PART II: Lattices and linear diophantine equations

By: Sandra Gregov

746 Combinatorial Optimization

Theory of lattices and linear diophantine equations
4.1. THE HERMITE NORMAL FORM

- A matrix of full row rank is in *Hermite normal form* if it has the form [B 0] where B is nonsingular, lower triangular, nonnegative matrix, in which each row has a unique maximum entry located on the main diagonal.

- *Elementary column operations:*
  I. Exchanging two columns
  II. Multiplying a column by -1
  III. Adding an integral multiple of one column to another column

Theory of lattices and linear diophantine equations
4.1. THE HERMITE NORMAL FORM

THEOREM 4.1: *Each rational matrix of full row rank can be brought into Hermite normal form by a series of elementary column operations.*

Proof: Let A be a rational matrix of full row rank. WLOG, A is integral. Suppose we have transformed A, by elementary column operations, to the form $\begin{bmatrix} \mathrm{B} & 0 \\ \mathrm{C} & D \end{bmatrix}$ where B is lower triangular with positive diagonal.

Using elementary column operations, modify D so that its first row $(\delta_{11},\ldots,\delta_{1k})$ is nonnegative, the sum $\delta_{11}+\ldots+\delta_{1k}$ is as small as possible. Assume that $\delta_{11} \geq \delta_{12} \geq \ldots \geq \delta_{1k}$. Then $\delta_{11} > 0$ since A has full row rank.

4.1. THE HERMITE NORMAL FORM

Moremore, if $\delta_{12} > 0$, by subtracting the second column of D from the first column of D, the first row will have smaller sum, contradicting our assumption. Hence, $\delta_{12} = \cdots = \delta_{1k} = 0$, and we have obtained a larger lower triangular matrix.

By repeating this procedure, the matrix A finally will be transformed into [B 0] with B=$\left(\beta_{\text{ij}}\right)$lower triangular with positive diagonal. Next:

for $i = 2,\ldots,n$ (order of B), for $\text{j} = 1,\ldots,i - 1$, add an integer multiple of the i-th column of B so that the (i, j)-th entry of B is nonnegative and less than β_{ii}. After these elementary column operations, the matrix is in Hermite normal form.

Corollary 4.1a. Let A be a rational matrix and let b be a rational column vector. Then the system $Ax = b$ has an integral solution $x \Leftrightarrow yb$ is an integer for each rational row vector y for which yA is integral.

Proof : If x and yA are integral vectors and $Ax = b$, then $yb = yAx$ is an integer. Suppose yb is an integer whenever yA is intgral. Then $Ax = b$ has a (possibly fractional) solution (if not, then $yA = 0$ and $yb = \frac{1}{2}$ for some rational vector y). Assume that the rows of A are linearly independent. Both sides of $\Leftrightarrow$ are invariant under elementary column operations. So by **THM 4.1** assume that A is in Hermite normal form $[B\ 0]$.

Theory of lattices and linear diophantine equations
4.1. THE HERMITE NORMAL FORM

Since $B^{-1}[B\ 0] = [I\ 0]$ is an integral matrix, it follows from our assumption that also $B^{-1}b$ is an integral vector.

Since $\begin{bmatrix} B & 0 \end{bmatrix}\begin{pmatrix} B^{-1}b \\ 0 \end{pmatrix} = b$ the vector $x := \begin{pmatrix} B^{-1}b \\ 0 \end{pmatrix}$ is an integral solution for $Ax = b$.

Theory of lattices and linear diophantine equations
4.1. THE HERMITE NORMAL FORM

A subset Λ of $\mathbb{R}^n$ is called an ***(additive) group*** if:

(i) $0 \in \Lambda$

(ii) if x, y $\in \Lambda$ then x+y $\in \Lambda$ and -x $\in \Lambda$.

The group is said to be ***generated*** by $a_1,\ldots,a_m$ if

$\Lambda=\left\{\lambda_1 a_1+\cdots+\lambda_m a_m \mid \lambda_1,\ldots,\lambda_m \in \mathbb{Z}\right\}$.

The group is called a ***lattice*** if it can be generated by linearly independent vectors. These vectors are called a ***basis*** for the lattice.

Corollary 4.1b. If $a_1,\ldots,a_m$ are rational vectors, then the group generated by $a_1,\ldots,a_m$ is a lattice, i.e, is generated by linearly independent vectors.

