
[7] D. Cox, J. Little, H. Schenck, Toric Varieties, Springer-Verlag, New York, 2010.

[8] N. Courtois, A. Klimov, J. Patarin, A. Shamir, Efficient algorithms for solving overdefined systems of multivariate polynomial equations, in: Eurocrypt 2000, in: Lecture Notes in Comput. Sci., vol. 1807, Springer, 2000, pp. 392–407.
[9] P.D. Domich, R. Kannan, L.E. Trotter Jr., Hermite normal form computation using modulo determinant arithmetic, Math. Oper. Res. 12 (1987) 50–59.
[10] D. Eisenbud, Commutative Algebra: With a View Toward Algebraic Geometry, Springer, 1995.
[11] J.C. Faugere, A new efficient algorithm for computing Gröbner bases (F4), J. Pure Appl. Algebra 139 (1999) 61–88.
[12] X.S. Gao, Z. Huang, C.M. Yuan, Binomial difference ideals, J. Symbolic Comput. 80 (3) (2017) 665–706.
[13] X.S. Gao, Z. Huang, J. Wang, C.M. Yuan, Toric difference variety, J. Syst. Sci. Complex. 30 (1) (2017) 173–195.
[14] A.O. Gelfond, Transcendental and Algebraic Numbers, Dover, New York, 1960.
[15] E. Kaltofen, M.S. Krishnamoorthy, B.D. Saunders, Fast parallel computation of Hermite and Smith forms of polynomial matrices, SIAM J. Algebr. Discrete Methods 8 (1987) 683–690.
[16] Ä. Kandri-Rody, D. Kapur, Computing a Gröbner basis of a polynomial ideal over a Euclidean domain, J. Symbolic Comput. 6 (1988) 37–57.
[17] R. Kannan, A. Bachem, Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix, SIAM J. Comput. 8 (1979) 499–507.
[18] D. Lazard, Ideal bases and primary decomposition: case of two variables, J. Symbolic Comput. 3 (1985) 261–270.
[19] D. Lichtblau, Revisiting Strong Gröbner Bases over Euclidean Domains, Wolfram Library Archive, 2003.
[20] E. Mayr, A. Meyer, The complexity of the word problems for commutative semigroups and polynomial ideals, Adv. Math. 46 (1982) 305–329.
[21] D. Micciancio, B. Warinschi, A linear space algorithm for computing the Hermite normal form, in: Proc. ISSAC'01, ACM Press, New York, 2001, pp. 231–236.
[22] T. Mulders, A. Storjohann, On lattice reduction for polynomial matrices, J. Symbolic Comput. 35 (2003) 377–401.
[23] A. Storjohann, Algorithms for Matrix Canonical Forms, PhD thesis, Swiss Federal Institute of Technology, 2013.
[24] A. Storjohann, G. Labahn, Asymptotically fast computation of Hermite normal forms of integer matrices, in: Proc. ISSAC'96, ACM Press, 1996, pp. 259–266.
[25] R. Zippel, Effective Polynomial Computation, Kluwer Academic Publishers, Boston, 1993.