

Computing the Smith form with multipliers of a nonsingular integer matrix

George Labahn and Arne Storjohann

Cheriton School of Computer Science
University of Waterloo

Recent Trends in Computer Algebra, Institut Henri Poincaré,
September 2023

Smith normal form

Given

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

Determine

- ▶ 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)

Smith normal form

Given

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

Determine

- ▶ 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)

$$\begin{array}{c} A \\ \left[\begin{array}{cccc} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{array} \right] \end{array} \rightarrow \begin{array}{c} S \\ \left[\begin{array}{cccc} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{array} \right] \end{array}$$

Smith normal form

Given

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

Determine

- ▶ 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)

$$\begin{array}{c} A \\ \left[\begin{array}{cccc} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{array} \right] \end{array} \rightarrow \begin{array}{c} S \\ \left[\begin{array}{cccc} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{array} \right] \end{array}$$

- ▶ S obtained using unimodular row and column operations.

Smith normal form

Additionally, we also want multiplier matrices U and V

- ▶ represents integer row and column operations
- ▶ typically $UAV = S$ or $A = USV$

Smith normal form

Additionally, we also want multiplier matrices U and V

- ▶ represents integer row and column operations
- ▶ typically $UAV = S$ or $A = USV$

$$\begin{array}{c} A \\ \left[\begin{array}{cccc} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{array} \right] \end{array} \rightarrow \begin{array}{c} S \\ \left[\begin{array}{cccc} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{array} \right] \end{array}$$

Smith normal form

Additionally, we also want multiplier matrices U and V

- ▶ represents integer row and column operations
- ▶ typically $UAV = S$ or $A = USV$ or $AV = US$

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

Smith normal form

Additionally, we also want multiplier matrices U and V

- ▶ represents integer row and column operations
- ▶ typically $UAV = S$ or $A = USV$ or $AV = US$
- ▶ We remark that multiplier matrices are not unique

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

Uses?

- ▶ Solving integer linear equations
- ▶ Classifying finite abelian groups:
SNF of generators $\rightarrow \mathbb{Z}_{s_1} \oplus \cdots \oplus \mathbb{Z}_{s_n}$
- ▶ Useful for solving polynomial systems invariant under finite abelian groups via Gröbner bases [Faugère, Svartz, 2013]
- ▶ Rational invariants and rewrite rules for systems invariant under a finite abelian group [Hubert, Labahn, 2016]
- ▶ Outer Adjoint formula [Storjohann; Birmpilis, Labahn, Storjohann]
- ▶ ...

Example

Example

Suppose we want to solve

$$x \begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix} = \begin{bmatrix} 277 & 50 & 290 & -132 \end{bmatrix}.$$

Example

Suppose we want to solve

$$xU \begin{bmatrix} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{bmatrix} = \begin{bmatrix} 277 & 50 & b & -132 \end{bmatrix} V.$$

Example

Suppose we want to solve

$$(xU) \begin{bmatrix} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{bmatrix} = \begin{matrix} (bV) \\ -9106 & 1701 & 6885 & 18795 \end{matrix} .$$

Example

End up with

$$\bar{x} \begin{bmatrix} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{bmatrix}^S = [-9106 \quad 1701 \bar{b} \quad 6885 \quad 18795] .$$

History

- ▶ Form dates back to H.J.S. Smith (1861)
- ▶ Extended Euclidean Algorithm used for elimination.

History

- ▶ Form dates back to H.J.S. Smith (1861)
- ▶ Extended Euclidean Algorithm used for elimination. e.g.:

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

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

History

- ▶ Form dates back to H.J.S. Smith (1861)
- ▶ Extended Euclidean Algorithm used for elimination. e.g.:

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

$$\begin{array}{c} A \\ \left[\begin{array}{cccc} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{array} \right] \end{array} \quad \begin{array}{c} V_1 \\ \left[\begin{array}{cccc} 3 & 10 & 0 & 0 \\ 4 & 13 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right] \end{array} = \begin{array}{c} A_1 \\ \left[\begin{array}{cccc} 1 & 0 & -20 & 27 \\ 201 & 660 & 15 & 30 \\ 60 & 195 & 15 & 6 \\ -63 & -210 & -15 & 9 \end{array} \right] \end{array}$$

History

- ▶ Form dates back to H.J.S. Smith (1861)
- ▶ Extended Euclidean Algorithm used for elimination. e.g.:

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

$$\begin{array}{c} A \\ \left[\begin{array}{cccc} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{array} \right] \end{array} \quad \begin{array}{c} V_4 \\ \left[\begin{array}{cccc} 3 & 10 & 60 & -81 \\ 4 & 13 & 80 & -108 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right] \end{array} = \begin{array}{c} A_4 \\ \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 201 & 660 & 4035 & -5397 \\ 60 & 195 & 1215 & -1614 \\ -63 & -210 & -1275 & 1710 \end{array} \right] \end{array}$$

History

- ▶ Form dates back to H.J.S. Smith (1861)
- ▶ Extended Euclidean Algorithm used for elimination. e.g.:

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

$$\begin{array}{c} A \\ \left[\begin{array}{cccc} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{array} \right] \end{array} \begin{array}{c} V_4 \\ \left[\begin{array}{cccc} 3 & 10 & 60 & -81 \\ 4 & 13 & 80 & -108 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right] \end{array} = \begin{array}{c} A_4 \\ \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 201 & 660 & 4035 & -5397 \\ 60 & 195 & 1215 & -1614 \\ -63 & -210 & -1275 & 1710 \end{array} \right] \end{array}$$

