Tools for fast computation of integer matrix normal forms

George Labahn

Cheriton School of Computer Science
University of Waterloo

ACA 2025, July 14-19

Session on Symbolic Linear Algebra and its Applications

Introduction

1. Goal (of research): Find Hermite form of a matrix $M \in \mathbb{Z}^{m \times n}$

   - M square, nonsingular, $||M|| = \max_{ij} |M_{ij}|$

     Currently: $O(n^3(\log n + \log ||M||)^2(\log n)^2)$ bit ops

     Variant cost $(n^3 \log ||M||)^{1+o(1)}$ bit ops (fast integer arith)

Introduction

1. Goal (of research): Find Hermite form of a matrix $M \in \mathbb{Z}^{m\times n}$
   - M square, nonsingular, $||M|| = \max_{ij} |M_{ij}|$

     Currently: $O(n^3(\log n + \log ||M||)^2(\log n)^2)$ bit ops

     Variant cost $(n^3 \log ||M||)^{1+o(1)}$ bit ops (fast integer arith)
   - Better: "cost of matrix multiplication"
   - Also results for M full column rank case

Introduction

1. Goal (of research): Find Hermite form of a matrix $M \in \mathbb{Z}^{m \times n}$
   - M square, nonsingular, $||M|| = \max_{ij} |M_{ij}|$

     Currently: $O(n^3(\log n + \log ||M||)^2(\log n)^2)$ bit ops

     Variant cost $(n^3 \log ||M||)^{1+o(1)}$ bit ops (fast integer arith)
   - Better: "cost of matrix multiplication"
   - Also results for M full column rank case
2. Goal (of talk): Give introduction to tools needed in Arne's talk

Introduction

Tools: (this talk)

1. Denominators of M^{-1}
2. Approximate $M^{-1} \approx FS^{-1}$
3. Generalize: NM^{-1}
4. Computation ideas
5. Relate to normal form over $\mathbb{Z}_N^{m \times n}$

Introduction

Tools: (this talk)

1. Denominators of M^{-1} : Minimal denominators
2. Approximate $M^{-1} \approx FS^{-1}$: Make use of Smith form of M
3. Generalize: NM^{-1} : Hermite bases of integer relation lattices
4. Computation ideas : Relate to rational approximation
5. Relate to normal form over $\mathbb{Z}_N^{m\times n}$

Topic 1. Minimal Matrix Denominators

- Denominator h for $b \in Q$: $hb \in Z$

  Denominator for $B \in \mathbb{Q}^{n \times m}$: H with $HB \in \mathbb{Z}^{n \times m}$

  Minimal Matrix Denominator : H with minimal $|det(H)|$.

Topic 1. Minimal Matrix Denominators

- Denominator h for $b \in Q$: $hb \in Z$

  Denominator for $B \in \mathbb{Q}^{n\times m}$: H with $HB \in \mathbb{Z}^{n\times m}$

  Minimal Matrix Denominator : H with minimal $|det(H)|$.

- Example : $UM = H,\ U$ unimodular $\quad\rightarrow\quad HM^{-1} = U \in \mathbb{Z}^{n\times n}$

Topic 1. Minimal Matrix Denominators

- Denominator h for $b \in Q$: $hb \in Z$

  Denominator for $B \in \mathbb{Q}^{n\times m}$: H with $HB \in \mathbb{Z}^{n\times m}$

  Minimal Matrix Denominator : H with minimal $|det(H)|$.

- Example : $UM = H,\ U$ unimodular $\quad \rightarrow \quad HM^{-1} = U \in \mathbb{Z}^{n\times n}$

$$\begin{array}{c} M \\ \begin{bmatrix} -8 & 3 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 4 & -2 & -1 & -1 \\ 4 & -1 & 0 & 0 \end{bmatrix} \end{array}$$

Topic 1. Minimal Matrix Denominators

- Denominator h for $b \in Q$: $hb \in Z$

  Denominator for $B \in \mathbb{Q}^{n\times m}$: H with $HB \in \mathbb{Z}^{n\times m}$

  Minimal Matrix Denominator : H with minimal $|det(H)|$.

