

Normal Forms for integer matrices

George Labahn

Cheriton School of Computer Science
University of Waterloo

CASC, Havana University
August 29, 2023

Outline

Motivation

Hermite Normal Form

Computing the Hermite Normal Form

Fast Hermite Normal Form (Integer)

Motivation

Recall: Gcds and Bezout equation

Given $b, c \in \mathbb{Z}$

Finding $\mathbf{gcd}(b, c) = d$ typically involves:

- (1) find v_1, v_2 such that $b = v_1d$ and $c = v_2d$
- (2) find u_1, u_2 such that $u_1b + u_2c = d$
- (3) d is 'normalized'

Recall: Gcds and Bezout equation

Given $b, c \in \mathbb{Z}$

Finding $\mathbf{gcd}(b, c) = d$ typically involves:

(1) find v_1, v_2 such that $b = v_1d$ and $c = v_2d$

(2) find u_1, u_2 such that $u_1b + u_2c = d$

(3) d is 'normalized'

Note: (1) and (2) implies $u_1v_1 + u_2v_2 = 1$

Recall: Gcds and Bezout equation

Given $b, c \in \mathbb{Z}$

Finding $\mathbf{gcd}(b, c) = d$ typically involves:

(1) find v_1, v_2 such that $b = v_1d$ and $c = v_2d$

(2) find u_1, u_2 such that $u_1b + u_2c = d$

(3) d is 'normalized'

Note: (1) and (2) implies $u_1v_1 + u_2v_2 = 1$

What about when b, c are both **matrices**?

Matrix gcds?

Given $b, c \in \mathbb{Z}^{m \times m}$: Find $\mathbf{rgcd}(b, c) = d$

Matrix gcds?

Given $b, c \in \mathbb{Z}^{m \times m}$: Find $\mathbf{rgcd}(b, c) = d$

$$\begin{bmatrix} b \\ c \end{bmatrix}$$

Matrix gcds?

Given $b, c \in \mathbb{Z}^{m \times m}$: Find $\mathbf{rgcd}(b, c) = d$

$$\begin{bmatrix} u_1 & u_2 \\ * & * \end{bmatrix} \begin{bmatrix} b \\ c \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}$$

Matrix gcds?

Given $b, c \in \mathbb{Z}^{m \times m}$: Find $\mathbf{rgcd}(b, c) = d$

$$\begin{bmatrix} u_1 & u_2 \\ * & * \end{bmatrix} \begin{bmatrix} b \\ c \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} v_1 & * \\ v_2 & * \end{bmatrix} \begin{bmatrix} u_1 & u_2 \\ * & * \end{bmatrix} = \begin{bmatrix} I_m & 0 \\ 0 & I_m \end{bmatrix}$$

Matrix gcds?

Given $b, c \in \mathbb{Z}^{m \times m}$: Find $\mathbf{rgcd}(b, c) = d$.

$$\begin{bmatrix} b \\ c \end{bmatrix} = \begin{bmatrix} v_1 & * \\ v_2 & * \end{bmatrix} \begin{bmatrix} d \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} u_1 & u_2 \\ * & * \end{bmatrix} \begin{bmatrix} v_1 & * \\ v_2 & * \end{bmatrix} = \begin{bmatrix} I_m & 0 \\ 0 & I_m \end{bmatrix}$$

Matrix gcds?

Given $b, c \in \mathbb{Z}^{m \times m}$: Find $\mathbf{rgcd}(b, c) = d$.

$$\begin{bmatrix} b \\ c \end{bmatrix} = \begin{bmatrix} v_1 & * \\ v_2 & * \end{bmatrix} \begin{bmatrix} d \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} u_1 & u_2 \\ * & * \end{bmatrix} \begin{bmatrix} v_1 & * \\ v_2 & * \end{bmatrix} = \begin{bmatrix} I_m & 0 \\ 0 & I_m \end{bmatrix}$$

Implies:

$$b = v_1 d$$

$$c = v_2 d$$

Matrix gcds?