Proof : Assume that $a_1,\ldots,a_m$ span all space. (Otherwise we could apply a linear transformation to a lower dimensional space.) Let A be the matrix with columns $a_1,\ldots,a_m$ (so A has full row rank). Let $[B\ 0]$ be the Hermite normal form of A. Then the columns of B are linearly independent vectors generating the same group as $a_1,\ldots,a_m$.

Theory of lattices and linear diophantine equations
4.1. THE HERMITE NORMAL FORM

If $a_1,\ldots,a_m$ are rational vectors we can speak of the lattice generated by $a_1,\ldots,a_m$.

Given a rational matrix A, **Corollary 4.1a** gives necessary and sufficient conditions for being an element of the lattice Λ generated by the columns of A.

Corollary 4.1a implies that if A has full row rank, with Hermite normal form $[B\ \ 0]$ (B lower triangular), then b belongs to $\Lambda \Leftrightarrow B^{-1}b$ is integral.

Theory of lattices and linear diophantine equations
4.1. THE HERMITE NORMAL FORM

Corollary 4.1c. Let A be an integral $m \times n -$ matrix of full row rank.
Then the following are equivalent:

(i) the g.c.d. of the subdeterminants of A of order m is 1;

(ii) the system $Ax = b$ has an integral solution x, for each integral vector b;

(iii) for each vector y, if yA is integral then y is integral.

From the Hermite normal form theorem, for any rational system $Ax = b$ with at least one integral solution there exist integral vectors $x_0,\ x_1, \ldots,\ x_t$ such that

$$\{x \mid Ax = b; x \text{ integral}\} = \{x_0 + \lambda_1 x_1 + \cdots + \lambda_t x_t \mid \lambda_1, \ldots, \lambda_t \in \mathbb{Z}\}$$

where $x_1, \ldots,\ x_t$ are linearly independent and $t = (\#\ of\ columns\ of\ A) - rank(A)$.

4.2. UNIQUENESS OF THE HERMITE NORMAL FORM

Theorem 4.2. Let A and A' be rational matrices of full row rank, with Hermite normal forms $[B\ \ 0]$ and $[B'\ \ 0]$, respectively. Then the columns of A generate the same lattice as those of A' if and only if $B = B'$.

In other words, two lattices are equal $\Leftrightarrow$ their respective matrices have the same Hermite normal form.

Theory of lattices and linear diophantine equations
4.2. UNIQUENESS OF THE HERMITE NORMAL FORM

Proof : Sufficiency: The columns of B and A generate the same lattice, and similarly for B' and A'.

Necessity: Suppose the columns of A and those of A' generate the same lattice Λ. Then the same holds for B and B' (by elementary column operations from A & A'). Denote $B =: (\beta_{ij})$ and $B' =: (\beta'_{ij})$.

Suppose $B \neq B'$ and choose $\beta_{ij} \neq \beta'_{ij}$ with i as small as possible.

WLOG, $\beta_{ii} \geq \beta'_{ii}$. Let b_j and b'_j be the j-th column of B and B'.

Theory of lattices and linear diophantine equations
4.2. UNIQUENESS OF THE HERMITE NORMAL FORM

Then $b_j \in \Lambda$ and $b'_j \in \Lambda$, and hence $b_j - b'_j \in \Lambda$. This implies that $b_j - b'_j$ is an integral linear combination of the columns of B. By the choice of i, the vector $b_j - b'_j$ has zeros in the first (i-1) positions. Hence, as B is lower triangular, $b_j - b'_j$ is an integral linear combination of columns indexed i,...n. So $\beta_{ij} - \beta'_{ij}$ is an integral multiple of β_{ii}. However, this contradicts the fact that $0 < \left|\beta_{ij} - \beta'_{ij}\right| < \beta_{ii}$ (since if i=j, then $0 < \beta'_{ii} < \beta_{ii}$, and if j<i, then $0 \le \beta_{ij} < \beta_{ii}$ and $0 < \beta'_{ij} < \beta'_{ii} \le \beta_{ii}$).

4.2. UNIQUENESS OF THE HERMITE NORMAL FORM

Corollary 4.2a. Every rational matrix of full row rank has a unique Hermite normal form.

NOTE : If $\beta_{11},\ldots,\beta_{\mathrm{mm}}$ are the diagonal entries of Hermite normal form of [B 0] of A, then for each $j=1,\ldots,m$ the product $\beta_{11},\ldots,\beta_{\mathrm{jj}}$ is equal to the g.c.d. of the subdeterminants of order j of the first j rows of A (this g.c.d. is invariant under elementary column operations).