Exponential growth of intermediate integers

Modern History

Citation	Time complexity	U, V	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, 2000)	$n^{\omega+1} \log \ A\ $	✓	Det
Eberly, Giesbrecht and Villard (2000)	$n^{2+\omega/2} \log \ A\ $		MC
Kaltofen and Villard (2004)	$n^{2.695591} \log \ A\ $		MC
Birmpilis, Labahn, Storjohann (2021)	$n^\omega \log \ A\ $	✓	LV

- ▶ ω exponent of matrix multiplication
- ▶ Complexity is given without the extra $\log n$ and $\log \log \|A\|$ factors.
- ▶ Det = deterministic, MC = Monte Carlo or LV = Las Vegas.

Challenges

- ▶ The Smith form is unique but the Smith multipliers are not.
- ▶ Because $s_n \mid \det A$, their size can be large.

Challenges

- ▶ The Smith form is unique but the Smith multipliers are not.
- ▶ Because $s_n \mid \det A$, their size can be large.

Randomization:

- ▶ Our algorithm is of type Las Vegas.
- ▶ Return the correct output with probability at least $1/2$ or fail.

Part 1: Determine first the Smith Form

Part 1: Determine first the Smith Form

Step 1: First determine s_n . Use random linear system solving.

- ▶ For a random vector $b \in \mathbb{Z}^{n \times 1}$,
- ▶ the denominator of $A^{-1}b \in \mathbb{Q}^{n \times 1}$ is likely a large factor of s_n .

Part 1: Determine first the Smith Form

Step 1: First determine s_n . Use random linear system solving.

- ▶ For a random vector $b \in \mathbb{Z}^{n \times 1}$,
- ▶ the denominator of $A^{-1}b \in \mathbb{Q}^{n \times 1}$ is likely a large factor of s_n .

Example

$$\begin{bmatrix} \frac{3}{7} & -\frac{5}{21} & \frac{4}{21} & -\frac{13}{21} \\ \frac{101}{35} & -\frac{12}{7} & \frac{11}{7} & -\frac{419}{105} \\ -\frac{69}{35} & \frac{122}{105} & -\frac{106}{105} & \frac{19}{7} \\ -\frac{16}{7} & \frac{29}{21} & -\frac{26}{21} & \frac{67}{21} \end{bmatrix} \begin{matrix} A^{-1} \\ \\ \\ \end{matrix} \begin{bmatrix} b \\ 5 \\ 5 \\ 3 \\ 2 \end{bmatrix} = \begin{bmatrix} \frac{2}{7} \\ \frac{272}{105} \\ -\frac{173}{105} \\ -\frac{13}{7} \end{bmatrix}$$

Part 1: Determine first the Smith Form

Step 1: First determine s_n . Use random linear system solving.

- ▶ For a random vector $b \in \mathbb{Z}^{n \times 1}$,
- ▶ the denominator of $A^{-1}b \in \mathbb{Q}^{n \times 1}$ is likely a large factor of s_n .

Example

$$\begin{bmatrix} \frac{3}{7} & -\frac{5}{21} & \frac{4}{21} & -\frac{13}{21} \\ \frac{101}{35} & -\frac{12}{7} & \frac{11}{7} & -\frac{419}{105} \\ -\frac{69}{35} & \frac{122}{105} & -\frac{106}{105} & \frac{19}{7} \\ -\frac{16}{7} & \frac{29}{21} & -\frac{26}{21} & \frac{67}{21} \end{bmatrix} \begin{bmatrix} b \\ 7 \\ -3 \\ 6 \\ 3 \end{bmatrix} = \begin{bmatrix} 3 \\ \frac{114}{5} \\ -\frac{76}{5} \\ -18 \end{bmatrix}$$

Part 1: Determine first the Smith Form

Step 1: First determine s_n . Use random linear system solving.

- ▶ For a random vector $b \in \mathbb{Z}^{n \times 1}$,
- ▶ the denominator of $A^{-1}b \in \mathbb{Q}^{n \times 1}$ is likely a large factor of s_n .

Example

$$\begin{bmatrix} \frac{3}{7} & -\frac{5}{21} & \frac{4}{21} & -\frac{13}{21} \\ \frac{101}{35} & -\frac{12}{7} & \frac{11}{7} & -\frac{419}{105} \\ -\frac{69}{35} & \frac{122}{105} & -\frac{106}{105} & \frac{19}{7} \\ -\frac{16}{7} & \frac{29}{21} & -\frac{26}{21} & \frac{67}{21} \end{bmatrix} \begin{matrix} A^{-1} \\ \\ \\ \end{matrix} \begin{bmatrix} 7 \\ -3 \\ 6 \\ 3 \end{bmatrix} \begin{matrix} b \\ \\ \\ \end{matrix} = \begin{bmatrix} 3 & \frac{460}{21} \\ \frac{114}{5} & \frac{395}{21} \\ -\frac{76}{5} & -\frac{193}{7} \\ -18 & -\frac{88}{21} \end{bmatrix}$$

Part 1: Determine first the Smith Form

Step 1: First determine s_n . Use random linear system solving.