Given $b, c \in \mathbb{Z}^{m \times m}$: Find $\mathbf{rgcd}(b, c) = d$.

$$\begin{bmatrix} b \\ c \end{bmatrix} = \begin{bmatrix} v_1 & * \\ v_2 & * \end{bmatrix} \begin{bmatrix} d \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} u_1 & u_2 \\ * & * \end{bmatrix} \begin{bmatrix} v_1 & * \\ v_2 & * \end{bmatrix} = \begin{bmatrix} I_m & 0 \\ 0 & I_m \end{bmatrix}$$

Implies:

$$b = v_1 d$$

$$c = v_2 d$$

$$u_1 v_1 + u_2 v_2 = I_m$$

Matrix gcds?

Given $b, c \in \mathbb{Z}^{m \times m}$: Find $\mathbf{rgcd}(b, c) = d$.

$$\begin{bmatrix} b \\ c \end{bmatrix} = \begin{bmatrix} v_1 & * \\ v_2 & * \end{bmatrix} \begin{bmatrix} d \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} u_1 & u_2 \\ * & * \end{bmatrix} \begin{bmatrix} v_1 & * \\ v_2 & * \end{bmatrix} = \begin{bmatrix} I_m & 0 \\ 0 & I_m \end{bmatrix}$$

Implies:

$$b = v_1 d$$

$$c = v_2 d$$

$$u_1 v_1 + u_2 v_2 = I_m$$

$$d \quad \text{'normalized'}$$

Matrix gcds?

Given $b, c \in \mathbb{Z}^{m \times m}$: Find $\mathbf{rgcd}(b, c) = d$.

$$\begin{bmatrix} b \\ c \end{bmatrix} = \begin{bmatrix} v_1 & * \\ v_2 & * \end{bmatrix} \begin{bmatrix} d \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} u_1 & u_2 \\ * & * \end{bmatrix} \begin{bmatrix} v_1 & * \\ v_2 & * \end{bmatrix} = \begin{bmatrix} I_m & 0 \\ 0 & I_m \end{bmatrix}$$

Implies:

$$b = v_1 d$$

$$c = v_2 d$$

$$u_1 v_1 + u_2 v_2 = I_m$$

$$d \quad \text{'normalized'}$$

Similarly for $b, c \in \mathbb{K}[z]^{m \times m}$.

Hermite Normal Form

Definition

$A \in \mathbb{Z}^{m \times n}$, 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 $UA = H$

Definition

$A \in \mathbb{Z}^{m \times n}$, 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, i.e. $\det U = \pm 1$
 - U represents the integer row operations

Definition

$A \in \mathbb{Z}^{m \times n}$, 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, i.e. $\det U = \pm 1$
 - U represents the integer row operations

Similar notion for polynomial matrices

Example 1:

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

Example 1:

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

Example 1:

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

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

Example 2: (simpler) :

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

Interesting Points:

- (1) HNF dates back to Hermite in 1851
- (2) Can also define HNF for singular matrices
- (3) A nonsingular $A \in \mathbb{Z}^{n \times n}$ implies HNF is unique:
- (4) Also have column Hermite forms
- (5) Lots of other variations
 - ▶ lower triangular rather than upper triangular
 - ▶ first rather than last zero rows
 - ▶ etc

Applications

Integer HNF form used in

- ▶ Solving systems of integer equations
- ▶ Finding rational invariants of scaling symmetries
- ▶ Finding rational invariants of abelian finite group actions
- ▶ etc

We are interested in computing H efficiently.

