Fast Computation of the Hermite Normal Form of Integer Matrices

George Labahn

Cheriton School of Computer Science
University of Waterloo

May 16, 2024

Journées Approximation,

Cité Scientifique, Université de Lille

Joint work with Stavros Birmpilis and Arne Storjohann

Outline

In this talk

We wish to:

- Triangularize integer matrices (efficiently)

In this talk

We wish to:

- Triangularize integer matrices (efficiently)
- Diagonalize integer matrices
- Do both using only integer operations (row or column)
- Normalize results so answers are unique

Issue: intermediate integers get large during computation

In this talk

We wish to:

- Triangularize integer matrices (efficiently)
- Diagonalize integer matrices
- Do both using only integer operations (row or column)
- Normalize results so answers are unique

Issue: intermediate integers get large during computation

We will also need to discuss:

- Triangularize integer mod N matrices

Triangularize and Diagonalize

- Triangularize: Hermite normal form
- Diagonalize: Smith normal Form
- Triangularize (over $\mathbb{Z}_N$): Howell normal form
- Integer operations: Unimodular matrices
  - U with det $U = \pm 1$
- Forms date back to 1851 (Hermite) and 1861 (Smith).

Hermite Normal Form

Example

$$\begin{bmatrix} -8 & -1 & 5 & 1 & 6 & 0 \\ 2 & -3 & -8 & -3 & 2 & -1 \\ -5 & -4 & -5 & 9 & -4 & 4 \\ 2 & -6 & -1 & -8 & 9 & -7 \\ -9 & 5 & -5 & -6 & 2 & -7 \\ 0 & -6 & -4 & 6 & 0 & -8 \end{bmatrix}$$

Hermite Normal Form

Example

$$\begin{bmatrix} -8 & -1 & 5 & 1 & 6 & 0 \\ 2 & -3 & -8 & -3 & 2 & -1 \\ -5 & -4 & -5 & 9 & -4 & 4 \\ 2 & -6 & -1 & -8 & 9 & -7 \\ -9 & 5 & -5 & -6 & 2 & -7 \\ 0 & -6 & -4 & 6 & 0 & -8 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 7657 \\ 0 & 1 & 0 & 1 & 4 & 6283 \\ 0 & 0 & 1 & 0 & 1 & 22951 \\ 0 & 0 & 0 & 2 & 3 & 14998 \\ 0 & 0 & 0 & 0 & 5 & 40428 \\ 0 & 0 & 0 & 0 & 0 & 41350 \end{bmatrix}$$

Hermite Normal Form

Example

$$\underset{U}{\begin{bmatrix} 235 & 454 & 256 & -84 & -269 & -577 \\ 194 & 374 & 209 & -70 & -221 & -473 \\ 704 & 1360 & 768 & -251 & -806 & -1730 \\ 461 & 890 & 501 & -165 & -527 & -1130 \\ 1241 & 2397 & 1352 & -443 & -1420 & -3047 \\ 1268 & 2450 & 1384 & -452 & -1452 & -3117 \end{bmatrix}} \underset{A}{\begin{bmatrix} -8 & -1 & 5 & 1 & 6 & 0 \\ 2 & -3 & -8 & -3 & 2 & -1 \\ -5 & -4 & -5 & 9 & -4 & 4 \\ 2 & -6 & -1 & -8 & 9 & -7 \\ -9 & 5 & -5 & -6 & 2 & -7 \\ 0 & -6 & -4 & 6 & 0 & -8 \end{bmatrix}} = \underset{H}{\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 7657 \\ 0 & 1 & 0 & 1 & 4 & 6283 \\ 0 & 0 & 1 & 0 & 1 & 22951 \\ 0 & 0 & 0 & 2 & 3 & 14998 \\ 0 & 0 & 0 & 0 & 5 & 40428 \\ 0 & 0 & 0 & 0 & 0 & 41350 \end{bmatrix}}$$

Can check that $UA = H$ and that $\det U = -1$.

Hermite Normal Form

Example

$$\underset{U}{\begin{bmatrix} 235 & 454 & 256 & -84 & -269 & -577 \\ 194 & 374 & 209 & -70 & -221 & -473 \\ 704 & 1360 & 768 & -251 & -806 & -1730 \\ 461 & 890 & 501 & -165 & -527 & -1130 \\ 1241 & 2397 & 1352 & -443 & -1420 & -3047 \\ 1268 & 2450 & 1384 & -452 & -1452 & -3117 \end{bmatrix}} \underset{A}{\begin{bmatrix} -8 & -1 & 5 & 1 & 6 & 0 \\ 2 & -3 & -8 & -3 & 2 & -1 \\ -5 & -4 & -5 & 9 & -4 & 4 \\ 2 & -6 & -1 & -8 & 9 & -7 \\ -9 & 5 & -5 & -6 & 2 & -7 \\ 0 & -6 & -4 & 6 & 0 & -8 \end{bmatrix}} = \underset{H}{\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 7657 \\ 0 & 1 & 0 & 1 & 4 & 6283 \\ 0 & 0 & 1 & 0 & 1 & 22951 \\ 0 & 0 & 0 & 2 & 3 & 14998 \\ 0 & 0 & 0 & 0 & 5 & 40428 \\ 0 & 0 & 0 & 0 & 0 & 41350 \end{bmatrix}}$$

Can check that $UA = H$ and that $\det U = -1$.

Example (simpler) :

$$\underset{U}{\begin{bmatrix} -25 & -160 & 109 & 128 \\ -46 & -295 & 201 & 236 \\ -25 & -156 & 107 & 125 \\ -65 & -419 & 285 & 335 \end{bmatrix}} \underset{A}{\begin{bmatrix} -13 & 27 & 0 & -21 \\ 10 & 30 & 15 & 0 \\ -20 & 15 & 15 & -15 \\ 27 & 30 & 6 & 9 \end{bmatrix}} = \underset{H}{\begin{bmatrix} 1 & 0 & 3 & 42 \\ 0 & 3 & 6 & 75 \\ 0 & 0 & 15 & 45 \\ 0 & 0 & 0 & 105 \end{bmatrix}}$$

(Row) Hermite Normal Form

$A \in \mathbb{Z}^{m \times n}$, an integer matrix, full column rank. Hermite form of A:

$$H = \begin{bmatrix} h_1 & h_{12} & \cdots & h_{1n} \\ & h_2 & \cdots & h_{2n} \\ & & \ddots & \vdots \\ & & & h_n \\ & & & \\ & & & \end{bmatrix}$$