- Example : $UM = H,\ U$ unimodular $\quad \rightarrow \quad HM^{-1} = U \in \mathbb{Z}^{n\times n}$

$$\overset{M}{\begin{bmatrix} -8 & 3 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 4 & -2 & -1 & -1 \\ 4 & -1 & 0 & 0 \end{bmatrix}} \quad \Longrightarrow \quad \overset{H}{\begin{bmatrix} 4 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}} \overset{M^{-1}}{\begin{bmatrix} 1/8 & 1/16 & -1/16 & 9/16 \\ 1/2 & 1/4 & -1/4 & 5/4 \\ -1/2 & 1/4 & -1/4 & -3/4 \\ 0 & -1/2 & -1/2 & 1/2 \end{bmatrix}} \quad \in \mathbb{Z}^{4\times 4}.$$

Topic 1. Minimal Matrix Denominators

- Denominator h for $b \in Q$: $hb \in Z$

  Denominator for $B \in \mathbb{Q}^{n\times m}$: H with $HB \in \mathbb{Z}^{n\times m}$

  Minimal Matrix Denominator : H with minimal $|det(H)|$.

- Example : $UM = H,\ U$ unimodular $\quad \rightarrow \quad HM^{-1} = U \in \mathbb{Z}^{n\times n}$

$$\overset{M}{\begin{bmatrix} -8 & 3 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 4 & -2 & -1 & -1 \\ 4 & -1 & 0 & 0 \end{bmatrix}} \Longrightarrow \overset{H}{\begin{bmatrix} 4 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}} \overset{M^{-1}}{\begin{bmatrix} 1/8 & 1/16 & -1/16 & 9/16 \\ 1/2 & 1/4 & -1/4 & 5/4 \\ -1/2 & 1/4 & -1/4 & -3/4 \\ 0 & -1/2 & -1/2 & 1/2 \end{bmatrix}} \in \mathbb{Z}^{4\times 4}.$$

  - H: Minimal determinant in Hermite form
  - All minimal sized multipliers are left equivalent
  - det H divides det of all matrix denominators of M^{-1}.

Hermite Minimal Denominators

Example :

$$UM = H \quad \rightarrow \quad HM^{-1} = U \in \mathbb{Z}^{n\times n}$$

$$\overset{M}{\begin{bmatrix} -8 & 3 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 4 & -2 & -1 & -1 \\ 4 & -1 & 0 & 0 \end{bmatrix}} \Longrightarrow \overset{H}{\begin{bmatrix} 4 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}} \overset{M^{-1}}{\begin{bmatrix} 1/8 & 1/16 & -1/16 & 9/16 \\ 1/2 & 1/4 & -1/4 & 5/4 \\ -1/2 & 1/4 & -1/4 & -3/4 \\ 0 & -1/2 & -1/2 & 1/2 \end{bmatrix}} \quad \in \mathbb{Z}^{4\times 4}.$$

- But we do not actually want to compute M^{-1}

  - since in worst case requires $\Omega(n^3(\log n + \log ||M|))$ space

Hermite Minimal Denominators

Example :

$$UM = H \quad \rightarrow \quad HM^{-1} = U \in \mathbb{Z}^{n\times n}$$

$$\overset{M}{\begin{bmatrix} -8 & 3 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 4 & -2 & -1 & -1 \\ 4 & -1 & 0 & 0 \end{bmatrix}} \Longrightarrow \overset{H}{\begin{bmatrix} 4 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}} \overset{M^{-1}}{\begin{bmatrix} 1/8 & 1/16 & -1/16 & 9/16 \\ 1/2 & 1/4 & -1/4 & 5/4 \\ -1/2 & 1/4 & -1/4 & -3/4 \\ 0 & -1/2 & -1/2 & 1/2 \end{bmatrix}} \quad \in \mathbb{Z}^{4\times 4}.$$

- But we do not actually want to compute M^{-1}

  - since in worst case requires $\Omega(n^3(\log n + \log ||M|))$ space

- However minimal denominator approach brings Smith form into play

Topic 2. Smith Massagers of M

Smith Multipliers. (S diagonal, $\hat{U}MV = S$, $\hat{U}, V$ unimodular).

1. Equivalently $MV = WS$ with V, W unimodular

Topic 2. Smith Massagers of M

Smith Multipliers. (S diagonal, $\hat{U}MV = S$, $\hat{U}, V$ unimodular).