Another normal form: Smith

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

The Smith normal form

- ▶ $S = \text{diag}(s_1, s_2, \dots, s_n) \in \mathbb{Z}^{n \times n}$.
- ▶ $s_1 \mid s_2 \mid \dots \mid s_n$. (invariant factors)

Another normal form: Smith

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

The Smith normal form

- ▶ $S = \text{diag}(s_1, s_2, \dots, s_n) \in \mathbb{Z}^{n \times n}$.
- ▶ $s_1 \mid s_2 \mid \dots \mid s_n$. (invariant factors)

$$\begin{array}{c} A \\ \left[\begin{array}{cccccc} -8 & -1 & 5 & 1 & 6 & 0 \\ 2 & -3 & -8 & -3 & 2 & -1 \\ -5 & -4 & -5 & 9 & -4 & 4 \\ 2 & -6 & -1 & -8 & 9 & -7 \\ -9 & 5 & -5 & -6 & 2 & -7 \\ 0 & -6 & -4 & 6 & 0 & -8 \end{array} \right] \end{array} \rightarrow \begin{array}{c} S \\ \left[\begin{array}{cccccc} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 2 & \\ & & & & & 206750 \end{array} \right] \end{array}$$

Another normal form: Smith

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

The Smith normal form

- ▶ $S = \text{diag}(s_1, s_2, \dots, s_n) \in \mathbb{Z}^{n \times n}$.
- ▶ $s_1 \mid s_2 \mid \dots \mid s_n$. (invariant factors)

$$\begin{array}{c} A \\ \left[\begin{array}{cccccc} -8 & -1 & 5 & 1 & 6 & 0 \\ 2 & -3 & -8 & -3 & 2 & -1 \\ -5 & -4 & -5 & 9 & -4 & 4 \\ 2 & -6 & -1 & -8 & 9 & -7 \\ -9 & 5 & -5 & -6 & 2 & -7 \\ 0 & -6 & -4 & 6 & 0 & -8 \end{array} \right] \end{array} \rightarrow \begin{array}{c} S \\ \left[\begin{array}{cccccc} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 2 & \\ & & & & & 206750 \end{array} \right] \end{array}$$

- ▶ S obtained using unimodular row and column operations.
- ▶ typically $UAV = S$ or $AV = WS$

Computing the Hermite Normal Form

Computation: Naive Methods

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

Computation: Naive Methods

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

- ▶ Extended Euclidean Algorithm e.g.:

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

Computation: Naive Methods

$$\begin{matrix} U_1 & & A & & & & A_1 \\ \left[\begin{array}{cccc} 3 & 4 & 0 & 0 \\ 10 & 13 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right] & & \left[\begin{array}{cccc} -13 & 27 & 0 & -21 \\ 10 & 30 & 15 & 0 \\ -20 & 15 & 15 & -15 \\ 27 & 30 & 6 & 9 \end{array} \right] & = & & \left[\begin{array}{cccc} 1 & 201 & 60 & -63 \\ 0 & 660 & 195 & -210 \\ -20 & 15 & 15 & -15 \\ 27 & 30 & 6 & 9 \end{array} \right] \end{matrix}$$

- ▶ Extended Euclidean Algorithm e.g.:

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

Example

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

- ▶ Extended Euclidean Algorithm used for elimination. e.g.:

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

Example

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

- ▶ Extended Euclidean Algorithm used for elimination. e.g.:

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

- ▶ Exponential growth of intermediate integers

Historical Results

- (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 $1 \times 1, 2 \times 2, \dots, n \times n$ 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

Modulo Determinant?

(7) If $UA = H$ with HNF $A = H$ then

$$\text{HNF} \begin{bmatrix} A & 0 \\ dI_n & I_n \end{bmatrix} = \begin{bmatrix} H & 0 \\ 0 & I_n \end{bmatrix} \quad (d = \det A)$$

Modulo Determinant?

(7) If $UA = H$ with HNF $A = H$ then

$$\text{HNF} \begin{bmatrix} A & 0 \\ dI_n & I_n \end{bmatrix} = \begin{bmatrix} H & 0 \\ 0 & I_n \end{bmatrix} \quad (d = \det A)$$

- Why?
$$\begin{bmatrix} U & 0 \\ -\text{adj}(A) & I_n \end{bmatrix} \begin{bmatrix} A & 0 \\ dI_n & I_n \end{bmatrix} = \begin{bmatrix} H & 0 \\ 0 & I_n \end{bmatrix}$$

Modulo Determinant?