- has all entries nonnegative
- in each column: $h_{ij} < h_j$
- A left equivalent to H, there exists U with $UA = H$
- $U \in \mathbb{Z}^{m \times m}$ unimodular, represents the integer row operations

(Row) Hermite Normal Form

$A \in \mathbb{Z}^{m \times n}$, an integer matrix, full column rank. Hermite form of A:

$$UA = H = \begin{bmatrix} h_1 & h_{12} & \cdots & h_{1n} \\ & h_2 & \cdots & h_{2n} \\ & & \ddots & \vdots \\ & & & h_n \\ & & & \\ & & & \end{bmatrix}$$

- has all entries nonnegative
- in each column: $h_{ij} < h_j$
- A left equivalent to H, there exists U with $UA = H$
- $U \in \mathbb{Z}^{m \times m}$ unimodular, represents the integer row operations

Focus today will be on Hermite Normal Form:

Focus today will be on Hermite Normal Form:

Interesting points:

(1) Can also define HNF for singular matrices

(2) A nonsingular $A \in \mathbb{Z}^{n \times n}$ implies HNF is unique:

(3) Also have column Hermite forms

(4) Lots of other variations

- lower triangular rather than upper triangular
- first rather than last zero rows
- etc

Focus today will be on Hermite Normal Form:

Interesting points:

(1) Can also define HNF for singular matrices

(2) A nonsingular $A \in \mathbb{Z}^{n \times n}$ implies HNF is unique:

(3) Also have column Hermite forms

(4) Lots of other variations

- lower triangular rather than upper triangular
- first rather than last zero rows
- etc

- Goal: to compute HNF efficiently

Smith Normal Form

Given a nonsingular integer matrix $A \in \mathbb{Z}^{n \times n}$,

- the Smith normal form $S = \mathrm{diag}(s_1, s_2, \ldots, s_n) \in \mathbb{Z}^{n \times n}$.
- $s_1 \,|s_2\, | \ldots |\, s_n$ (invariant factors)

Smith Normal Form

Given a nonsingular integer matrix $A \in \mathbb{Z}^{n \times n}$,

- the Smith normal form $S = \mathrm{diag}(s_1, s_2, \ldots, s_n) \in \mathbb{Z}^{n \times n}$.
- $s_1 \,|s_2\, | \ldots |\, s_n$ (invariant factors)

$$\overset{A}{\begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}} \rightarrow \overset{S}{\begin{bmatrix} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{bmatrix}}$$

Smith Normal Form

Given a nonsingular integer matrix $A \in \mathbb{Z}^{n \times n}$,

- the Smith normal form $S = \mathrm{diag}(s_1, s_2, \ldots, s_n) \in \mathbb{Z}^{n \times n}$.
- $s_1 \mid s_2 \mid \ldots \mid s_n$ (invariant factors)

$$\overset{A}{\begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}} \rightarrow \overset{S}{\begin{bmatrix} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{bmatrix}}$$

- S is obtained using unimodular row and column operations.
- typically $UAV = S$ or $A = USV$

Smith normal form

In case we want multiplier matrices U and V

* We like the form $AV = US$

Smith normal form

In case we want multiplier matrices U and V

* We like the form $AV = US$

$$\overset{A}{\begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}} \rightarrow \overset{S}{\begin{bmatrix} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{bmatrix}}$$

Smith normal form

In case we want multiplier matrices U and V

* We like the form $AV = US$

$$\underset{A}{\begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}} \underset{V}{\begin{bmatrix} -26 & 5 & 15 & 55 \\ -62 & 0 & 22 & 137 \\ -20 & 2 & 17 & 41 \\ -53 & 2 & 25 & 115 \end{bmatrix}} = \underset{U}{\begin{bmatrix} -1313 & -17 & 24 & 28 \\ -4452 & 75 & 138 & 92 \\ -1548 & 14 & 49 & 32 \\ 369 & -39 & -23 & -7 \end{bmatrix}} \underset{S}{\begin{bmatrix} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{bmatrix}}$$

Smith normal form

In case we want multiplier matrices U and V

* We like the form $AV = US$
* However multiplier matrices are not unique

$$\underset{A}{\begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}} \underset{V}{\begin{bmatrix} -26 & 5 & 15 & 55 \\ -62 & 0 & 22 & 137 \\ -20 & 2 & 17 & 41 \\ -53 & 2 & 25 & 115 \end{bmatrix}} = \underset{U}{\begin{bmatrix} -1313 & -17 & 24 & 28 \\ -4452 & 75 & 138 & 92 \\ -1548 & 14 & 49 & 32 \\ 369 & -39 & -23 & -7 \end{bmatrix}} \underset{S}{\begin{bmatrix} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{bmatrix}}$$

Smith Normal Form

In case we want multiplier matrices U and V

* We like the form $AV = US$
* However multiplier matrices are not unique

$$\underset{A}{\begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}} \underset{\hat{V}}{\begin{bmatrix} 0 & -41968 & -41970 & -36695 \\ -4 & 19731 & 19732 & 17252 \\ 0 & 167 & 167 & 146 \\ -1 & -21004 & -21005 & -18365 \end{bmatrix}} = \underset{\hat{U}}{\begin{bmatrix} -67 & 57482 & 11497 & 1436 \\ -150 & -389607 & -77925 & -9733 \\ -66 & 57482 & 11497 & 1436 \\ -9 & 229929 & 45988 & 5744 \end{bmatrix}} \underset{S}{\begin{bmatrix} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{bmatrix}}$$

Some uses of Hermite and Smith Normal Forms

Integer Hermite and Smith forms are used in

- Solving systems of integer equations
- Finding rational invariants of scaling symmetries
- Classifying finite abellian groups, i.e. $G \equiv \mathbb{Z}_{p_1}^{n_1} \oplus \cdots \oplus \mathbb{Z}_{p_k}^{n_k}$
- Finding rational invariants of abelian finite group actions
- etc

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:

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 $H \in \mathbb{Z}_N^{m \times m}$:

- span of the rows of A is equal to span of the rows of H,
- H is in echelon form, leading non-zero entry in each row divides N,
- if h_{ij} is the first non-zero element in row i, then
  - $0 \leq h_{kj} < h_{ij}$ 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

Howell's algorithm (1986)

Let $A \in \mathbb{Z}_N^{n \times m}$ have rows $A_1, A_2, \ldots, A_n$. Assume $a_{11} \neq 0$.