$\Rightarrow$ the main diagonal of the HNF is unique

$\Rightarrow$ size of HNF is polynomially bounded by the size of the original matrix

4.3. UNIMODULAR MATRICES

Definition : Let U be nonsingular matrix. Then U is called ***unimodular*** if U is integral and has determinant ± 1.

Theorem 4.3. The following are equivalent for a nonsingular rational matrix U of order n:

(i) U is unimodular;

(ii) U^{-1} is unimodular;

(iii) the lattice generated by the columns of U is $\mathbb{Z}^n$;

(iv) U has the identity matrix as its Hermite normal form;

(v) U comes from the identity matrix by elementary column operations.

Theory of lattices and linear diophantine equations
4.3. UNIMODULAR MATRICES

Corollary 4.3a. Let A and A' be nonsingular matrices. Then TFAE:

(i) the columns of A and of A' generate the same lattice;

(ii) A' comes from A by elementary column operations;

(iii) $A' = AU$ for some unimodular matrix U (A^{-1}A' is unimodular);

Corollary 4.3b. For each rational matrix A of full row rank there is a unimodular matrix U such that AU is the HNF of A. If A is nonsingular, U is unique.

Example. Consider the following matrices A, B, and U. Then BU is Hermite decomposition of A.

$$A = \begin{bmatrix} 1 & 2 & 3 \\ -3 & 2 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 5 & 6 \end{bmatrix}, \quad U = \begin{bmatrix} 1 & 2 & 3 \\ -3 & 2 & 0 \\ 2 & -3 & -3 \end{bmatrix}$$

U encodes the composite effect of the elementary column operations on A needed to bring A into normal form.

Algorithms for linear diophantine equations
5.1 THE EUCLIDEAN ALGORITHM

The Euclidean determines the g.c.d. of two positive rational numbers α and β.

1. Replace α by α-$\left\lfloor \alpha/\beta \right\rfloor \beta$ and β by β-$\left\lfloor \beta/\alpha \right\rfloor \alpha$.
2. Repeat until one of them is 0.
3. The nonzero among them is the g.c.d. of the original α and β.

Example : $\alpha = 18,\ \beta = 27;$ find $g.c.d\ \{18, 27\}$

$18 - 0 \times 27 = 18$

$27 - 1 \times 18 = 9$

$18 - 2 \times 9 = 0 \Rightarrow g.c.d\ \{18, 27\} = 9.$

Algorithms for linear diophantine equations
5.1 THE EUCLIDEAN ALGORITHM

FACTS : (i) $g.c.d\ \{\alpha,\ \beta\} = g.c.d\ \{\alpha - \left\lfloor \alpha/\beta \right\rfloor \beta,\ \beta\}$ and

(ii) $g.c.d\ \{\alpha,\ 0\} = \alpha$.

Proof of (i) : Define $\alpha - \left\lfloor \alpha/\beta \right\rfloor \beta = r$. Let d be any common divisor of α and β. So $d|\alpha$ and $d|\beta$. Then $r = \alpha - \left\lfloor \alpha/\beta \right\rfloor \beta$ is a multiple of d. Thus, any common divisor of α and β is also a common divisor of $r = \alpha - \left\lfloor \alpha/\beta \right\rfloor \beta$ and β.

Algorithms for linear diophantine equations
5.1 THE EUCLIDEAN ALGORITHM

Linear Diophantine Equation

- find integers γ and ε such that $\gamma\alpha+\varepsilon\beta=\eta$, with α, β both rational integers

Theorem : Suppose α,β,η are integers. Then $\gamma\alpha+\varepsilon\beta=\eta$ has an integer solution if and only if g.c.d$\{\alpha,\beta\}$ divides η.

Proof: ($\Rightarrow$) Since g.c.d$\{\alpha,\beta\}$ divides α, β, it must divide $\gamma\alpha+\varepsilon\beta$ for any integer γ,ε. Thus is divides η.

($\Leftarrow$) g.c.d$\{\alpha,\beta\}=\alpha x+\beta y$, x,y integers. If g.c.d$\{\alpha,\beta\}$ divides η, $\exists$ an η' such that $\eta'\times$g.c.d$\{\alpha,\beta\}=\eta'\times(\alpha x+\beta y)=\eta'(\alpha x)+\eta'(\beta y)$. This implies that $\gamma=\eta' x$ and $\varepsilon=\eta' y$ is a solution of $\gamma\alpha+\varepsilon\beta=\eta$.