(7) If $UA = H$ with HNF $A = H$ then

$$\text{HNF} \begin{bmatrix} A & 0 \\ dI_n & I_n \end{bmatrix} = \begin{bmatrix} H & 0 \\ 0 & I_n \end{bmatrix} \quad (d = \det A)$$

- Why? $\begin{bmatrix} U & 0 \\ -\text{adj}(A) & I_n \end{bmatrix} \begin{bmatrix} A & 0 \\ dI_n & I_n \end{bmatrix} = \begin{bmatrix} H & 0 \\ 0 & I_n \end{bmatrix}$

- Also : $\begin{bmatrix} U & 0 \\ -\text{adj}(A) & I_n \end{bmatrix} \begin{bmatrix} A \\ dI_n \end{bmatrix} = \begin{bmatrix} H \\ 0 \end{bmatrix}$

- Implies we can compute HNF of $\begin{bmatrix} A \\ dI_n \end{bmatrix}$ working modulo d

Example: Domich et al algorithm

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & \cdots & a_{2n} \\ \vdots & & & & \vdots \\ a_{n1} & a_{n2} & \cdots & \cdots & a_{nn} \\ d & & & & \\ & d & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & d \end{bmatrix}$$

Example: Domich et al algorithm

$$\begin{bmatrix} h_{11} & b_{12} & \cdots & \cdots & b_{1n} \\ & b_{22} & \cdots & \cdots & b_{2n} \\ & \vdots & & & \vdots \\ & b_{n2} & \cdots & \cdots & b_{nn} \\ & * & * & * & * \\ & d & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & d \end{bmatrix}$$

Example: Domich et al algorithm

$$\begin{bmatrix} h_{11} & h_{12} & c_{13} & \cdots & c_{1n} \\ & h_{22} & c_{23} & \cdots & c_{2n} \\ & & \vdots & & \vdots \\ & & c_{n3} & \cdots & c_{nn} \\ & & * & * & * \\ & & * & * & * \\ & & d & & \\ & & & \ddots & \\ & & & & d \end{bmatrix}$$

Example: Domich et al algorithm

$$\begin{bmatrix} h_{11} & h_{12} & h_{13} & \cdots & h_{1n} \\ & h_{22} & h_{23} & \cdots & h_{2n} \\ & & & \ddots & \vdots \\ & & & & h_{nn} \end{bmatrix}$$

More recent history (integer)

Citation	Time complexity	Type
Kannan and Bachem (1979)	$\text{poly}(n, \log \ A\)$	Det
Chou and Collins (1982)	$n^6(\log \ A\)^{1+o(1)}$	Det
Domich et al (1987)	$n^4(\log \ A\)^{1+o(1)}$	Det
Illiopoulos(1989)	"	Det
Hafner and McCurley (1989)	"	Det
Storjohann and Labahn (1996)	$n^{\omega+1}(\log \ A\)^{1+o(1)}$	Det
Storjohann (2000)	"	Det
* Birmipilis, Labahn, Storjohann (2023)	$n^3(\log \ A\)^{1+o(1)}$	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.

Some Oddities

Oddity 1: Faster algorithms for polynomial HNF:

Labahn-Neiger-Zhou (2017)	$O^\sim(n^\omega s)$	Deterministic
---------------------------	----------------------	---------------

- ▶ d bound for the degree of entries in A
- ▶ s minimum of the average of column/row degrees

Oddity 2: Faster algorithms for SNF (with multipliers)

Birmpilis, Labahn, Storjohann (2023)	$O^\sim(n^\omega \log \ A\)$	LV
--------------------------------------	-------------------------------	----

- ▶ Complexity is given without the extra $\log n$ and $\log \log \|A\|$ factors.

Fast Hermite Normal Form (Integer)

Algorithm of BLS. ACM Trans. of Algorithms (2024)

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),
- ▶ $(n^3 \log \|A\|)^{1+o(1)}$ bit operations,
 - variant assumes fast (pseudo-linear) integer multiplication

Algorithm of BLS. ACM Trans. of Algorithms (2024)

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),
- ▶ $(n^3 \log \|A\|)^{1+o(1)}$ 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 .