1. Let $g_1 = \gcd(a_{11}, a_{21}, \ldots, a_{n1}, N)$. (In $\mathbb{Z}$.)
2. Get $g_1 = \sum_{i=1}^{n} f_i a_{i1}$. (In $\mathbb{Z}_N$.)
3. Let $H_1 = \sum_{i=1}^{n} f_i A_i$. (We get that the first element is g_1.)
4. Let $A'_i = A_i - b_i H_1$ where $a_{i1} = b_i g_1$ for $1 < i \leq m$.
5. Let $A'_{n+1} = (N/g_1) \cdot A_1$. (We get the first element is zero.)

Repeat second column of $A'_2, A'_3, \ldots, A'_{n+1}$ to get H_2,

Howell's algorithm (1986)

Let $A \in \mathbb{Z}_N^{n \times m}$ have rows $A_1, A_2, \ldots, A_n$. Assume $a_{11} \neq 0$.

1. Let $g_1 = \gcd(a_{11}, a_{21}, \ldots, a_{n1}, N)$. (In $\mathbb{Z}$.)
2. Get $g_1 = \sum_{i=1}^{n} f_i a_{i1}$. (In $\mathbb{Z}_N$.)
3. Let $H_1 = \sum_{i=1}^{n} f_i A_i$. (We get that the first element is g_1.)
4. Let $A'_i = A_i - b_i H_1$ where $a_{i1} = b_i g_1$ for $1 < i \leq m$.
5. Let $A'_{n+1} = (N/g_1) \cdot A_1$. (We get the first element is zero.)

Repeat second column of $A'_2, A'_3, \ldots, A'_{n+1}$ to get $H_2, \ldots, H_n$.

Computing the Howell Form

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

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix}$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix}$$

$$\gcd(9, 6, 12) = 3 \implies 1 \cdot 9 - 1 \cdot 6 \equiv 3 \mod 12$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ & & \end{bmatrix}$$

$$\gcd(9, 6, 12) = 3 \implies 1 \cdot 9 - 1 \cdot 6 \equiv 3 \mod 12$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 6 & 10 \\ & & \end{bmatrix}$$

$$6 \equiv 2 \cdot 3 \mod 12$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 6 & 10 \\ 0 & 8 & 11 \\ & & \end{bmatrix}$$

$$6 \equiv 2 \cdot 3 \mod 12$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 6 & 10 \\ 0 & 8 & 11 \\ & & \end{bmatrix}$$

$$9 \cdot 4 \equiv 0 \mod 12$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \rightarrow \begin{bmatrix} 3 & 6 & 10 \\ 0 & 8 & 11 \\ 0 & 8 & 8 \end{bmatrix}$$

$$9 \cdot 4 \equiv 0 \mod 12$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 8 & 11 \\ 0 & 8 & 8 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ & & \\ & & \end{bmatrix}$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 8 & 11 \\ 0 & 8 & 8 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ & & \\ & & \end{bmatrix}$$

$$\gcd(8, 8, 12) = 4 \implies 1 \cdot 8 + 1 \cdot 8 \equiv 4 \mod 12$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 8 & 11 \\ 0 & 8 & 8 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 4 & 7 \\ & & \end{bmatrix}$$

$$\gcd(8, 8, 12) = 4 \implies 1 \cdot 8 + 1 \cdot 8 \equiv 4 \mod 12$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 8 & 11 \\ 0 & 8 & 8 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 4 & 7 \\ & & \end{bmatrix}$$

$$8 \equiv 2 \cdot 4 \mod 12$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 8 & 11 \\ 0 & 8 & 8 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 4 & 7 \\ 0 & 0 & 6 \\ & & \end{bmatrix}$$

$$8 \equiv 2 \cdot 4 \mod 12$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 8 & 11 \\ 0 & 8 & 8 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 4 & 7 \\ 0 & 0 & 6 \\ & & \end{bmatrix}$$

$$8 \cdot 3 \equiv 0 \mod 12$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 8 & 11 \\ 0 & 8 & 8 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 4 & 7 \\ 0 & 0 & 6 \\ 0 & 0 & 9 \end{bmatrix}$$

$$8 \cdot 3 \equiv 0 \mod 12$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 8 & 11 \\ 0 & 8 & 8 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 4 & 7 \\ 0 & 0 & 6 \\ 0 & 0 & 9 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 4 & 7 \\ & & \end{bmatrix}$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 8 & 11 \\ 0 & 8 & 8 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 4 & 7 \\ 0 & 0 & 6 \\ 0 & 0 & 9 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 4 & 7 \\ & & \end{bmatrix}$$

$$\gcd(6, 9, 12) = 3 \implies -1 \cdot 6 + 1 \cdot 9 \equiv 3 \mod 12$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 8 & 11 \\ 0 & 8 & 8 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 4 & 7 \\ 0 & 0 & 6 \\ 0 & 0 & 9 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 4 & 7 \\ 0 & 0 & 3 \end{bmatrix}$$

$$\gcd(6, 9, 12) = 3 \implies -1 \cdot 6 + 1 \cdot 9 \equiv 3 \mod 12$$

Computing the Howell Form

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

Example

$$\begin{bmatrix} 9 & 2 & 5 \\ 6 & 8 & 7 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 8 & 11 \\ 0 & 8 & 8 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 4 & 7 \\ 0 & 0 & 6 \\ 0 & 0 & 9 \end{bmatrix} \to \begin{bmatrix} 3 & 6 & 10 \\ 0 & 4 & 7 \\ 0 & 0 & 3 \end{bmatrix} \to \begin{bmatrix} 3 & 2 & 0 \\ 0 & 4 & 1 \\ 0 & 0 & 3 \end{bmatrix}$$

How do we compute a Hermite form?

Naive Method (Using Extended Euclidean Algorithm)

$$A = \begin{bmatrix} -13 & 27 & 0 & -21 \\ 10 & 30 & 15 & 0 \\ -20 & 15 & 15 & -15 \\ 27 & 30 & 6 & 9 \end{bmatrix}$$

How do we compute a Hermite form?

