Fast Hermite Normal Form Computation

(integer case)

George Labahn and Arne Storjohann

Cheriton School of Computer Science
University of Waterloo

Recent Trends in Computer Algebra, Institut Henri Poincaré,

September 2023

Outline

Cubic Hermite Form

Birmilis, Labahn, Storjohann. ACM Transactions of Algorithms (2023)

Cubic Hermite Form

Birmilis, Labahn, Storjohann. ACM Transactions of Algorithms (2023)

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

Cubic Hermite Form

Birmilis, Labahn, Storjohann. ACM Transactions of Algorithms (2023)

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

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

Approach used in BLS

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. $HB \in \mathbb{Z}^{n \times n}$

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

Approach used in BLS

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. $HB \in \mathbb{Z}^{n \times n}$

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

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

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 $HA^* = 0 \bmod s$

Approach used in BLS

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. $HB \in \mathbb{Z}^{n\times n}$

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 $HA^* = 0 \bmod s$

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

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

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 $HA^* = 0 \bmod s$

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 :

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

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 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, $\hat{U}AV = S$, $\hat{U}, V$ 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 $M = V$ 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 $M = V$ 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 $M = V$ 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 $M = V$ cmod S. Then M is a Smith Massager.

- Notice that $AM = \hat{W}S$

Why is Smith Massager useful for us?

- $MS^{-1} = A^{-1}\hat{W}$

Step 2: Smith Massager

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

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

  Set $M = V$ cmod S. Then M is a Smith Massager.

- Notice that $AM = \hat{W}S$

Why is Smith Massager useful for us?

- $MS^{-1} = A^{-1}\hat{W}$

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

- Let $s = s_n$ and $A^* = sA^{-1}$, $S^* = sS^{-1}$

  Find H with $HA^* \equiv 0 \mod s \iff HMS^* \equiv 0 \mod s$

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.

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

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

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

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

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

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

Example

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

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

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}

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

Example

Now use hcol algorithm of Pauderis-Storjohann

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

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:

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

Our Workhorse: hcol algorithm (ISSAC 2013)

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.*

- This is where eliminations are actually done!
- Works with $\left[\begin{array}{c|c} d & 0 \\ \hline \vec{w} & I_n \end{array}\right]$ and eliminates from outside in
- Obtains Hermite diagonals and then reduces remaining elements

What about multiple columns?

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.

What about multiple columns?

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

What about multiple columns?

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
  $\quad \hat{H}_i := \texttt{hcol}(\mathrm{Column}(M, i), s_i)$
  $\quad M := cmod(\hat{H}_i M, S)$
  od

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

What about multiple columns?

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.

What about multiple columns?

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

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

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

◇ Therefore $H = \begin{bmatrix} 1 & h_{12} & h_{13} & h_{14} \\ 0 & 15 & h_{23} & h_{24} \\ 0 & 0 & 15 & h_{34} \\ 0 & 0 & 0 & 21 \end{bmatrix}$

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.

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

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.

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

Notice: $(s = s_n)$

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

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

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.

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

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: $Span_k(B) = Span(T_k)$

  (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 $\begin{bmatrix} 2 \\ 8 \\ 8 \\ \end{bmatrix}$ so B not Howell.

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 $\begin{bmatrix} 2 \\ 8 \\ 8 \\ \end{bmatrix}$ so B not Howell.

However $BU = T$ where

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

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:

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

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

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

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 $h_1 = 1, h_2 = 15, h_3 = 15, h_4 = 21$.

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

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 $T = MS^*\tilde{U} \mod s$
  - ◇ Basically emulate Howells algorithm
  - ◇ Keep things small: reduce $\tilde{U}$ row modulo S
  - ◇ At iteration j compute $-\frac{h_j}{s}\mathsf{Rem}(MS^*U, s) \in \mathbb{Z}/(h_j)^{n\times 1}$

    $+$ gives offdiagonal entries for column j
  - ◇ Then update T by $M = \mathsf{cmod}(H_j M, S)$

Computing $\tilde{U}$: (simple modification of Howell's algorithm)

To find column j of $H_{j-1}H_{j-2}\cdots H_1T$, need to determine

$$(v_1,\ldots,v_n) = (-h_{1j},\ldots,-h_{j-1,j},1,0,\ldots,0)$$

where

$$\overbrace{\frac{s}{h_j}\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}}^{v} \equiv \overbrace{\begin{bmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{n1} & \cdots & m_{nn} \end{bmatrix}}^{\tilde{M}} \overbrace{\begin{bmatrix} \frac{s}{s_1} & & \\ & \ddots & \\ & & \frac{s}{s_n} \end{bmatrix}}^{S^*} \overbrace{\begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix}}^{u} \bmod s,$$

where $\tilde{M} = \text{cmod}(H_{j-1}H_{j-2}\cdots H_1M, S)$, and u is column j of $\tilde{U}$.

- Note $\tilde{M}$ and u are column and row reduced modulo S, respectively.
- We know the diagonal entries and so scaling factor s/h_j.
- Cost for computing column j depends on $\log||v|| \leq \log h_j$ not $\log s$.