Approach used in BLS

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

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

Approach used in BLS

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

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

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

Approach used in BLS

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

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

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

Approach used in BLS

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

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

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

4. View as modular equation

- Set $A^* = sA^{-1}$ with $s = s_n$ the largest invariant factor of A .
- Then $HA^{-1} \in \mathbb{Z}^{n \times n}$ same as $HA^* = 0 \pmod{s}$

Approach used in BLS

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

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

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

4. View as modular equation

- Set $A^* = sA^{-1}$ with $s = s_n$ the largest invariant factor of A .
- Then $HA^{-1} \in \mathbb{Z}^{n \times n}$ same as $HA^* = 0 \pmod s$

5. Duality and Howell Form :

- Let $H^* = sH^{-1}$. Then $A^*U^* = H^*$ with U^* unimodular.
- Replace H^* by any upper triang. T having same diag. entries.

Approach used in BLS

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

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

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

4. View as modular equation

- Set $A^* = sA^{-1}$ with $s = s_n$ the largest invariant factor of A .
- Then $HA^{-1} \in \mathbb{Z}^{n \times n}$ same as $HA^* = 0 \pmod s$

5. Duality and Howell Form :

- Let $H^* = sH^{-1}$. Then $A^*U^* = H^*$ with U^* unimodular.
- Replace H^* by any upper triang. T having same diag. entries.
- Column Howell form appropriate choice for T .

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 :

$$\begin{array}{c} A \\ \left[\begin{array}{cccc} -8 & 3 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 4 & -2 & -1 & -1 \\ 4 & -1 & 0 & 0 \end{array} \right] \end{array} \Rightarrow \begin{array}{c} H \\ \left[\begin{array}{cccc} 4 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{array} \right] \end{array} \begin{array}{c} A^{-1} \\ \left[\begin{array}{cccc} 1/8 & 1/16 & -1/16 & 9/16 \\ 1/2 & 1/4 & -1/4 & 5/4 \\ -1/2 & 1/4 & -1/4 & -3/4 \\ 0 & -1/2 & -1/2 & 1/2 \end{array} \right] \end{array} \in \mathbb{Z}^{4 \times 4}.$$

Step 1: Hermite Minimal Denominators

Example :

$$\begin{array}{c} A \\ \left[\begin{array}{cccc} -8 & 3 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 4 & -2 & -1 & -1 \\ 4 & -1 & 0 & 0 \end{array} \right] \end{array} \Rightarrow \begin{array}{c} H \\ \left[\begin{array}{cccc} 4 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{array} \right] \end{array} \begin{array}{c} A^{-1} \\ \left[\begin{array}{cccc} 1/8 & 1/16 & -1/16 & 9/16 \\ 1/2 & 1/4 & -1/4 & 5/4 \\ -1/2 & 1/4 & -1/4 & -3/4 \\ 0 & -1/2 & -1/2 & 1/2 \end{array} \right] \end{array} \in \mathbb{Z}^{4 \times 4}.$$

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

Step 1: Hermite Minimal Denominators

Example :

$$\begin{array}{c} A \\ \left[\begin{array}{cccc} -8 & 3 & -1 & 0 \\ 0 & 1 & 1 & -1 \\ 4 & -2 & -1 & -1 \\ 4 & -1 & 0 & 0 \end{array} \right] \end{array} \Rightarrow \begin{array}{c} H \\ \left[\begin{array}{cccc} 4 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{array} \right] \end{array} \begin{array}{c} A^{-1} \\ \left[\begin{array}{cccc} 1/8 & 1/16 & -1/16 & 9/16 \\ 1/2 & 1/4 & -1/4 & 5/4 \\ -1/2 & 1/4 & -1/4 & -3/4 \\ 0 & -1/2 & -1/2 & 1/2 \end{array} \right] \end{array} \in \mathbb{Z}^{4 \times 4}.$$

- ▶ 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 :

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

- ▶ 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, $\hat{U}AV = S$, \hat{U}, V unimodular).