Naive Method (Using Extended Euclidean Algorithm)

$$A = \begin{bmatrix} -13 & 27 & 0 & -21 \\ 10 & 30 & 15 & 0 \\ -20 & 15 & 15 & -15 \\ 27 & 30 & 6 & 9 \end{bmatrix}$$

Extended Euclidean Algorithm:

$$\begin{aligned} 3(-13) + 4(10) &= 1 \\ 10(-13) + 13(10) &= 0 \end{aligned}$$

How do we compute a Hermite form?

Naive Method (Using Extended Euclidean Algorithm)

$$A = \begin{bmatrix} -13 & 27 & 0 & -21 \\ 10 & 30 & 15 & 0 \\ -20 & 15 & 15 & -15 \\ 27 & 30 & 6 & 9 \end{bmatrix}$$

Extended Euclidean Algorithm:

$$\begin{aligned} 3(-13) + 4(10) &= 1 \\ 10(-13) + 13(10) &= 0 \end{aligned} \quad \text{i.e.} \quad \begin{bmatrix} 3 & 4 \\ 10 & 13 \end{bmatrix} \begin{bmatrix} -13 \\ 10 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

How do we compute a Hermite form?

Naive Method (Using Extended Euclidean Algorithm)

$$\underset{U_1}{\begin{bmatrix} 3 & 4 & 0 & 0 \\ 10 & 13 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}} \quad \underset{A}{\begin{bmatrix} -13 & 27 & 0 & -21 \\ 10 & 30 & 15 & 0 \\ -20 & 15 & 15 & -15 \\ 27 & 30 & 6 & 9 \end{bmatrix}} = \underset{A_1}{\begin{bmatrix} 1 & 201 & 60 & -63 \\ 0 & 660 & 195 & -210 \\ -20 & 15 & 15 & -15 \\ 27 & 30 & 6 & 9 \end{bmatrix}}$$

Extended Euclidean Algorithm:

$$\begin{aligned} 3(-13) + 4(10) &= 1 \\ 10(-13) + 13(10) &= 0 \end{aligned} \quad \text{i.e.} \quad \begin{bmatrix} 3 & 4 \\ 10 & 13 \end{bmatrix} \begin{bmatrix} -13 \\ 10 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Example

Naive Method

$$\underset{U_4}{\begin{bmatrix} 3 & 4 & 0 & 0 \\ 10 & 13 & 0 & 0 \\ 60 & 80 & 1 & 0 \\ -81 & -108 & 0 & 1 \end{bmatrix}} \quad \underset{A}{\begin{bmatrix} -13 & 27 & 0 & -21 \\ 10 & 30 & 15 & 0 \\ -20 & 15 & 15 & -15 \\ 27 & 30 & 6 & 9 \end{bmatrix}} = \underset{A_4}{\begin{bmatrix} 1 & 201 & 60 & -63 \\ 0 & 660 & 195 & -210 \\ 0 & 4035 & 1215 & -1275 \\ 0 & -5397 & -1614 & 1710 \end{bmatrix}}$$

Extended Euclidean Algorithm:

$$\begin{array}{rcl} 3(-13) + 4(10) & = & 1 \\ 10(-13) + 13(10) & = & 0 \end{array} \quad \text{i.e.} \quad \begin{bmatrix} 3 & 4 \\ 10 & 13 \end{bmatrix} \begin{bmatrix} -13 \\ 10 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Example

Naive Method

$$\underset{U}{\begin{bmatrix} -25 & -160 & 109 & 128 \\ -46 & -295 & 201 & 236 \\ -25 & -156 & 107 & 125 \\ -65 & -419 & 285 & 335 \end{bmatrix}} \underset{A}{\begin{bmatrix} -13 & 27 & 0 & -21 \\ 10 & 30 & 15 & 0 \\ -20 & 15 & 15 & -15 \\ 27 & 30 & 6 & 9 \end{bmatrix}} = \underset{H}{\begin{bmatrix} 1 & 0 & 3 & 42 \\ 0 & 3 & 6 & 75 \\ 0 & 0 & 15 & 45 \\ 0 & 0 & 0 & 105 \end{bmatrix}}$$

- Extended Euclidean Algorithm:

$$\begin{aligned} 3(-13) + 4(10) &= 1 \\ 10(-13) + 13(10) &= 0 \end{aligned} \quad \text{i.e.} \quad \begin{bmatrix} 3 & 4 \\ 10 & 13 \end{bmatrix} \begin{bmatrix} -13 \\ 10 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

- Exponential growth of intermediate integers

Sometimes it is okay though

$$A = \begin{bmatrix} d & & & & \\ w_1 & 1 & & & \\ w_2 & & 1 & & \\ w_3 & & & 1 & \\ w_4 & & & & 1 \end{bmatrix}.$$

Sometimes it is okay though

$$A = \begin{bmatrix} d & & & & \\ w_1 & 1 & & & \\ w_2 & & 1 & & \\ w_3 & & & 1 & \\ w_4 & & & & 1 \end{bmatrix}.$$

$$\begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{bmatrix} A = \begin{bmatrix} * & & & & \\ * & 1 & & & \\ * & & 1 & & \\ * & & & 1 & \\ * & & & & 1 \end{bmatrix}.$$

Sometimes it is okay though

$$A = \begin{bmatrix} d & & & & \\ w_1 & 1 & & & \\ w_2 & & 1 & & \\ w_3 & & & 1 & \\ w_4 & & & & 1 \end{bmatrix}.$$

$$\begin{bmatrix} * & & & & * \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ * & & & & * \end{bmatrix} A = \begin{bmatrix} * & & & & * \\ * & 1 & & & \\ * & & 1 & & \\ * & & & 1 & \\ & & & & h_4 \end{bmatrix}.$$

Sometimes its okay though

$$A = \begin{bmatrix} d & & & & \\ w_1 & 1 & & & \\ w_2 & & 1 & & \\ w_3 & & & 1 & \\ w_4 & & & & 1 \end{bmatrix}.$$

$$\begin{bmatrix} * & & & * & * \\ & 1 & & & \\ & & 1 & & \\ * & & & * & * \\ * & & & & * \end{bmatrix} A = \begin{bmatrix} * & & & * & * \\ * & 1 & & & \\ * & & 1 & & \\ & & & h_3 & * \\ & & & & h_4 \end{bmatrix}.$$