- ▶ For a random vector $b \in \mathbb{Z}^{n \times 1}$,
- ▶ the denominator of $A^{-1}b \in \mathbb{Q}^{n \times 1}$ is likely a large factor of s_n .

Example

$$\begin{bmatrix} \frac{3}{7} & -\frac{5}{21} & \frac{4}{21} & -\frac{13}{21} \\ \frac{101}{35} & -\frac{12}{7} & \frac{11}{7} & -\frac{419}{105} \\ -\frac{69}{35} & \frac{122}{105} & -\frac{106}{105} & \frac{19}{7} \\ -\frac{16}{7} & \frac{29}{21} & -\frac{26}{21} & \frac{67}{21} \end{bmatrix} \begin{matrix} A^{-1} \\ \\ \\ \end{matrix} \begin{bmatrix} 7 & 3 \\ -3 & 0 \\ 6 & -1 \\ 3 & -6 \end{bmatrix} \begin{matrix} b \\ \\ \\ \end{matrix} = \begin{bmatrix} 3 & \frac{460}{21} \\ \frac{114}{5} & \frac{395}{21} \\ -\frac{76}{5} & -\frac{193}{7} \\ -18 & -\frac{88}{21} \end{bmatrix}$$

For two vectors, the probability of success is at least $1/2$.

- ▶ “On computing the determinant and Smith form of an integer matrix.” [Eberly, Giesbrecht, Villard (2000)]

Fast linear system solving

Any rational vector $v \in \mathbb{Q}^{n \times 1}$ with denominator $s \in \mathbb{Z}_{>0}$ has an integral $q \in \mathbb{Z}^{n \times 1}$ and a fractional part $r \in (\mathbb{Z}/s)^{n \times 1}$ such that

$$v = q + \frac{1}{s}r.$$

Fast linear system solving

Any rational vector $v \in \mathbb{Q}^{n \times 1}$ with denominator $s \in \mathbb{Z}_{>0}$ has an integral $q \in \mathbb{Z}^{n \times 1}$ and a fractional part $r \in (\mathbb{Z}/s)^{n \times 1}$ such that

$$v = q + \frac{1}{s}r.$$

Example

$$A^{-1}b = \begin{bmatrix} \frac{8779881118476697407}{11711} \\ \frac{3610327141445948005}{23422} \\ \frac{5416863976649117543}{11711} \\ \frac{13839883865944116065}{23422} \end{bmatrix} \quad v$$

Fast linear system solving

Any rational vector $v \in \mathbb{Q}^{n \times 1}$ with denominator $s \in \mathbb{Z}_{>0}$ has an integral $q \in \mathbb{Z}^{n \times 1}$ and a fractional part $r \in (\mathbb{Z}/s)^{n \times 1}$ such that

$$v = q + \frac{1}{s}r.$$

Example

$$A^{-1}b = \begin{bmatrix} q + \frac{r}{s} \\ 749712331865485 + \frac{2572}{11711} \\ 154142564317562 + \frac{10841}{23422} \\ 462544955738119 + \frac{5934}{11711} \\ 590892488512685 + \frac{7995}{23422} \end{bmatrix}$$

Fast linear system solving

Any rational vector $v \in \mathbb{Q}^{n \times 1}$ with denominator $s \in \mathbb{Z}_{>0}$ has an integral $q \in \mathbb{Z}^{n \times 1}$ and a fractional part $r \in (\mathbb{Z}/s)^{n \times 1}$ such that

$$v = q + \frac{1}{s}r.$$

Example

$$A^{-1}b = \left[\begin{array}{c} q + \frac{r}{s} \\ 749712331865485 + \frac{2572}{11711} \\ 154142564317562 + \frac{10841}{23422} \\ 462544955738119 + \frac{5934}{11711} \\ 590892488512685 + \frac{7995}{23422} \end{array} \right]$$

Fast linear system solving

Any rational vector $v \in \mathbb{Q}^{n \times 1}$ with denominator $s \in \mathbb{Z}_{>0}$ has an integral $q \in \mathbb{Z}^{n \times 1}$ and a fractional part $r \in (\mathbb{Z}/s)^{n \times 1}$ such that

$$v = q + \frac{1}{s}r.$$

Example

$$A^{-1}b = \begin{bmatrix} q + \frac{r}{s} \\ 749712331865485 + \frac{2572}{11711} \\ 154142564317562 + \frac{10841}{23422} \\ 462544955738119 + \frac{5934}{11711} \\ 590892488512685 + \frac{7995}{23422} \end{bmatrix}$$

- Cost of computing only r/s
 \sim the bitlength of s .

Fast linear system solving

Any rational vector $v \in \mathbb{Q}^{n \times 1}$ with denominator $s \in \mathbb{Z}_{>0}$ has an integral $q \in \mathbb{Z}^{n \times 1}$ and a fractional part $r \in (\mathbb{Z}/s)^{n \times 1}$ such that

$$v = q + \frac{1}{s}r.$$

Example

$$A^{-1}b = \begin{bmatrix} q + \frac{r}{s} \\ 749712331865485 + \frac{2572}{11711} \\ 154142564317562 + \frac{10841}{23422} \\ 462544955738119 + \frac{5934}{11711} \\ 590892488512685 + \frac{7995}{23422} \end{bmatrix}$$

- ▶ Cost of computing only r/s
 \sim the bitlength of s .