Step 2: Smith Massager

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

► Write: $AV = WS$ with V, W unimodular

Set $M = V \text{ cmod } S$. Then M is a Smith Massager.

Step 2: Smith Massager

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

▶ Write: $AV = WS$ with V, W unimodular

Set $M = V \text{ cmod } S$. Then M is a Smith Massager.

▶ Notice that $AM = \hat{W}S$

Step 2: Smith Massager

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

▶ Write: $AV = WS$ with V, W unimodular

Set $M = V \text{ cmod } S$. Then M is a Smith Massager.

▶ Notice that $AM = \hat{W}S$

Why is Smith Massager useful for us?

Step 2: Smith Massager

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

▶ Write: $AV = WS$ with V, W unimodular

Set $M = V \text{ cmod } S$. Then M is a Smith Massager.

▶ Notice that $AM = \hat{W}S$

Why is Smith Massager useful for us? $s = s_n$, $A^* = sA^{-1}$, $S^* = sS^{-1}$

▶ $MS^{-1} = A^{-1}\hat{W}$

Step 2: Smith Massager

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

▶ Write: $AV = WS$ with V, W unimodular

Set $M = V \text{ cmod } S$. Then M is a Smith Massager.

▶ Notice that $AM = \hat{W}S$

Why is Smith Massager useful for us? $s = s_n$, $A^* = sA^{-1}$, $S^* = sS^{-1}$

▶ $MS^{-1} = A^{-1}\hat{W}$

So A^{-1} and MS^{-1} have same Hermite minimal denominators

Find H with $HA^* \equiv 0 \pmod{s} \iff HMS^* \equiv 0 \pmod{s}$

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.

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

◇ 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 : $AM \equiv 0 \pmod{S}$ and $\hat{M}M \equiv I \pmod{S}$

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

◇ 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 : Basically $M = V \text{ cmod } S$

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

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

Example

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

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

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}

since $HMS^* \equiv 0 \pmod s \iff HA^* \equiv 0 \pmod s$

Example

Now use **hcol algorithm** of Pauderis-Storjohann

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

Theorem (Pauderis and Storjohann).

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

$$\begin{array}{c} M_4 \\ \left[\begin{array}{c} 9 \\ 4 \\ 4 \\ 8 \end{array} \right] \end{array} /16 \implies \begin{array}{c} H \\ \left[\begin{array}{cccc} 4 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{array} \right] \end{array}$$

Theorem (Pauderis and Storjohann).

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

$$\begin{array}{c} M_4 \\ \left[\begin{array}{c} 9 \\ 4 \\ 4 \\ 8 \end{array} \right] \end{array} /16 \implies \begin{array}{c} H \\ \left[\begin{array}{cccc} 4 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 2 \end{array} \right] \end{array}$$

Check:

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

What about multiple columns?

Lemma

Suppose $B = [B_1 \mid B_2]$. 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 .

What about multiple columns?

Lemma

Suppose $B = [B_1 \mid B_2]$. 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 $S = \text{diag}(s_1, \dots, s_n)$ then:

For $i = 1$ to n do

$\hat{H}_i := \text{hcol}(\text{Column}(M, i), s_i)$

$M := \text{cmod}(\hat{H}_i M, S)$

od

What about multiple columns?

Lemma

Suppose $B = [B_1 \mid B_2]$. 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 $S = \text{diag}(s_1, \dots, s_n)$ then:

For $i = 1$ to n do

$$\hat{H}_i := \text{hcol}(\text{Column}(M, i), s_i)$$

$$M := \text{cmod}(\hat{H}_i M, S)$$

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.

What about multiple columns?