Sometimes its okay though

$$A = \begin{bmatrix} d & & & & \\ w_1 & 1 & & & \\ w_2 & & 1 & & \\ w_3 & & & 1 & \\ w_4 & & & & 1 \end{bmatrix}.$$

$$\begin{bmatrix} * & & * & * & * \\ & 1 & & & \\ * & & * & * & * \\ * & & & * & * \\ * & & & & * \end{bmatrix} A = \begin{bmatrix} * & & * & * & * \\ * & 1 & & & \\ & & h_2 & * & * \\ & & & h_3 & * \\ & & & & h_4 \end{bmatrix}.$$

Sometimes its okay though

$$A = \begin{bmatrix} d & & & & \\ w_1 & 1 & & & \\ w_2 & & 1 & & \\ w_3 & & & 1 & \\ w_4 & & & & 1 \end{bmatrix}.$$

$$\begin{bmatrix} * & * & * & * & * \\ * & * & * & * & * \\ * & & * & * & * \\ * & & & * & * \\ * & & & & * \end{bmatrix} A = \begin{bmatrix} * & * & * & * & * \\ & h_1 & * & * & * \\ & & h_2 & * & * \\ & & & h_3 & * \\ & & & & h_4 \end{bmatrix}.$$

Sometimes its okay though

$$A = \begin{bmatrix} d & & & & \\ w_1 & 1 & & & \\ w_2 & & 1 & & \\ w_3 & & & 1 & \\ w_4 & & & & 1 \end{bmatrix}.$$

$$\begin{bmatrix} * & * & * & * & * \\ * & * & * & * & * \\ * & & * & * & * \\ * & & & * & * \\ * & & & & * \end{bmatrix} A = \begin{bmatrix} * & * & * & * & * \\ & h_1 & * & * & * \\ & & h_2 & * & * \\ & & & h_3 & * \\ & & & & h_4 \end{bmatrix}.$$

- Afterwards work low to high to reduce column sizes.

Sometimes its okay though

$$A = \begin{bmatrix} d & & & & \\ w_1 & 1 & & & \\ w_2 & & 1 & & \\ w_3 & & & 1 & \\ w_4 & & & & 1 \end{bmatrix}.$$

$$\begin{bmatrix} * & * & * & * & * \\ * & * & * & * & * \\ * & & * & * & * \\ * & & & * & * \\ * & & & & * \end{bmatrix} A = \begin{bmatrix} * & * & * & * & * \\ & h_1 & * & * & * \\ & & h_2 & * & * \\ & & & h_3 & * \\ & & & & h_4 \end{bmatrix}.$$

- Afterwards work low to high to reduce column sizes.
- Unfortunately terms in red very large

Computation: A Bit of History

(1) Bradley 1971:

- Triangulate using Extended Euclidean Algorithm
- Algo. not polynomial because of intermediate expression swell

(2) Kannan and Bachem [1979]

- Change flow of computation
- Worked along $1 \times 1, 2 \times 2, \cdots, n \times n$ submatrices
- Algorithm polynomial in bit-size and arithmetic operations
- Practical terms: still has intermediate expression swell

(3) Domich, Kannan, and Trotter [1987]

- Control sizes via working mod determinant

More recent history (integer)

Citation	Time complexity	Type
Chou and Collins (1982)	$O^{\sim}(n^6(\log \|\|A\|\|))$	Det
Domich et al (1987), Illiopoulos (1989) Hafner and McCurley (1989)	$O^{\sim}(n^4(\log \|\|A\|\|))$	Det
Storjohann and L.(1996)	$O^{\sim}(n^{\omega+1}(\log \|\|A\|\|))$	Det
$*$ Birmpilis, L., Storjohann (2023)	$O^{\sim}(n^3(\log \|\|A\|\|))$	LV

- ω exponent of matrix multiplication
  - Standard arithmetic $\omega = 3$; Sub-cubic arithmetic $\omega < 2.37286$
- $\log ||A|| \sim$ bound for the bit-length of entries in A
- Complexity is given without the extra $\log n$ and $\log \log ||A||$ factors.

History for Smith Normal Form

Citation	Time complexity	Type
Kannan and Bachem (1979)	$poly(n, \log \|\|A\|\|)$	Det
Iliopoulos (1989)	$n^5(\log \|\|A\|\|)^2$	Det
Hafner and McCurley (1991)	$n^5(\log \|\|A\|\|)^2$	Det
Storjohann (1996)	$n^{\omega+1} \log \|\|A\|\|$	Det
Eberly, Giesbrecht and Villard (2000)	$n^{2+\omega/2} \log \|\|A\|\|$	MC
Birmpilis, L.,Storjohann (2020)	$n^{\omega} \log \|\|A\|\|$	LV

History for Smith Normal Form

Citation	Time complexity	Type
Kannan and Bachem (1979)	$poly(n, \log \|\|A\|\|)$	Det
Iliopoulos (1989)	$n^5(\log \|\|A\|\|)^2$	Det
Hafner and McCurley (1991)	$n^5(\log \|\|A\|\|)^2$	Det
Storjohann (1996)	$n^{\omega+1} \log \|\|A\|\|$	Det
Eberly, Giesbrecht and Villard (2000)	$n^{2+\omega/2} \log \|\|A\|\|$	MC
Birmpilis, L.,Storjohann (2020)	$n^{\omega} \log \|\|A\|\|$	LV

Notice similar set of names (and dates) for Smith and Hermite

Some Oddities

Oddity 1: Faster algorithms for polynomial Hermite form:

L.-Neiger-Zhou (2017)	$O^{\sim}(n^{\omega}s)$	Deterministic

- s minimum of the average of column/row degrees

Oddity 2: Faster algorithms for Smith form (with multipliers)

Birmpilis, L., Storjohann (2023)	$O^{\sim}(n^{\omega}\log\|\|A\|\|)$	LV

Our Algorithm

Given $A \in \mathbb{Z}^{n \times n}$ a nonsingular integer. We compute H with cost:

- $O(n^3(\log n + \log ||A||)^2(\log n)^2)$ bit operations,
  - using standard integer multiplication and matrix multiplication.