1. Equivalently $MV = WS$ with V, W unimodular
2. Set $F = V \text{ cmod } S$ (i.e. modulo columns).

Topic 2. Smith Massagers of M

Smith Multipliers. (S diagonal, $\hat{U}MV = S$, $\hat{U}, V$ unimodular).

1. Equivalently $MV = WS$ with V, W unimodular
2. Set $F = V$ cmod S (i.e. modulo columns). Then
   - $MF = \hat{W}S$
   - $\hat{F}F = I$ cmod S for some $\hat{F}$.

F (or F, S) is a Smith Massager for M

Why is Smith Massager useful?

Given $MF = \hat{W}S$ and $\hat{F}F = I \text{ cmod } S$ for some $\hat{F}$.

Then:

$$FS^{-1} = M^{-1}\hat{W}$$

Why is Smith Massager useful?

Given $MF = \hat{W}S$ and $\hat{F}F = I \text{ cmod } S$ for some $\hat{F}$.

Then:

$$FS^{-1} = M^{-1}\hat{W}$$

1. M^{-1} and FS^{-1} have same Hermite minimal denominators
2. Also:

- F and S have predictable size in terms of bitlength.
- F and S have no common right factor (since $\hat{F}F + QS = I$).

  Hence FS^{-1} is reduced.

Example

Smith Form with Multipliers : $MV = WS$ with V, W unimodular.

$$\begin{array}{c} M \\ \begin{bmatrix} -8 & 3 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 4 & -2 & -1 & -1 \\ 4 & -1 & 0 & 0 \end{bmatrix} \end{array}$$

Example

Smith Form with Multipliers : $MV = WS$ with V, W unimodular.

$$\underset{M}{\begin{bmatrix} -8 & 3 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 4 & -2 & -1 & -1 \\ 4 & -1 & 0 & 0 \end{bmatrix}} \underset{V}{\begin{bmatrix} 0 & 0 & -1 & 9 \\ 0 & 1 & -4 & 36 \\ 1 & 3 & -4 & 36 \\ 0 & 0 & -1 & 8 \end{bmatrix}} = \underset{W}{\begin{bmatrix} -1 & 0 & 0 & 0 \\ 1 & 4 & -7 & 4 \\ -1 & -5 & 9 & -5 \\ 0 & -1 & 0 & 0 \end{bmatrix}} \underset{S}{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 16 \end{bmatrix}}$$

◇ Las Vegas algorithms : (BLS - ISSAC'20, JSC 2023)

◇ Cost : $O(n^3(\log n + \log \|M\|)^2(\log n)^2)$ bit operations

Example

Smith Massager : $MF \equiv 0 \text{ cmod } S$ and $\hat{F}F \equiv I \text{ cmod } S$

$$\overset{M}{\begin{bmatrix} -8 & 3 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 4 & -2 & -1 & -1 \\ 4 & -1 & 0 & 0 \end{bmatrix}} \overset{F}{\begin{bmatrix} 0 & 0 & 0 & 9 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 8 \end{bmatrix}} = \overset{\hat{W}}{\begin{bmatrix} 0 & 0 & 0 & -4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}} \overset{S}{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 16 \end{bmatrix}}$$

◇ Las Vegas algorithms : (BLS - ISSAC'20, JSC 2023)

◇ Cost : $O(n^3(\log n + \log \|M\|)^2(\log n)^2)$ bit operations

Example

Smith Massager : Basically $F = V \text{ cmod } S$

$$\begin{array}{cccc} M & F & & \hat{W} \quad\quad S \end{array}$$

$$\underbrace{\begin{bmatrix} -8 & 3 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 4 & -2 & -1 & -1 \\ 4 & -1 & 0 & 0 \end{bmatrix}}_{M} \underbrace{\begin{bmatrix} 0 & 0 & 0 & 9 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 8 \end{bmatrix}}_{F} = \underbrace{\begin{bmatrix} 0 & 0 & 0 & -4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}}_{\hat{W}} \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 16 \end{bmatrix}}_{S}$$

Example

For one column use hcol algorithm of Pauderis-Storjohann

$$\overset{F_4}{\begin{bmatrix} 9 \\ 4 \\ 4 \\ 8 \end{bmatrix}} /16 \quad \Longrightarrow \quad \overset{H}{\begin{bmatrix} 4 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}}$$

Theorem (Pauderis and Storhojann).