Lemma

Suppose $B = [B_1 \mid B_2]$. 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 $S = \text{diag}(s_1, \dots, s_n)$ then:

For $i = 1$ to n do

$$\hat{H}_i := \text{hcol}(\text{Column}(M, i), s_i)$$

$$M := \text{cmod}(\hat{H}_i M, S)$$

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

$$\begin{array}{c} A \\ \left[\begin{array}{cccc} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{array} \right] \end{array} \quad \text{BLS} \quad \Rightarrow \quad \begin{array}{c} S \\ \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 105 \end{array} \right] \end{array} \quad \text{and} \quad \begin{array}{c} M \\ \left[\begin{array}{cccc} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{array} \right] \end{array}$$

Example : Diagonals of H

$$\begin{array}{c} A \\ \left[\begin{array}{cccc} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{array} \right] \end{array} \quad \text{BLS} \quad \Rightarrow \quad \begin{array}{c} S \\ \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 105 \end{array} \right] \end{array} \quad \text{and} \quad \begin{array}{c} M \\ \left[\begin{array}{cccc} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{array} \right] \end{array}$$

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

Example : Diagonals of H

$$\begin{array}{c} A \\ \left[\begin{array}{cccc} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{array} \right] \end{array} \quad \text{BLS} \quad \Rightarrow \quad \begin{array}{c} S \\ \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 105 \end{array} \right] \end{array} \quad \text{and} \quad \begin{array}{c} M \\ \left[\begin{array}{cccc} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{array} \right] \end{array}$$

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

◇ Therefore $H = \left[\begin{array}{cccc} 1 & h_{12} & h_{13} & h_{14} \\ 0 & 15 & h_{23} & h_{24} \\ 0 & 0 & 15 & h_{34} \\ 0 & 0 & 0 & 21 \end{array} \right]$

Duality

Duality: Continue working with inverses

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

Duality: Continue working with inverses

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

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

Duality: Continue working with inverses

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

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

$$\begin{bmatrix} 1 & & & & & \\ & 1 & & & & \\ & & t_{13} & & & \\ & & t_{23} & & & \\ & & t_{33} & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{bmatrix} \begin{bmatrix} t_{11} & t_{12} & & & & \\ & t_{22} & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{bmatrix} = \begin{bmatrix} t_{11} & t_{12} & t_{13} & & & \\ & t_{22} & t_{23} & & & \\ & & t_{33} & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{bmatrix}$$

Duality: Continue working with inverses

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

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

$$\begin{bmatrix} 1 & & & & & \\ & 1 & & & & \\ & & t_{13} & & & \\ & & t_{23} & & & \\ & & t_{33} & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{bmatrix} \begin{bmatrix} t_{11} & t_{12} & & & & \\ & t_{22} & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{bmatrix} = \begin{bmatrix} t_{11} & t_{12} & t_{13} & & & \\ & t_{22} & t_{23} & & & \\ & & t_{33} & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{bmatrix}$$

Notice: ($s = s_n$)

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

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

Duality: Continue working with inverses

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

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

$$\begin{bmatrix} 1 & & & & & \\ & 1 & & & & \\ & & t_{13} & & & \\ & & t_{23} & & & \\ & & t_{33} & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{bmatrix} \begin{bmatrix} t_{11} & t_{12} & & & & \\ & t_{22} & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{bmatrix} = \begin{bmatrix} t_{11} & t_{12} & t_{13} & & & \\ & t_{22} & t_{23} & & & \\ & & t_{33} & & & \\ & & & 1 & & \\ & & & & 1 & \\ & & & & & 1 \end{bmatrix}$$

Notice: ($s = s_n$)

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

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

◇. we will replace H^* by a different 'column reduced matrix' T

Column Howell Form

Column Howell Form for $B \in \mathbb{Z}/(s)^{n \times n}$. Matrix T where:

- ▶ T right equivalent to B
- ▶ T is upper triangular
- ▶ Normalize diagonal entries (positive and divisors of s)
- ▶ **Howell Property**: for all k : $\text{Span}_k(B) = \text{Span}(T_k)$
(where T_k is the submatrix of T having last k entries 0)