Our Algorithm

Given $A \in \mathbb{Z}^{n \times n}$ a nonsingular integer. We compute H with cost:

- $O(n^3(\log n + \log ||A||)^2(\log n)^2)$ bit operations,
  - using standard integer multiplication and matrix multiplication.
- $O(n^3(\log n + \log ||A||)^2)$ bit operations ,
  - if use a subcubic matrix multiplication (e.g. Strassen's),
- $O^{\sim}(n^3 \log ||A||)$ bit operations,
  - variant assumes fast (pseudo-linear) integer multiplication

Our Algorithm

Given $A \in \mathbb{Z}^{n \times n}$ a nonsingular integer. We compute H with cost:

- $O(n^3(\log n + \log ||A||)^2(\log n)^2)$ bit operations,
  - using standard integer multiplication and matrix multiplication.
- $O(n^3(\log n + \log ||A||)^2)$ bit operations ,
  - if use a subcubic matrix multiplication (e.g. Strassen's),
- $O^{\sim}(n^3 \log ||A||)$ bit operations,
  - variant assumes fast (pseudo-linear) integer multiplication

Space: $O(n^2(\log n + \log ||A||))$ bits - same as required to write down H.

Our Approach (roughly, in words)

- View problem differently (normalized minimal denominators)
- Work with simpler objects (bring Smith form into play)
- Work column by column with normalized denominators
  (this gets us the diagonal elements of H)
- Work in dual with modular domain and normalize
  (normalization gives remaining elements of H)

Step 1: Hermite Minimal Denominators

1. Minimal Denominator : $UA = H \quad \rightarrow \quad HA^{-1} = U \in \mathbb{Z}^{n \times n}$

Note: Can define for any $B \in \mathbb{Q}^{n \times m}$, i.e. $HB \in \mathbb{Z}^{n \times m}$

Step 1: Hermite Minimal Denominators

1. Minimal Denominator : $UA = H \quad \rightarrow \quad HA^{-1} = U \in \mathbb{Z}^{n \times n}$

   Note: Can define for any $B \in \mathbb{Q}^{n \times m}$, i.e. $HB \in \mathbb{Z}^{n \times m}$

   Note: Example: $B = \vec{w}/d \in \mathbb{Q}^{n \times 1}$, $H\vec{w} = dU, U \in \mathbb{Z}^{n \times 1}$

Step 1: Hermite Minimal Denominators

Example :

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

Step 1: Hermite Minimal Denominators

Example :

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

Step 1: Hermite Minimal Denominators

Example :

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

- H: Minimal determinant in Hermite form
- All minimal sized multipliers are left equivalent
- det H divides det of all other denominators of A.

Step 1: Hermite Minimal Denominators

Example :

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

- Bad: We do not actually want to compute A^{-1}
  - In worst case requires $\Omega(n^3(\log n + \log ||A||))$ space

Step 1: Hermite Minimal Denominators

Example :

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

- Bad: We do not actually want to compute A^{-1}
  - In worst case requires $\Omega(n^3(\log n + \log ||A||))$ space
- Good: Minimal denominator approach brings Smith form into play

Step 2: Smith Massager

Smith Multipliers. (S diagonal).

$$AV = WS \quad \text{with } V, W \text{ unimodular}$$

Step 2: Smith Massager

Smith Multipliers. (S diagonal).

$$\begin{aligned} AV &= WS \quad \text{with } V, W \text{ unimodular} \\ VS^{-1} &= A^{-1}W \end{aligned}$$

Step 2: Smith Massager

Smith Multipliers. (S diagonal).

$$\begin{aligned} AV &= WS \quad \text{with } V, W \text{ unimodular} \\ VS^{-1} &= A^{-1}W \\ (M + RS)S^{-1} &= A^{-1}W \end{aligned}$$

Step 2: Smith Massager

Smith Multipliers. (S diagonal).

$$\begin{aligned} AV &= WS \quad \text{with } V, W \text{ unimodular} \\ VS^{-1} &= A^{-1}W \\ (M + RS)S^{-1} &= A^{-1}W \\ MS^{-1} &= A^{-1}W \mod \mathbb{Z} \end{aligned}$$

- $M = V$ cmod S is called a Smith Massager.
- A^{-1} and MS^{-1} have the same Hermite minimal denominators

Example

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

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

Example

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

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

- Las Vegas algorithms : (BLS - ISSAC'20, JSC 2023)
- Cost : $O(n^3(\log n + \log \|A\|)^2(\log n)^2)$ bit operations

Example

Smith Massager : Set $M = V \text{ cmod } S$

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

- ◇ Las Vegas algorithms : (BLS - ISSAC'20, JSC 2023)
- ◇ Cost : $O(n^3(\log n + \log \|A\|)^2(\log n)^2)$ bit operations

Example

Smith Massager : Set $M = V \text{ cmod } S$

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

Notice: $AV = WS \implies A(M + CS) = WS \implies AM = \hat{W}S$

Example

Smith Massager : Set $M = V \text{ cmod } S$

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

Notice: $AV = WS \implies A(M + CS) = WS \implies AM = \hat{W}S$

Minimal denominator of A^{-1} same as minimal denominator of MS^{-1}

Example

Now use hcol algorithm of Pauderis-Storjohann

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

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

Now use hcol algorithm of Pauderis-Storjohann

$$\underset{M_4}{\begin{bmatrix} 9 \\ 4 \\ 4 \\ 8 \end{bmatrix}} /16 \quad \Longrightarrow \quad \underset{H}{\begin{bmatrix} 4 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}}$$

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

Now use hcol algorithm of Pauderis-Storjohann

$$\underset{M_4}{\begin{bmatrix} 9 \\ 4 \\ 4 \\ 8 \end{bmatrix}} /16 \quad \Longrightarrow \quad \underset{H}{\begin{bmatrix} 4 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}}$$

Check:

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

How does Pauderis-Storjohann's hcol algorithm work?

hcol$(\vec{w}, d)$ same as finding Hermite Normal form of

$$\begin{bmatrix} d & & & & \\ w_1 & 1 & & & \\ w_2 & & 1 & & \\ w_3 & & & 1 & \\ w_4 & & & & 1 \end{bmatrix}$$

How does Pauderis-Storjohann's hcol algorithm work?