Algorithms for linear diophantine equations
5.1 THE EUCLIDEAN ALGORITHM

Linear Diophantine Equation

- find integers γ and ε such that $\gamma\alpha+\varepsilon\beta$=g.c.d$\{\alpha,\beta\}$, with α, β both rational integers

Method :

▹ determine a series of 3 x 2 matrices where

$$A_0 \coloneqq \begin{bmatrix} \alpha & \beta \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad A_k \coloneqq \begin{bmatrix} \alpha_k & \beta_k \\ \gamma_k & \delta_k \\ \varepsilon_k & \zeta_k \end{bmatrix}$$

Algorithms for linear diophantine equations
5.1 THE EUCLIDEAN ALGORITHM

- ▹ RULE to find A_{k+1} from A_k :

  (i) if k is even and $\beta_k > 0$, substract $\left\lfloor \alpha_k / \beta_k \right\rfloor$ times the 2nd column of A_k from the 1st;

  (ii) if k is odd and $\alpha_k > 0$, substract $\left\lfloor \beta_k / \alpha_k \right\rfloor$ times the 1st column of A_k from the 2nd.

- ▹ Repeat for $k = 0, 1, 2, \ldots, N$, $\quad \alpha_N = 0$ or $\beta_N = 0$.

Algorithms for linear diophantine equations
5.1 THE EUCLIDEAN ALGORITHM

$Example: \quad \alpha=15,\ \beta=6$

$$A_0 = \begin{bmatrix} 15 & 6 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \text{k=0},\ \beta_0 = 6 > 0,\ \text{so } \left\lfloor \alpha_0 / \beta_0 \right\rfloor = \left\lfloor 15/6 \right\rfloor = 2$$

$$A_1 = \begin{bmatrix} 3 & 6 \\ 1 & 0 \\ -2 & 1 \end{bmatrix} \qquad \text{k=1},\ \alpha_1 = 3 > 0,\ \text{so } \left\lfloor \beta_1 / \alpha_1 \right\rfloor = \left\lfloor 6/3 \right\rfloor = 2$$

$$A_2 = \begin{bmatrix} 3 & 0 \\ 1 & -2 \\ -2 & 5 \end{bmatrix} \qquad \beta_2 = 0,\ \text{so} \qquad \begin{aligned} \text{g.c.d}\{\alpha,\beta\} &= \gamma_2\alpha+\varepsilon_2\beta \\ 3 &= (1)(15)+(-2)(6) \end{aligned}$$

Algorithms for linear diophantine equations
5.1 THE EUCLIDEAN ALGORITHM

- if $\beta_N = 0$ and $\alpha_N \neq 0$, then α_N is g.c.d of α and β since the g.c.d. of upper row of A_k does not change with the iterations and $\alpha_N =$ g.c.d $\{\alpha_N, 0\}$

- if $\alpha_N = 0$ and $\beta_N \neq 0$, then $\beta_N =$ g.c.d $\{\alpha, \beta\}$

- find integers γ and ε with $\gamma\alpha+\varepsilon\beta=$g.c.d$\{\alpha,\beta\}$

- $(1,-\alpha,-\beta)A_0 = (0,0)$ and $(1,-\alpha,-\beta)A_k = (0,0)$ (elem. col. operations)

Algorithms for linear diophantine equations
5.1 THE EUCLIDEAN ALGORITHM

- $$\gamma_{\mathrm{k}}\alpha + \varepsilon_k \beta = \alpha_k$$
  $$\delta_k \alpha + \zeta_k \beta = \beta_k$$

- if $\beta_{\mathrm{N}} = 0, \alpha_N \neq 0$
  $$\gamma_{\mathrm{N}}\alpha + \varepsilon_N \beta = \alpha_N = g.c.d\{\alpha, \beta\}$$
  $$\delta_N \alpha + \zeta_N \beta = 0$$

- Similarly, if $\alpha_N = 0, \beta_{\mathrm{N}} \neq 0$

Algorithms for linear diophantine equations
5.1 THE EUCLIDEAN ALGORITHM

SOME NOTES :

- $$-\alpha_k\delta_k + \beta_k\gamma_k = \beta$$
  $$\alpha_k\zeta_k - \beta_k\varepsilon_k = \alpha$$

- $$\gamma_k\zeta_k - \delta_k\varepsilon_k = 1$$

- for all k, $\gamma_k \geq 1, \zeta_k \geq 1$, and $\delta_k \leq 0, \varepsilon_k \leq 0$.