Computing $\tilde{U}$ with $T = MS^*\tilde{U} \mod s$

First diagonal entries of the Howell form are $t_1, \ldots, t_n$, with $t_i = \frac{s}{h_i}$

Computing $\tilde{U}$ with $T = MS^*\tilde{U} \mod s$

First diagonal entries of the Howell form are $t_1, \ldots, t_n$, with $t_i = \frac{s}{h_i}$

Howell's algorithm proceeds in n iterations, starting at $\bar{U} = I_{2n}$.

At the start of iteration i, the matrix $\bar{U}$ has been updated so that

$$\bar{B}\bar{U} = \left[\begin{array}{c|ccc|ccc} & * & \cdots & * & * & * & \cdots & * \\ & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ & t_{n-i}a_1 & \cdots & t_{n-i}a_{n-1} & t_{n-i}a_n & * & \cdots & * \\ \hline & & & & & t_{n-i+1} & \cdots & * \\ & & & & & & \ddots & \vdots \\ & & & & & & & t_n \end{array}\right].$$

Only need the elements $a_1, \ldots, a_n \in \mathbb{Z}/(h_{n-i})$

Updating $\bar{U}$: Part I

There exist $c_1, \ldots, c_{n-1}, c_n \in \mathbb{Z}/(h_{n-i})$, with $gcd(c_n, s) = 1$ satisfying

$$c_1 a_1 + \cdots + c_{n-1} a_{n-1} + c_n a_n = 1 \bmod h_{n-i}.$$

Post multiply by

$$C_i = \begin{bmatrix} I_{n-i} & & & \\ & 1 & & c_1 \\ & & \ddots & \vdots \\ & & 1 & c_{n-1} \\ & & & c_n \\ & & & & I_i \end{bmatrix}$$

gives

$$\begin{bmatrix} & * & \cdots & * & * & * & \cdots & * \\ & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ & t_{n-i}a_1 & \cdots & t_{n-i}a_{n-1} & t_{n-i} & * & \cdots & * \\ & & & & & t_{n-i+1} & \cdots & * \\ & & & & & & \ddots & \vdots \\ & & & & & & & t_n \end{bmatrix}.$$

◇ Can use t_{n-i} to zero out the nonzero entries to the left of t_{n-i}

Updating $\bar{U}$: Part II

Post multiply by

$$W_i = \left[\begin{array}{ccccccc|c} I_{n-i-1} & & & & & & & \\ & 1 & & & & & & \\ \hline & & 1 & & & & & \\ & & & \ddots & & & & \\ & & & & & 1 & & \\ & h_i & -a_1 & \cdots & & -a_{n-1} & 1 & \\ \hline & & & & & & & I_i \end{array}\right]$$

gives

$$\left[\begin{array}{ccccc|ccc} * & * & \cdots & * & * & * & \cdots & * \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ * & * & \cdots & * & * & * & \cdots & * \\ & & & & t_{n-i} & * & \cdots & * \\ \hline & & & & & t_{n-i+1} & \cdots & * \\ & & & & & & \ddots & \vdots \\ & & & & & & & t_n \end{array}\right].$$

◇ Do these triangularizations implicitly as we only really need the a_*.

◇ At step i update $\bar{U} := \bar{U} C_i W_i$.

Summary for Special Howell Algorithm

At iteration i, the Howell transform algorithm has the steps:

1. Compute the entries $\begin{bmatrix} a_1 & \cdots & a_n \end{bmatrix} \in \mathbb{Z}/(h_{n-i})^{1\times n}$
2. Compute the matrices C_i and W_i.
3. Update $\bar{U} := \bar{U}C_iW_i$.

- Cost to construct the the entries $\begin{bmatrix} a_1 & \cdots & a_n \end{bmatrix} \in \mathbb{Z}/(h_{n-i})^{1\times n}$ is $O(n(\log \det S)(\log h_{n-i} + \log\log \det S) + (\log \det S)^2)$
- Cost for building C_i, W_i is $O(n(\log h_{n-i})^2)$
- Computing $\mathsf{rmod}(\bar{U}C_i, S)$ and $\mathsf{rmod}((\bar{U}C_i)W_i, S)$ is $O(n(\log \det S)(\log h_{n-i}))$

Cost to compute U is $O(n(\log \det S)^2 + n^2(\log \det S)(\log\log \det S))$

Future work for integer HNF

Las Vegas algorithm for Integer Hermite form

- faster versions when have fast matrix and integer multiplication
- Can extend for $A \in \mathbb{Z}^{m \times n}$ of full column rank n and $m > n$
- Note Smith Massager only probabilistic part of algorithm

Future work for integer HNF

Las Vegas algorithm for Integer Hermite form

- faster versions when have fast matrix and integer multiplication
- Can extend for $A \in \mathbb{Z}^{m \times n}$ of full column rank n and $m > n$
- Note Smith Massager only probabilistic part of algorithm

Future Work

.

- Deterministic SNF with multipliers.
    - gives a deterministic HNF with multipliers
- Integer Hermite with cost $(n^{\omega} \log ||A||)^{1+o(1)}$ bit operations