- ▶ Deterministic method for system solving based on high-order lifting [Bimpilis, Labahn, Storjohann (ISSAC, 2019)]
- ▶ Deterministic variant of integrality certification [Bimpilis, Labahn Storjohann (ISSAC, 2020)]

Remaining Invariant Factors

We build up on this idea to recover the r largest invariant factors.

Remaining Invariant Factors

We build up on this idea to recover the r largest invariant factors.

- ▶ Pick a random $R \in (\mathbb{Z}/(s_n))^{n \times r}$.

Remaining Invariant Factors

We build up on this idea to recover the r largest invariant factors.

- ▶ Pick a random $R \in (\mathbb{Z}/(s_n))^{n \times r}$.
- ▶ The Smith form of $s_n A^{-1} R$ over $\mathbb{Z}/(s_n)$ is likely to be

$$\begin{bmatrix} s_n/s_n & & & & \\ & s_n/s_{n-1} & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & s_n/s_{n-r+1} \end{bmatrix} \pmod{s_n}.$$

Remaining Invariant Factors

We build up on this idea to recover the r largest invariant factors.

- ▶ Pick a random $R \in (\mathbb{Z}/(s_n))^{n \times r}$.
- ▶ The Smith form of $s_n A^{-1} R$ over $\mathbb{Z}/(s_n)$ is likely to be

$$\begin{bmatrix} s_n/s_n & & & & \\ & s_n/s_{n-1} & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & s_n/s_{n-r+1} \end{bmatrix} \pmod{s_n}.$$

Problem

If we choose $r := n$, we can recover the Smith form of A , but the cost is too high.

Remaining Invariant Factors

We build up on this idea to recover the r largest invariant factors.

- ▶ Pick a random $R \in (\mathbb{Z}/(s_n))^{n \times r}$.
- ▶ The Smith form of $s_n A^{-1} R$ over $\mathbb{Z}/(s_n)$ is likely to be

$$\begin{bmatrix} s_n/s_n & & & & \\ & s_n/s_{n-1} & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & s_n/s_{n-r+1} \end{bmatrix} \pmod{s_n}.$$

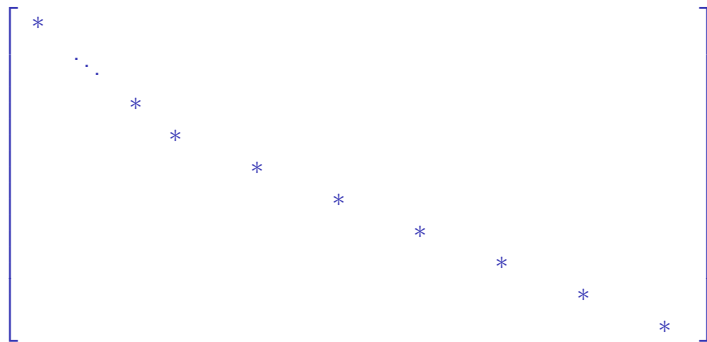
Problem

If we choose $r := n$, we can recover the Smith form of A , but the cost is too high.

- ▶ The length of s_n can be n times the length of entries in A .

Instead we use $\text{dimension} \times \text{precision} \leq \text{invariant}$

Computing the invariant factors of A :



A diagram representing a matrix structure. It consists of a large square bracket on the left and a large square bracket on the right. Inside the brackets, there is a sequence of elements along the main diagonal: an asterisk (*), followed by three dots (.), then another asterisk (*), then a second asterisk (*), then a third asterisk (*), then a fourth asterisk (*), then a fifth asterisk (*), then a sixth asterisk (*), then a seventh asterisk (*), and finally an eighth asterisk (*). The dots are positioned above the second asterisk, indicating a continuation of the diagonal pattern.

Instead we use $\text{dimension} \times \text{precision} \leq \text{invariant}$

Computing the invariant factors of A :

$$\left[\begin{array}{cccccccc|c} * & & & & & & & & \\ & \ddots & & & & & & & \\ & & * & & & & & & \\ & & & * & & & & & \\ & & & & * & & & & \\ & & & & & * & & & \\ & & & & & & * & & \\ & & & & & & & * & \\ & & & & & & & & * \\ \hline & & & & & & & & & s_n \end{array} \right] \text{ mod } s_n$$

Instead we use $\text{dimension} \times \text{precision} \leq \text{invariant}$

Computing the invariant factors of A :

$$\left[\begin{array}{ccc|cc} * & & & & \\ & \ddots & & & \\ & & * & & \\ & & & * & \\ & & & & * \\ & & & & & * \\ \hline & & & & & & s_{n-2} \\ \hline & & & & & & & s_{n-1} \\ \hline & & & & & & & & s_n \end{array} \right] \text{ mod } s_{n-1}$$

Instead we use dimension \times precision \leq invariant

Computing the invariant factors of A :

$$\left[\begin{array}{c|c|c} * & & \\ & \ddots & \\ & & * \\ \hline & s_{n-6} & \\ & & s_{n-5} \\ & & & s_{n-4} \\ & & & & s_{n-3} \\ \hline & & & s_{n-2} & \\ & & & & s_{n-1} \\ & & & & & s_n \end{array} \right] \text{ mod } s_{n-3}$$