Algorithms for linear diophantine equations
5.1 THE EUCLIDEAN ALGORITHM

Theorem 5.1. The Euclidean algorithm is polynomial-time method, i.e., polynomial in the size of the input.

Proof : ◦ Assume that α and β are natural numbers.

- All matrices A_k have nonnegative integers in 1^{st} row.
- Each iterations reduces α_k or β_k by a factor of at least 2.
- Recall that the length of an integer n as input is the # of bits, i.e., $\log_2 n + O(1)$
- After at most $\lfloor \log_2\alpha \rfloor + \lfloor \log_2\beta \rfloor + 1$ iterations, either $\alpha_k = 0$ or $\beta_k = 0$.
- Each iteration consists of elementary arithmetic operations, thus taking polynomial time.
- $\therefore$ the sizes of the numbers are polynomially bounded by the sizes of α and β.

Algorithms for linear diophantine equations
5.1 THE EUCLIDEAN ALGORITHM

Corollary 5.1a. A linear diophantine equation with rational coefficients can be solved in polynomial time.

Proof : Let $\alpha_1\zeta_1+\cdots+\alpha_n\zeta_n=\beta$ be a rational linear diophantine equation.

Algorithm : Case n=1: trivial. Let $n \geq 2$. Find $\alpha', \gamma, \varepsilon$ with Euclidean alg. satisfying: $\alpha' = \text{g.c.d.}\{\alpha_1, \alpha_2\} = \alpha_1\gamma + \alpha_2\varepsilon$, γ, ε : integers.

Solve the linear diophantine equation in (n-1) variables:

$$(*) \qquad \alpha'\zeta' + \alpha_3\zeta_3 + \cdots + \alpha_n\zeta_n = \beta.$$

If (*) has no integral solution, then neither does the original equation.

If (*) has an integral solution $\zeta', \zeta_3, \ldots, \zeta_n$ then $\zeta_1 = \gamma\zeta', \zeta_2 = \varepsilon\zeta', \zeta_3, \ldots, \zeta_n$ gives an integral solution to the original equation.

This defines a polynomial algorithm.

Theorem 5.2. The Hermite normal form [B 0] of a rational matrix of full row rank has size polynomially bounded by the size of A. Moreover, there exists a unimodular matrix U with AU=[B 0] such that the size of U is polynomially bounded by the size of A.

Proof : - Assume A is integral (multiplying A by porduct of the denominators of A, say κ, also multiplies the HNF of A by κ).

- Diagonal entries of B are divisors of subdeterminants of A (Sec. 4.2).
- Each row of B has its max. entry on the diagonal of B

  $\Rightarrow$ size of [B 0] is polynomially bounded by size of A.

Algorithms for linear diophantine equations
5.2 SIZES & GOOD CHARACTERIZATIONS

Proof : - Assume A=[A' A''] with A' nonsingular.

- Let HNF of

$$\begin{bmatrix} A' & A'' \\ 0 & I \end{bmatrix} \text{ is } \begin{bmatrix} B & 0 \\ B' & B'' \end{bmatrix}$$

for certain matrices B' and B''.

- Since the sizes of B, B', and B'' are polynomially bounded by the size of A, the size of unimodular matrix

$$U := \begin{bmatrix} A' & A'' \\ 0 & I \end{bmatrix}^{-1} \begin{bmatrix} B & 0 \\ B' & B'' \end{bmatrix}$$

is polynomially bounded by the size of A

- $AU = [A' \; A'']U = [B \; 0]$

Algorithms for linear diophantine equations
5.2 SIZES & GOOD CHARACTERIZATIONS

Corollary 5.2a. If a rational system Ax=b has an integral solution, it has one of size polynomially bounded by the sizes of A and b.

Corollary 5.2b. The following problem has a good characterization:

> *given a rational matrix A and a rational vector b, does the system $Ax = b$ have an integral solution?*

Polynomial algorithm to determine the HNF

Let A be an $m \times n$ integral matrix of full row rank.

Let M be the absolute value of the determinant of an (arbitrary) submatrix A of rank m.

The columns of A generate the same lattice as the columns of the martix:

$$A' := \left[\begin{array}{c|cccc} & M & & & \\ & & \ddots & 0 & \\ A & & & & \\ & & 0 & \ddots & \\ & & & & M \end{array} \right]$$

5.3 POLYNOMIAL ALGORITHMS FOR HNF & SYSTEMS LINEAR DIOPHANTINE EQUATIONS

◦ HNF of A is the same as that of A', except for the last m columns of the HNF of A'.