Like a column echelon form for B over $\mathbb{Z}/(s)^{n \times n}$

Example

$$B = \begin{bmatrix} 1 \\ 4 \\ 4 \\ 8 \end{bmatrix} \in \mathbb{Z}/(16)^{4 \times 4}$$

Example

$$B = \begin{bmatrix} 1 \\ 4 \\ 4 \\ 8 \end{bmatrix} \in \mathbb{Z}/(16)^{4 \times 4}$$

Span of columns with last entry 0 contains only the 0 vector

Example

$$B = \begin{bmatrix} & & & 1 \\ & & & 4 \\ & & & 4 \\ & & & 8 \end{bmatrix} \in \mathbb{Z}/(16)^{4 \times 4}$$

Span of columns with last entry 0 contains only the 0 vector

Multiplying last column of B by 2 gives $\begin{bmatrix} 2 \\ 8 \\ 8 \\ 8 \end{bmatrix}$ so B not Howell.

Example

$$B = \begin{bmatrix} 1 \\ 4 \\ 4 \\ 8 \end{bmatrix} \in \mathbb{Z}/(16)^{4 \times 4} \quad \text{Span of columns with last entry 0 contains only the 0 vector}$$

Multiplying last column of B by 2 gives $\begin{bmatrix} 2 \\ 8 \\ 8 \\ 8 \end{bmatrix}$ so B not Howell.

However $BU = T$ where

$$\begin{bmatrix} 1 \\ 4 \\ 4 \\ 8 \end{bmatrix} \begin{bmatrix} 1 & & & \\ & 1 & 13 & \\ & & 1 & 1 \\ 4 & 0 & 6 & 11 \end{bmatrix} = \begin{bmatrix} 4 & 2 & 1 \\ & 8 & 4 \\ & 8 & 4 \\ & & 8 \end{bmatrix} = T$$

with U nonsingular does satisfy the Howell property.

Working in the dual

$$UA = H:$$

Recall:

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

If we let $H^* = sH^{-1}$. Then $A^*U^* = H^*$ with U^* nonsingular

Working in the dual

$$UA = H:$$

Recall:

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

If we let $H^* = sH^{-1}$. Then $A^*U^* = H^*$ with U^* nonsingular

Then

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

Working in the dual

$$UA = H:$$

Recall:

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

If we let $H^* = sH^{-1}$. Then $A^*U^* = H^*$ with U^* nonsingular

Then

- ▶ 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:

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

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

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

Example

Recall:

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

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

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

Example

Recall:

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

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

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

Example

Recall:

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

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

$$\begin{matrix} & H_3 \\ \begin{bmatrix} 1 & 0 & 5 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 15 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} & \text{and} & \begin{matrix} H_3 H_2 H_1 T \\ \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 30 \\ 0 & 0 & 0 & 45 \\ 0 & 0 & 0 & 5 \end{bmatrix} \end{matrix} \end{matrix}$$

Example

Recall:

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

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

$$\begin{matrix} & H_4 \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 15 \\ 0 & 0 & 1 & 12 \\ 0 & 0 & 0 & 21 \end{bmatrix} & \text{and} & \begin{matrix} H_4 H_3 H_2 H_1 T \\ \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{matrix} \end{matrix}$$

Example

Recall:

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

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

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

Computing a Column Howell Form

- ▶ Can just use Howell's algorithm for A^*

Computing a Column Howell Form

- ▶ Can just use Howell's algorithm for A^*
- ▶ But size of A^* and Howell form is $\Omega(n^2 \log s)$ bits.
 - ◊ Better: Use Smith Massager (only $\Omega(n \log \det S)$ bits)

Computing a Column Howell Form

- ▶ Can just use Howell's algorithm for A^*
- ▶ But size of A^* and Howell form is $\Omega(n^2 \log s)$ bits.
 - ◊ Better: Use Smith Massager (only $\Omega(n \log \det S)$ bits)
- ▶ Howell form too big but multiplier okay so
 - ◊ Find \tilde{U} with $T = MS^*\tilde{U} \pmod s$
 - ◊ Basically emulate Howells algorithm but implicitly