Example

$$B_0 := \text{diag}(A, I_n) =$$

$$\begin{bmatrix} -13 & 10 & -20 & 27 & & & & \\ 27 & 30 & 15 & 30 & & & & \\ 0 & 15 & 15 & 6 & & & & \\ -21 & 0 & -15 & 9 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{bmatrix}$$

$$S = \text{diag}(*, *, *, *) \text{ and } \det B_0 = \det A$$

Example

$$B_0 =$$

$$\begin{bmatrix} -13 & 10 & -20 & 27 & & & & \\ 27 & 30 & 15 & 30 & & & & \\ 0 & 15 & 15 & 6 & & & & \\ -21 & 0 & -15 & 9 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & 1 \end{bmatrix}$$

$$S = \text{diag}(*, *, *, 105) \text{ and } \det B_0 = \det A$$

Example

$$B_1 =$$

$$\begin{bmatrix} -13 & 10 & -20 & 27 & & & & 0 \\ 27 & 30 & 15 & 30 & & & & 43 \cdot 105 \\ 0 & 15 & 15 & 6 & & & & 9 \cdot 105 \\ -21 & 0 & -15 & 9 & & & & -15 \cdot 105 \\ & & & & 1 & & & 0 \\ & & & & & 1 & & 0 \\ & & & & & & 1 & 0 \\ 0 & 41 & 17 & 67 & & & & 40 \cdot 105 \end{bmatrix}$$

$$S = \text{diag}(*, *, *, 105) \text{ and } \det B_1 = \det A$$

Example

$$B_1 =$$

$$\begin{bmatrix} -13 & 10 & -20 & 27 & & & & 0 \\ 27 & 30 & 15 & 30 & & & & 43 \\ 0 & 15 & 15 & 6 & & & & 9 \\ -21 & 0 & -15 & 9 & & & & -15 \\ & & & & 1 & & & 0 \\ & & & & & 1 & & 0 \\ & & & & & & 1 & 0 \\ 0 & 41 & 17 & 67 & & & & 40 \end{bmatrix}$$

$$S = \text{diag}(*, *, *, 105) \text{ and } \det B_1 = \det A/105$$

Example

$$B_1 :=$$

$$\begin{bmatrix} -13 & 10 & -20 & 27 & & & & 0 \\ 27 & 30 & 15 & 30 & & & & 43 \\ 0 & 15 & 15 & 6 & & & & 9 \\ -21 & 0 & -15 & 9 & & & & -15 \\ & & & & 1 & & & 0 \\ & & & & & 1 & & 0 \\ & & & & & & 1 & 0 \\ 0 & 41 & 17 & 67 & & & & 40 \end{bmatrix}$$

$$S = \text{diag}(*, *, *, 105) \text{ and } \det B_1 = \det A/105$$

Example

$$B_1 =$$

$$\begin{bmatrix} -13 & 10 & -20 & 27 & & & & 0 \\ 27 & 30 & 15 & 30 & & & & 43 \\ 0 & 15 & 15 & 6 & & & & 9 \\ -21 & 0 & -15 & 9 & & & & -15 \\ & & & & 1 & & & 0 \\ & & & & & 1 & & 0 \\ & & & & & & 1 & 0 \\ 0 & 41 & 17 & 67 & & & & 40 \end{bmatrix}$$

$$S = \text{diag}(*, \mathbf{3}, \mathbf{15}, 105) \text{ and } \det B_1 = \det A / 105$$

Example

$$B_2 =$$

$$\begin{bmatrix} -13 & 10 & -20 & 27 & -2 \cdot 3 & 12 \cdot 15 & 0 \\ 27 & 30 & 15 & 30 & 24 \cdot 3 & 46 \cdot 15 & 43 \\ 0 & 15 & 15 & 6 & 7 \cdot 3 & 16 \cdot 15 & 9 \\ -21 & 0 & -15 & 9 & -9 \cdot 3 & -5 \cdot 15 & -15 \\ & & & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 \cdot 3 & 1 \cdot 15 & 0 \\ 0 & 8 & 0 & 0 & 0 & 7 \cdot 15 & 0 \\ 0 & 41 & 17 & 67 & 28 \cdot 3 & 59 \cdot 15 & 40 \end{bmatrix}$$

$$S = \text{diag}(*, 3, 15, 105) \text{ and } \det B_2 = \det A / 105$$

Example

$$B_2 :=$$

$$\begin{bmatrix} -13 & 10 & -20 & 27 & -2 & 12 & 0 \\ 27 & 30 & 15 & 30 & 24 & 46 & 43 \\ 0 & 15 & 15 & 6 & 7 & 16 & 9 \\ -21 & 0 & -15 & 9 & -9 & -5 & -15 \\ & & & & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 1 & 0 \\ 0 & 8 & 0 & 0 & 0 & 7 & 0 \\ 0 & 41 & 17 & 67 & 28 & 59 & 40 \end{bmatrix}$$

$$S = \text{diag}(*, 3, 15, 105) \text{ and } \det B_2 = \det A / (105 \cdot 15 \cdot 3)$$

Example

$$B_3 :=$$

$$\begin{bmatrix} -13 & 10 & -20 & 27 & 0 & -2 & 12 & 0 \\ 27 & 30 & 15 & 30 & 0 & 24 & 46 & 43 \\ 0 & 15 & 15 & 6 & 0 & 7 & 16 & 9 \\ -21 & 0 & -15 & 9 & 0 & -9 & -5 & -15 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 & 1 & 0 \\ 0 & 8 & 0 & 0 & 0 & 0 & 7 & 0 \\ 0 & 41 & 17 & 67 & 0 & 28 & 59 & 40 \end{bmatrix}$$

$$S = \text{diag}(1, 3, 15, 105) \text{ and } \det B_3 = \det A / (105 \cdot 15 \cdot 3 \cdot 1)$$