hcol$(\vec{w}, d)$ same as finding Hermite Normal form of

$$\begin{bmatrix} * & * & * & * & * \\ * & * & * & * & * \\ * & & * & * & * \\ * & & & * & * \\ * & & & & * \end{bmatrix} \begin{bmatrix} d & & & & \\ w_1 & 1 & & & \\ w_2 & & 1 & & \\ w_3 & & & 1 & \\ w_4 & & & & 1 \end{bmatrix} = \begin{bmatrix} * & * & * & * & * \\ & h_1 & * & * & * \\ & & h_2 & * & * \\ & & & h_3 & * \\ & & & & h_4 \end{bmatrix}.$$

with Hermite denominator in bottom $n \times n$ corner

How does Pauderis-Storjohann's hcol algorithm work?

hcol$(\vec{w}, d)$ same as finding Hermite Normal form of

$$\begin{bmatrix} * & * & * & * & * \\ * & * & * & * & * \\ * & & * & * & * \\ * & & & * & * \\ * & & & & * \end{bmatrix} \begin{bmatrix} d & & & & \\ w_1 & 1 & & & \\ w_2 & & 1 & & \\ w_3 & & & 1 & \\ w_4 & & & & 1 \end{bmatrix} = \begin{bmatrix} * & * & * & * & * \\ & h_1 & * & * & * \\ & & h_2 & * & * \\ & & & h_3 & * \\ & & & & h_4 \end{bmatrix}.$$

with Hermite denominator in bottom $n \times n$ corner

Notice that we do not need to actually generate red entries

Continuing

1. Minimal Denominator : $UA = H \quad \rightarrow \quad HA^{-1} = U \in \mathbb{Z}^{n \times n}$

   Note: Can define for any $B \in \mathbb{Q}^{n \times m}$, i.e. $HB \in \mathbb{Z}^{n \times m}$

2. Smith Massager : Bring Smith Normal Form computation into play.

3. Hermite Minimal Denominators for columns

   Get a minimal triangular denominator as product of n minimal Hermite denominators. Gives diagonals of H

Step 3: Finding diagonals of H

Lemma

Suppose $B = \left[\begin{array}{c|c} B_1 & B_2 \end{array}\right]$. *If* H_1 *is a minimal denom. of* B_1, *and* H_2 *is a minimal denom. of* $H_1 B_2$, *then* $H_2 H_1$ *is a minimal denom. of* B.

Step 3: Finding diagonals of H

Lemma

Suppose $B = \left[\begin{array}{c|c} B_1 & B_2 \end{array}\right]$. *If* H_1 *is a minimal denom. of* B_1, *and* H_2 *is a minimal denom. of* $H_1 B_2$, *then* $H_2 H_1$ *is a minimal denom. of* B.

- If M is Smith massager and $S = diag(s_1, \ldots, s_n)$ then:

  For $i = 1$ to n do
  $\quad \hat{H}_i := \texttt{hcol}(\text{Column}(M, i), s_i)$
  $\quad M := cmod(\hat{H}_i M, S)$
  od

Step 3: Finding diagonals of H

Lemma

Suppose $B = \left[\begin{array}{c|c} B_1 & B_2 \end{array}\right]$. *If* H_1 *is a minimal denom. of* B_1, *and* H_2 *is a minimal denom. of* $H_1 B_2$, *then* $H_2 H_1$ *is a minimal denom. of* B.

- If M is Smith massager and $S = diag(s_1, \ldots, s_n)$ then:

  For $i = 1$ to n do
  $\quad \hat{H}_i := \texttt{hcol}(\text{Column}(M, i), s_i)$
  $\quad M := cmod(\hat{H}_i M, S)$
  od

- Product $\hat{H}_n \hat{H}_{n-1} \cdots \hat{H}_1$ is a minimal denominator of MS^{-1}

- Product is upper triangular but not in Hermite form.

Step 3: Finding diagonals of H

Lemma

Suppose $B = \left[\begin{array}{c|c} B_1 & B_2 \end{array}\right]$. *If* H_1 *is a minimal denom. of* B_1, *and* H_2 *is a minimal denom. of* $H_1 B_2$, *then* $H_2 H_1$ *is a minimal denom. of* B.

- If M is Smith massager and $S = diag(s_1, \ldots, s_n)$ then:

  For $i = 1$ to n do
  $\quad \hat{H}_i := \texttt{hcol}(\text{Column}(M, i), s_i)$
  $\quad M := cmod(\hat{H}_i M, S)$
  od

- Product $\hat{H}_n \hat{H}_{n-1} \cdots \hat{H}_1$ is a minimal denominator of MS^{-1}
- Product is upper triangular but not in Hermite form.
- Product of diagonals of $\hat{H}_n \hat{H}_{n-1} \cdots \hat{H}_1$ gives diagonals of H

Example : Diagonals of H

$$A = \begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}$$

Example : Diagonals of H

$$A = \begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix} \quad \text{BLS} \implies S = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 105 \end{bmatrix} \quad \text{and} \quad M = \begin{bmatrix} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{bmatrix}$$

Example : Diagonals of H

$$A = \begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix} \quad \text{BLS} \implies S = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 105 \end{bmatrix} \quad \text{and} \quad M = \begin{bmatrix} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{bmatrix}$$

- Diagonal elements of H turn out: $h_1 = 1, h_2 = 15, h_3 = 15, h_4 = 21$.

Example : Diagonals of H

$$A = \begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix} \quad \text{BLS} \implies S = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 105 \end{bmatrix} \quad \text{and} \quad M = \begin{bmatrix} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{bmatrix}$$

- Diagonal elements of H turn out: $h_1 = 1, h_2 = 15, h_3 = 15, h_4 = 21$.
- Therefore $H = \begin{bmatrix} 1 & h_{12} & h_{13} & h_{14} \\ 0 & 15 & h_{23} & h_{24} \\ 0 & 0 & 15 & h_{34} \\ 0 & 0 & 0 & 21 \end{bmatrix}$

Step 4: Duality

Step 4: Duality: Continue working with inverses

Finding H^{-1} as good as finding H.

Step 4: Duality: Continue working with inverses

Finding H^{-1} as good as finding H.

Let H_j be j^{th} column of H^{-1}. Then $H^{-1} = H_n H_{n-1} \cdots H_1$.

Step 4: Duality: Continue working with inverses

Finding H^{-1} as good as finding H.

Let H_j be j^{th} column of H^{-1}. Then $H^{-1} = H_n H_{n-1} \cdots H_1$.