Algorithm hcol$(\vec{w}, d)$, $\vec{w} \in \mathbb{Z}/(d)^{n\times 1}$ returns the Hermite denominator H of $\vec{w}d^{-1}$. Cost is $O(n(\log d)^2)$ bit operations.

Example

For one column use hcol algorithm of Pauderis-Storjohann

$$\overset{F_4}{\begin{bmatrix} 9 \\ 4 \\ 4 \\ 8 \end{bmatrix}} /16 \quad \Longrightarrow \quad \overset{H}{\begin{bmatrix} 4 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}}$$

Check:

$$\begin{bmatrix} -0 & 0 & -1 & 2 \\ 0 & 0 & -1 & 1 \\ -1 & 0 & -1 & -1 \\ 0 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} -8 & 3 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 4 & -2 & -1 & -1 \\ 4 & -1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}$$

Topic 3. Lattice of Integer Relations

Goal now:

Finding Hermite minimal denominator for FS^{-1}.

Equivalently $HF = 0 \mod S$.

Topic 3. Lattice of Integer Relations

Goal now:

Finding Hermite minimal denominator for FS^{-1}.

Equivalently $HF = 0 \mod S$.

1. Generalize to Hermite minimal denominator for NM^{-1}.

   Equivalently $HN = 0 \mod M$.

Topic 3. Lattice of Integer Relations

Goal now:

Finding Hermite minimal denominator for FS^{-1}.

Equivalently $HF = 0 \mod S$.

1. Generalize to Hermite minimal denominator for NM^{-1}.

   Equivalently $HN = 0 \mod M$.

2. Also want M rectangular with full column rank

Topic 3. Lattice of Integer Relations

Goal now:

Finding Hermite minimal denominator for FS^{-1}.

Equivalently $HF = 0 \mod S$.

1. Generalize to Hermite minimal denominator for NM^{-1}.

   Equivalently $HN = 0 \mod M$.

2. Also want M rectangular with full column rank

3. Same as finding Hermite basis for lattice

$$\mathcal{R}(M, N) := \left\{ p \in \mathbb{Z}^{1 \times n} \mid pN = \mathbf{0} \bmod M \right\}$$

   This defines integer relations lattice for N with modulus M.

Observe

Given $M \in \mathbb{Z}^{\ell \times m}$, full column rank, $N \in \mathbb{Z}^{n \times m}$, let

$$\mathcal{R}(M,N) := \left\{ p \in \mathbb{Z}^{1 \times n} \mid pN = \mathbf{0} \bmod M \right\}$$

1. If M square, nonsingular, then $\mathcal{R}(M,N)$ is free of rank n.
2. Basis represented as rows of nonsingular $P \in \mathbb{Z}^{n \times n}$ satisfying

   $$PN = \mathbf{0} \bmod M.$$

   Also works for M full column rank
3. Used by Neiger and Vu, ISSAC'17 for polynomial matrices

Examples

Given $M \in \mathbb{Z}^{\ell \times m}$, full column rank, $F \in \mathbb{Z}^{n \times m}$, let

$$\mathcal{R}(M, F) := \left\{ p \in \mathbb{Z}^{1 \times n} \mid pF = \mathbf{0} \bmod M \right\}$$

1. M is square then $\mathcal{R}(M, I)$ defines row space of M
2. Generalized Chinese remaindering: solving

   $$\vec{x}A = \vec{b} \mod \vec{m}$$

   same as $\mathcal{R}(M, F)$, M diagonal and $F = \begin{bmatrix} -\vec{b} \\ A \end{bmatrix}$

Examples

Given $M \in \mathbb{Z}^{\ell \times m}$, full column rank, $F \in \mathbb{Z}^{n \times m}$, let

$$\mathcal{R}(M, F) := \left\{ p \in \mathbb{Z}^{1 \times n} \mid pF = \mathbf{0} \bmod M \right\}$$

1. M is square then $\mathcal{R}(M, I)$ defines row space of M
2. Generalized Chinese remaindering: solving

   $$\vec{x}A = \vec{b} \mod \vec{m}$$

   same as $\mathcal{R}(M, F)$, M diagonal and $F = \begin{bmatrix} -\vec{b} \\ A \end{bmatrix}$
3. Also product, remainder modulo Hermite form, etc