Example

$$B_3 :=$$

$$\begin{bmatrix} -13 & 10 & -20 & 27 & 0 & -2 & 12 & 0 \\ 27 & 30 & 15 & 30 & 0 & 24 & 46 & 43 \\ 0 & 15 & 15 & 6 & 0 & 7 & 16 & 9 \\ -21 & 0 & -15 & 9 & 0 & -9 & -5 & -15 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 & 1 & 0 \\ 0 & 8 & 0 & 0 & 0 & 0 & 7 & 0 \\ 0 & 41 & 17 & 67 & 0 & 28 & 59 & 40 \end{bmatrix}$$

$$S = \text{diag}(1, 3, 15, 105) \text{ and } \det B_3 = -1$$

Part 2: What about the multiplier matrices?

Part 2: What about the multiplier matrices?

$$\text{e.g. } \begin{matrix} & & A & & \\ & & & & \\ & & & & \\ & & & & \\ & & & & \end{matrix} \begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix} \text{ with Smith form } \begin{matrix} & & & & S & & \\ & & & & & & \\ & & & & & & \\ & & & & & & \\ & & & & & & \\ & & & & & & \\ & & & & & & \end{matrix} \begin{bmatrix} 1 & & & & & & \\ & 3 & & & & & \\ & & 15 & & & & \\ & & & & & & \\ & & & & & & \\ & & & & & & \\ & & & & & & 105 \end{bmatrix} .$$

Part 2: What about the multiplier matrices?

$$\text{e.g. } \begin{matrix} & A \\ \begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix} & \text{with Smith form} & \begin{matrix} S \\ \begin{bmatrix} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{bmatrix} \end{matrix} \end{matrix}.$$

How do we get the unimodular matrices? That is, U, V such that

$$A \begin{matrix} & V \\ \begin{bmatrix} -26 & 5 & 15 & 55 \\ -62 & 0 & 22 & 137 \\ -20 & 2 & 17 & 41 \\ -53 & 2 & 25 & 115 \end{bmatrix} \end{matrix} = \begin{matrix} & U \\ \begin{bmatrix} -1313 & -17 & 24 & 28 \\ -4452 & 75 & 138 & 92 \\ -1548 & 14 & 49 & 32 \\ 369 & -39 & -23 & -7 \end{bmatrix} \end{matrix} S.$$

Seems to be a harder problem

Consider matrix $A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ with $\gcd(a, b) = 1$.

Suppose $\begin{array}{rcl} au + bv & = & 1 \\ a(-b) + b(a) & = & 0 \end{array}$.

Then $\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} u & b \\ -v & a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ bu - av & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & a^2 + b^2 \end{bmatrix}$

Main tool : Smith Massager (again)

Recall

- ▶ From before **Smith massager** satisfied:

Main tool : Smith Massager (again)

Recall

► From before **Smith massager** satisfied:

a. AMS^{-1} is integral,

b. $(CM + T)S^{-1}$ is integral

Main tool : Smith Massager (again)

Recall

► From before **Smith massager** satisfied:

a. AMS^{-1} is integral,

b. $(CM + T)S^{-1}$ is integral

Rewrite as

a. $AM \equiv 0 \pmod{S}$

b. $(CM + T) \equiv 0 \pmod{S}$

Main tool : Smith Massager (again)

Recall

► From before **Smith massager** satisfied:

a. AMS^{-1} is integral,

b. $(CM + T)S^{-1}$ is integral

Rewrite as

a. $AM \equiv 0 \pmod{S}$

b. $(M'M - I) \equiv 0 \pmod{S}$

Better view of Smith messenger

Better view of Smith massager

Definition

Let $A \in \mathbb{Z}^{n \times n}$ be nonsingular with Smith normal form $S \in \mathbb{Z}^{n \times n}$. A matrix $M \in \mathbb{Z}^{n \times n}$ is a *Smith massager* for A if

- it satisfies that

$$AM \equiv 0 \pmod{S},$$

- there exists a matrix $M' \in \mathbb{Z}^{n \times n}$ such that

$$M'M \equiv I_n \pmod{S}.$$

Better view of Smith massager

Definition

Let $A \in \mathbb{Z}^{n \times n}$ be nonsingular with Smith normal form $S \in \mathbb{Z}^{n \times n}$. A matrix $M \in \mathbb{Z}^{n \times n}$ is a *Smith massager* for A if

- it satisfies that

$$AM \equiv 0 \pmod{S},$$

- there exists a matrix $M' \in \mathbb{Z}^{n \times n}$ such that

$$M'M \equiv I_n \pmod{S}.$$

- A Smith massager can be always reduced column modulo S .

Better view of Smith massager

Definition

Let $A \in \mathbb{Z}^{n \times n}$ be nonsingular with Smith normal form $S \in \mathbb{Z}^{n \times n}$. A matrix $M \in \mathbb{Z}^{n \times n}$ is a *Smith massager* for A if

- it satisfies that

$$AM \equiv 0 \pmod{S},$$

- there exists a matrix $M' \in \mathbb{Z}^{n \times n}$ such that

$$M'M \equiv I_n \pmod{S}.$$

- ▶ A Smith massager can be always reduced column modulo S .
- ▶ The length of the average entry in M is in $(\log \|A\|)^{1+o(1)}$.