Let: $s = s_n$, largest invariant factor

$\diamond$. Let $H^* = sH^{-1}$, $\quad A^* = sA^{-1}$ and $\quad U^* = U^{-1}$

$\diamond$. Then $UA = H \implies H^{-1} = A^{-1}U^{-1} \implies H^* = A^*U^*$

Step 4: Duality: Continue working with inverses

Finding H^{-1} as good as finding H.

Let H_j be j^{th} column of H^{-1}. Then $H^{-1} = H_n H_{n-1} \cdots H_1$.

Let: $s = s_n$, largest invariant factor

$\diamond$. Let $H^* = sH^{-1}$, $A^* = sA^{-1}$ and $U^* = U^{-1}$

$\diamond$. Then $UA = H \implies H^{-1} = A^{-1}U^{-1} \implies H^* = A^*U^*$

$\diamond$. we will replace H^* by a different 'column reduced matrix' T

Working in the dual

$A^*U^* = H^*$:

- Can prove that H^* is a column Howell form for A^* in $\mathbb{Z}/(s)$

Working in the dual

$A^*U^* = H^*$:

- Can prove that H^* is a column Howell form for A^* in $\mathbb{Z}/(s)$
- Replace H^* by any upper triang. T having same diag. entries.
- Column Howell form is a natural choice for T

Example: Replace H^{-1} by Howell form

Recall:

$$\underset{A}{\begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}} \quad \text{BLS} \implies \underset{S}{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 105 \end{bmatrix}} \quad \text{and} \quad \underset{M}{\begin{bmatrix} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{bmatrix}}$$

◇ Diagonal elements of H then $h_1 = 1, h_2 = 15, h_3 = 15, h_4 = 21$.

$$\text{Know} \quad \underset{H}{\begin{bmatrix} 1 & h_{12} & h_{13} & h_{14} \\ 0 & 15 & h_{23} & h_{24} \\ 0 & 0 & 15 & h_{34} \\ 0 & 0 & 0 & 21 \end{bmatrix}}.$$

Example: Replace H^{-1} by Howell form

Recall:

$$\underset{A}{\begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}} \quad \text{BLS} \implies \underset{S}{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 105 \end{bmatrix}} \quad \text{and} \quad \underset{M}{\begin{bmatrix} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{bmatrix}}$$

◇ Diagonal elements of H then $h_1 = 1, h_2 = 15, h_3 = 15, h_4 = 21$.

$$\underset{HowellForm}{\begin{bmatrix} \frac{105}{h_1} & 70 & 70 & 45 \\ 0 & \frac{105}{h_2} & 0 & 100 \\ 0 & 0 & \frac{105}{h_3} & 101 \\ 0 & 0 & 0 & \frac{105}{h_4} \end{bmatrix}} = \underset{T}{\begin{bmatrix} 105 & 70 & 70 & 45 \\ 0 & 7 & 0 & 100 \\ 0 & 0 & 7 & 101 \\ 0 & 0 & 0 & 5 \end{bmatrix}}$$

Example

Recall:

$$\underset{A}{\begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}} \quad \text{BLS} \implies \underset{S}{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 105 \end{bmatrix}} \quad \text{and} \quad \underset{M}{\begin{bmatrix} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{bmatrix}}$$

◇ Diagonal elements of H then $h_1 = 1, h_2 = 15, h_3 = 15, h_4 = 21$.

$$\underset{H_1}{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}} \quad \text{and} \quad \underset{H_1T}{\begin{bmatrix} 105 & 70 & 70 & 45 \\ 0 & 7 & 0 & 100 \\ 0 & 0 & 7 & 101 \\ 0 & 0 & 0 & 5 \end{bmatrix}}$$

Example

Recall:

$$\underset{A}{\begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}} \quad \text{BLS} \implies \underset{S}{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 105 \end{bmatrix}} \quad \text{and} \quad \underset{M}{\begin{bmatrix} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{bmatrix}}$$

◇ Diagonal elements of H then $h_1 = 1, h_2 = 15, h_3 = 15, h_4 = 21$.

$$\underset{H_2}{\begin{bmatrix} 1 & 5 & 0 & 0 \\ 0 & 15 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}} \quad \text{and} \quad \underset{H_2 H_1 T}{\begin{bmatrix} 0 & 0 & 70 & 20 \\ 0 & 0 & 0 & 30 \\ 0 & 0 & 7 & 101 \\ 0 & 0 & 0 & 5 \end{bmatrix}}$$

Example

Recall:

$$\underset{A}{\begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}} \quad \text{BLS} \implies \underset{S}{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 105 \end{bmatrix}} \quad \text{and} \quad \underset{M}{\begin{bmatrix} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{bmatrix}}$$

◇ Diagonal elements of H then $h_1 = 1, h_2 = 15, h_3 = 15, h_4 = 21$.

$$\underset{H_3}{\begin{bmatrix} 1 & 0 & 5 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}} \quad \text{and} \quad \underset{H_3H_2H_1T}{\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 30 \\ 0 & 0 & 0 & 45 \\ 0 & 0 & 0 & 5 \end{bmatrix}}$$

Example

Recall:

$$\underset{A}{\begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}} \quad \text{BLS} \implies \underset{S}{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 105 \end{bmatrix}} \quad \text{and} \quad \underset{M}{\begin{bmatrix} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{bmatrix}}$$

◇ Diagonal elements of H then $h_1 = 1, h_2 = 15, h_3 = 15, h_4 = 21$.

$$\underset{H_4}{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 15 \\ 0 & 0 & 1 & 12 \\ 0 & 0 & 0 & 21 \end{bmatrix}} \quad \text{and} \quad \underset{H_4H_3H_2H_1T}{\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}}$$

Example

Recall:

$$\underset{A}{\begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}} \quad \text{BLS} \implies \underset{S}{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 105 \end{bmatrix}} \quad \text{and} \quad \underset{M}{\begin{bmatrix} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{bmatrix}}$$

◇ Diagonal elements of H then $h_1 = 1, h_2 = 15, h_3 = 15, h_4 = 21$.

$$\text{Finally: } H = H_4 H_3 H_2 H_1 = \underset{H}{\begin{bmatrix} 1 & 5 & 5 & 0 \\ 0 & 15 & 0 & 15 \\ 0 & 0 & 15 & 12 \\ 0 & 0 & 0 & 21 \end{bmatrix}}$$