◦ Thus, it suffices to find the HNF of A'.

Method : (1) Add integral multiples of the last m columns of A' to the first n columns of A' so that all components with be at least 0 or at most M.

Algorithms for linear diophantine equations
5.3 POLYNOMIAL ALGORITHMS FOR HNF & SYSTEMS LINEAR DIOPHANTINE EQUATIONS

(2) Suppose we have the matrix

$$(*) \qquad \left[\begin{array}{c|c|ccccc} B & 0 & & & 0 & & \\ \hline & & 0 & & & & 0 \\ & & M & & 0 & & \\ & & & & & \ddots & \\ C & D & 0 & & & & \\ & & & & & & M \end{array}\right]$$

where B is lower triangular $k \times k$ matrix, C is an $(m-k)\times k$ matrix, D is an $(m-k)\times(n+1)$ matrix such that the first row of D is nonzero.

Algorithms for linear diophantine equations
5.3 POLYNOMIAL ALGORITHMS FOR HNF & SYSTEMS LINEAR DIOPHANTINE EQUATIONS

(3) Writing $D =: \left(\delta_{ij}\right)_{i=1,j=1}^{m-k\ n+1}$:

if there are $i \neq j$ with $\delta_{1i} \geq \delta_{1j} > 0$, then:

(i) subtract $\left\lfloor \delta_{1i} / \delta_{1j} \right\rfloor$ times the j^{th} column of D from the i^{th} column of D;

(ii) add integral multiples of the last $(m-k-1)$ columns of $(*)$ to the other columns to bring all components between 0 and M.

(4) Repeat (i) and (ii) while the first row of D has more than one nonzero entry.

When D obtains exactly one nonzero entry, repeat for $(k+1)$.

5.3 POLYNOMIAL ALGORITHMS FOR HNF & SYSTEMS LINEAR DIOPHANTINE EQUATIONS

(4) If $k = m$, then the matrix $(*)$ is in the form [B 0] with B lower triangular.

(5) HNF: for $i = 2,\ldots n$, do for $j = 1,\ldots, i - 1$, add an integral multiple of the i^{th} column of B to the j^{th} column of B to get the $(i, j)^{th}$ entry of B nonnegative and less than β_{ij}.

(6) Then the HNF is obtained by deleting the last m columns.

Algorithms for linear diophantine equations
5.3 POLYNOMIAL ALGORITHMS FOR HNF & SYSTEMS LINEAR DIOPHANTINE EQUATIONS

Theorem 5.3. The described mathod finds the HNF in polynomial time.

Proof : • Executions on the matrix D is polynomially bounded by n and $\log_2 M$

• *Procedure on first row of D :* ∘ one more zero entry in the row or

∘ reduce the row by a factor of at least 2 $\left(\delta_{1i} - \left\lfloor \delta_{1i} / \delta_{1j} \right\rfloor \delta_{1j} \leq \frac{1}{2}\delta_{1i}\right)$

$\Rightarrow$ after at most $n \log_2 M$ iterations, D has at most one nonzero entry in the first row and $k \to k+1$

• Then $k = m$ (B is upper triangular form) after at most $mn \log_2 M$ iterations, we begin to transform [B 0] into HNF $\Rightarrow$ polynomial-time

• Thus, the algorithm is polynomially bounded

Algorithms for linear diophantine equations
5.3 POLYNOMIAL ALGORITHMS FOR HNF & SYSTEMS LINEAR DIOPHANTINE EQUATIONS

Corollary 5.3a. Given a rational matrix A of full row rank, we can find in polynomial time a unimodular matrix U such that AU is in HNF.

Corollary 5.3b. Given a system of rational linear equations, we can decide if it has an integral solution, and if so, find one, in polynomial time.

Corollary 5.3c. Given a feasible system Ax=b of rational linear diophantine equations, we can find in polynomial time integral vectors $x_0, x_1, \ldots, x_t$ such that

$$\{x \mid Ax = b;\ x \text{ is integral}\} = \{x_0 + \lambda_1 x_1 + \cdots + \lambda_t x_t \mid \lambda_1, \ldots, \lambda_t \in \mathbb{Z}\}$$

with $x_0, x_1, \ldots, x_t$ linearly independent.