Example

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

M looks like a relaxed version of V

For Smith multipliers, we are looking for $V \in \mathbb{Z}^{n \times n}$ that satisfies

- 1a. AVS^{-1} is integral, and
- 1b. V is unimodular, namely, there exists a matrix $V' \in \mathbb{Z}^{n \times n}$ such that $V'V = I_n$.

M looks like a relaxed version of V

For Smith multipliers, we are looking for $V \in \mathbb{Z}^{n \times n}$ that satisfies

- 1a. AVS^{-1} is integral, and
- 1b. V is unimodular, namely, there exists a matrix $V' \in \mathbb{Z}^{n \times n}$ such that $V'V = I_n$.

Smith massager $M \in \mathbb{Z}^{n \times n}$ instead satisfies

- 2a. AMS^{-1} is integral, and
- 2b. there exists a matrix $M' \in \mathbb{Z}^{n \times n}$ such that $M'M = I_n \pmod{S}$.

M looks like a relaxed version of V

For Smith multipliers, we are looking for $V \in \mathbb{Z}^{n \times n}$ that satisfies

- 1a. AVS^{-1} is integral, and
- 1b. V is unimodular, namely, there exists a matrix $V' \in \mathbb{Z}^{n \times n}$ such that $V'V = I_n$.

Smith massager $M \in \mathbb{Z}^{n \times n}$ instead satisfies

- 2a. AMS^{-1} is integral, and
- 2b. there exists a matrix $M' \in \mathbb{Z}^{n \times n}$ such that $M'M = I_n \pmod{S}$.

Question

How do we go from M to V ?

We arrive at V by perturbation

Let $\begin{matrix} & & M & & \\ & & & & \\ & & & & \\ & & & & \\ & & & & \end{matrix} \begin{bmatrix} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{bmatrix}$ be a relaxed version of $\begin{matrix} & & & & V & & \\ & & & & & & \\ & & & & & & \\ & & & & & & \\ & & & & & & \\ & & & & & & \end{matrix} \begin{bmatrix} -26 & 5 & 15 & 55 \\ -62 & 0 & 22 & 137 \\ -20 & 2 & 17 & 41 \\ -53 & 2 & 25 & 115 \end{bmatrix}$.

We arrive at V by perturbation

Let $\begin{bmatrix} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{bmatrix}$ be a relaxed version of $\begin{bmatrix} -26 & 5 & 15 & 55 \\ -62 & 0 & 22 & 137 \\ -20 & 2 & 17 & 41 \\ -53 & 2 & 25 & 115 \end{bmatrix}$.

Because of the addition of $\text{cmod } S$,

- ▶ we might expect V to satisfy $V = M + QS$ for some Q .

This implies that

- ▶ we just need a suitable perturbation for M scaled by S .

We arrive at V by perturbation

Let $\begin{bmatrix} & M & \\ 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{bmatrix}$ be a relaxed version of $\begin{bmatrix} & V & \\ -26 & 5 & 15 & 55 \\ -62 & 0 & 22 & 137 \\ -20 & 2 & 17 & 41 \\ -53 & 2 & 25 & 115 \end{bmatrix}$.

Because of the addition of $\text{cmod } S$,

- ▶ we might expect V to satisfy $V = M + QS$ for some Q .

This implies that

- ▶ we just need a suitable perturbation for M scaled by S .

Idea

A random perturbation should work just fine!

- ▶ “On computing the determinant and Smith form of an integer matrix.” [Eberly, Giesbrecht, Villard (2000)]

Example: Going from M to V

$$\begin{array}{c} M \\ \left[\begin{array}{cccc} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{array} \right] \end{array}$$

Example: Going from M to V

$$\begin{array}{c} M \\ \left[\begin{array}{cccc} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{array} \right] \end{array}$$

- ▶ Perturb M by a random $R \in \mathbb{Z}^{n \times n}$ times Smith form S .

Example: Going from M to V

$$\begin{bmatrix} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{bmatrix}$$

- ▶ Perturb M by a random $R \in \mathbb{Z}^{n \times n}$ times Smith form S .

Example: Going from M to V

$$M + RS \begin{bmatrix} 1 & 5 & 15 & 55 \\ 0 & 0 & 22 & 137 \\ 1 & 2 & 17 & 41 \\ 0 & 2 & 25 & 115 \end{bmatrix}$$

- ▶ Perturb M by a random $R \in \mathbb{Z}^{n \times n}$ times Smith form S .

Example: Going from M to V

$$M + RS \begin{bmatrix} 1 & 5 & 15 & 55 \\ 0 & 0 & 22 & 137 \\ 1 & 2 & 17 & 41 \\ 0 & 2 & 25 & 115 \end{bmatrix}$$

- ▶ Perturb M by a random $R \in \mathbb{Z}^{n \times n}$ times Smith form S .
- ▶ $M + RS$ won't be unimodular. But with high probability,
 - a. it will be nonsingular, and
 - b. it's lower row Hermite form will be trivial.