Example: Hermite form of products

1. Given A and B, nonsingular. Hermite form of A B?

   Example: $A, B \in \mathbb{Z}^{(2n+1)\times(2n+1)}$, $\vec{e} = (1, \ldots, 1)$.

$$A = \begin{bmatrix} I_n & 2^n \vec{e}^{\,t} & \\ & 2^n + 1 & \\ & & I_n \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} I_n & & \\ & 1 & \vec{e} \\ & & 2I_n \end{bmatrix}$$

Example: Hermite form of products

1. Given A and B, nonsingular. Hermite form of A B?

   Example: $A, B \in \mathbb{Z}^{(2n+1)\times(2n+1)}$, $\vec{e} = (1, \ldots, 1)$.

$$A = \begin{bmatrix} I_n & 2^n\vec{e}^{\,t} & \\ & 2^n+1 & \\ & & I_n \end{bmatrix} \text{ and } B = \begin{bmatrix} I_n & & \\ & 1 & \vec{e} \\ & & 2I_n \end{bmatrix}$$

   Problem: AB is large (it has an $n \times n$ submatrix $2^n\vec{e}^{\,t}\vec{e}$)

Example: Hermite form of products

1. Given A and B, nonsingular. Hermite form of A B?

   Example: $A, B \in \mathbb{Z}^{(2n+1)\times(2n+1)}$, $\vec{e} = (1, \ldots, 1)$.

   $$A = \left[\begin{array}{ccc} I_n & 2^n\vec{e}^{\,t} & \\ & 2^n+1 & \\ & & I_n \end{array}\right] \text{ and } B = \left[\begin{array}{ccc} I_n & & \\ & 1 & \vec{e} \\ & & 2I_n \end{array}\right]$$

   Problem: AB is large (it has an $n \times n$ submatrix $2^n\vec{e}^{\,t}\vec{e}$)

2. Instead we can compute Hermite basis for

   $$\mathcal{R}(AB, I) = \mathcal{R}\left(\left[\begin{array}{cc} A & \\ I & B \end{array}\right], \left[\begin{array}{cc} \mathbf{0} & I \end{array}\right]\right).$$

Reductions of $\mathcal{R}(M, N)$ to $\mathcal{R}(S, F)$

We reduce $\mathcal{R}(M, N)$ to $\mathcal{R}(S, F)$ through a sequence of equivalences:

$$(M, N) \xrightarrow{1} \left(\left[\frac{M_1}{M_2} \right], N \right) \xrightarrow{2} \left(\left[\frac{S_1}{M_3} \right], N_1 \right) \xrightarrow{3} (T_1, N_1) \xrightarrow{4} (S_2, N_2) \xrightarrow{5} (K, C) \xrightarrow{6} (S, F).$$

Reductions of $\mathcal{R}(M,N)$ to $\mathcal{R}(S,F)$

We reduce $\mathcal{R}(M,N)$ to $\mathcal{R}(S,F)$ through a sequence of equivalences:

$$(M,N) \xrightarrow{1} \left(\left[\frac{M_1}{M_2} \right], N \right) \xrightarrow{2} \left(\left[\frac{S_1}{M_3} \right], N_1 \right) \xrightarrow{3} (T_1, N_1) \xrightarrow{4} (S_2, N_2) \xrightarrow{5} (K, C) \xrightarrow{6} (S, F).$$

Theorem

Let S be a nonsingular Smith form, and let T be the Hermite basis of

$$\begin{bmatrix} S \\ F \end{bmatrix}.$$

Then the Hermite basis of $\mathcal{R}\left(S, \left[\frac{F}{T}\right]\right)$ has the shape

$$\left[\begin{array}{c|c} I & C \\ \hline & K \end{array}\right],$$

and $\mathcal{R}(S,F)$ is equal to $\mathcal{R}(K,C)$, with the latter having a reduced input.

Topic 5. Matrix normal forms over $\mathbb{Z}_N$

Recall: Smith massager S, F for M:

1. M^{-1} and FS^{-1} have same Hermite minimal denominators

Topic 5. Matrix normal forms over $\mathbb{Z}_N$

Recall: Smith massager S, F for M:

1. M^{-1} and FS^{-1} have same Hermite minimal denominators
2. Let $s = s_n$ and $M^* = sM^{-1}$, $S^* = sS^{-1}$

   Then H with $HM^* \equiv 0 \mod s \iff HFS^* \equiv 0 \mod s$

Normal forms matrices over $\mathbb{Z}_N$

Example:

$$H = \begin{bmatrix} 3 & 2 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 3 \end{bmatrix} \in \mathbb{Z}_{12}^{3\times 3}$$

Normal forms matrices over $\mathbb{Z}_N$

Recall: Row echelon form over a field or integral domain:

$$\begin{bmatrix} * & * & * & * & * & * \\ & * & * & * & * & * \\ & & * & * & * & * \\ & & * & * & * & * \\ & & * & * & * & * \\ & & * & * & * & * \end{bmatrix}$$

Normal forms matrices over $\mathbb{Z}_N$

Recall: Row echelon form over a field or integral domain:

$$\begin{bmatrix} * & * & * & * & * & * \\ & * & * & * & * & * \\ & & * & * & * & * \\ & & * & * & * & * \\ & & * & * & * & * \\ & & * & * & * & * \end{bmatrix}$$

Notice:

Vectors in row space of form $[0, *, \ldots, *]$ spanned by rows 2 to n

Normal forms matrices over $\mathbb{Z}_N$

Recall: Row echelon form over a field or integral domain:

$$\begin{bmatrix} * & * & * & * & * & * \\ & * & * & * & * & * \\ & & * & * & * & * \\ & & * & * & * & * \\ & & * & * & * & * \\ & & * & * & * & * \end{bmatrix}$$

Notice:

Vectors in row space of form $[0, *, \ldots, *]$ spanned by rows 2 to n

Vectors in row space of form $[0, 0, *, \ldots, *]$ spanned by rows $3 - n$,

etc

Howell Form

Not the case for example for matrices of $\mathbb{Z}_{12}$. e.g.:

$$H = \begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix} \in \mathbb{Z}_{12}^{2\times 2}$$

looks like it is in row echelon form.

Howell Form

Not the case for example for matrices of $\mathbb{Z}_{12}$. e.g.:

$$H = \begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix} \in \mathbb{Z}_{12}^{2\times 2}$$

looks like it is in row echelon form. But

$$[0, 2] = 6R_1 + 2R_2$$

is in span of H but is not generated by row 2.

Howell Form

The Howell normal form of $A \in \mathbb{Z}_N^{n \times m}$ is a square matrix $H \in \mathbb{Z}_N^{m \times m}$:

Howell Form

The Howell normal form of $A \in \mathbb{Z}_N^{n \times m}$ is a square matrix $H \in \mathbb{Z}_N^{m \times m}$:

1. span of the rows of A is equal to span of the rows of H,
2. H is in echelon form, leading non-zero entry in each row divides N,
3. if h_{ij} is the first non-zero element in row i, then
   - $0 \le h_{kj} < h_{ij}$ for $k < i$,
   - if $X \in \mathrm{span}(A)$ has first $j-1$ elements zero, then $X \in \mathrm{span}_j(H)$.

Howell Form

Example 1: $A = \begin{bmatrix} 8 & 2 \\ 6 & 1 \end{bmatrix} \in \mathbb{Z}_{12}^{2\times 2}$.

$$H = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \in \mathbb{Z}_{12}^{2\times 2}$$

Example 2: $A = \begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \in \mathbb{Z}_{12}^{2\times 3}$.

$$H = \begin{bmatrix} 3 & 2 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 3 \end{bmatrix} \in \mathbb{Z}_{12}^{3\times 3}$$

Howell Form

Example 1: $A = \begin{bmatrix} 8 & 2 \\ 6 & 1 \end{bmatrix} \in \mathbb{Z}_{12}^{2\times 2}$.

$$H = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \in \mathbb{Z}_{12}^{2\times 2}$$

Example 2: $A = \begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \in \mathbb{Z}_{12}^{2\times 3}$.

$$H = \begin{bmatrix} 3 & 2 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 3 \end{bmatrix} \in \mathbb{Z}_{12}^{3\times 3}$$

Why are these correct? Howell's construction