Example: Going from M to V

$$M + RS \begin{bmatrix} 1 & 5 & 15 & 55 \\ 0 & 0 & 22 & 137 \\ 1 & 2 & 17 & 41 \\ 0 & 2 & 25 & 115 \end{bmatrix}$$

- ▶ Perturb M by a random $R \in \mathbb{Z}^{n \times n}$ times Smith form S .
- ▶ $M + RS$ won't be unimodular. But with high probability,
 - it will be nonsingular, and
 - it's lower row Hermite form will be trivial.
- ▶ Therefore, we can compute it and extract it fast.

Example: Going from M to V

$$\begin{bmatrix} M + RS \\ 1 & 5 & 15 & 55 \\ 0 & 0 & 22 & 137 \\ 1 & 2 & 17 & 41 \\ 0 & 2 & 25 & 115 \end{bmatrix} \cdot \begin{bmatrix} H \\ 3849 & & & \\ 256 & 1 & & \\ 485 & & 1 & \\ 1664 & & & 1 \end{bmatrix}^{-1}$$

- ▶ Perturb M by a random $R \in \mathbb{Z}^{n \times n}$ times Smith form S .
- ▶ $M + RS$ won't be unimodular. But with high probability,
 - it will be nonsingular, and
 - it's lower row Hermite form will be trivial.
- ▶ Therefore, we can compute it and extract it fast.

Example: Going from M to V

$$(M + RS)H^{-1} \\ \begin{bmatrix} -26 & 5 & 15 & 55 \\ -62 & 0 & 22 & 137 \\ -20 & 2 & 17 & 41 \\ -53 & 2 & 25 & 115 \end{bmatrix}$$

- ▶ Perturb M by a random $R \in \mathbb{Z}^{n \times n}$ times Smith form S .
- ▶ $M + RS$ won't be unimodular. But with high probability,
 - it will be nonsingular, and
 - it's lower row Hermite form will be trivial.
- ▶ Therefore, we can compute it and extract it fast.

Example: Going from M to V

$$\begin{bmatrix} -26 & 5 & 15 & 55 \\ -62 & 0 & 22 & 137 \\ -20 & 2 & 17 & 41 \\ -53 & 2 & 25 & 115 \end{bmatrix} \quad V$$

- ▶ Perturb M by a random $R \in \mathbb{Z}^{n \times n}$ times Smith form S .
- ▶ $M + RS$ won't be unimodular. But with high probability,
 - a. it will be nonsingular, and
 - b. it's lower row Hermite form will be trivial.
- ▶ Therefore, we can compute it and extract it fast.

Example: Going from M to V

$$\begin{bmatrix} & V \\ -26 & 5 & 15 & 55 \\ -62 & 0 & 22 & 137 \\ -20 & 2 & 17 & 41 \\ -53 & 2 & 25 & 115 \end{bmatrix} \text{ and } \begin{bmatrix} U = AVS^{-1} \\ -1313 & -17 & 24 & 28 \\ -4452 & 75 & 138 & 92 \\ -1548 & 14 & 49 & 32 \\ 369 & -39 & -23 & -7 \end{bmatrix}$$

- ▶ Perturb M by a random $R \in \mathbb{Z}^{n \times n}$ times Smith form S .
- ▶ $M + RS$ won't be unimodular. But with high probability,
 - a. it will be nonsingular, and
 - b. it's lower row Hermite form will be trivial.
- ▶ Therefore, we can compute it and extract it fast.

Example: Going from M to V

$$\begin{bmatrix} & V \\ -26 & 5 & 15 & 55 \\ -62 & 0 & 22 & 137 \\ -20 & 2 & 17 & 41 \\ -53 & 2 & 25 & 115 \end{bmatrix} \text{ and } \begin{bmatrix} & U = AVS^{-1} \\ -1313 & -17 & 24 & 28 \\ -4452 & 75 & 138 & 92 \\ -1548 & 14 & 49 & 32 \\ 369 & -39 & -23 & -7 \end{bmatrix}$$

- ▶ Perturb M by a random $R \in \mathbb{Z}^{n \times n}$ times Smith form S .
- ▶ $M + RS$ won't be unimodular. But with high probability,
 - a. it will be nonsingular, and
 - b. it's lower row Hermite form will be trivial.
- ▶ Therefore, we can compute it and extract it fast.

We can obtain U, V from S, M in a Las Vegas fashion in time

$$(n^\omega \log \|A\|)^{1+o(1)}.$$

Conclusion

1. A Las Vegas algorithm which computes the Smith form S and a Smith massager M for a nonsingular matrix A in time

$$O(n^\omega B(\log \|A\| + \log n)(\log n)^2).$$

$B(d)$ = cost of integer gcds, $M(d)$ = cost of integer multiplication

Conclusion

1. A Las Vegas algorithm which computes the Smith form S and a Smith massager M for a nonsingular matrix A in time

$$O(n^\omega B(\log \|A\| + \log n)(\log n)^2).$$

2. A Las Vegas algorithm to compute unimodular matrices $U, V \in \mathbb{Z}^{n \times n}$ such that $AV = US$ in extra time

$$O(n^\omega B(\log \|A\| + \log n) \log n).$$

$B(d)$ = cost of integer gcds, $M(d)$ = cost of integer multiplication

Conclusion

1. A Las Vegas algorithm which computes the Smith form S and a Smith massager M for a nonsingular matrix A in time

$$O(n^\omega B(\log \|A\| + \log n)(\log n)^2).$$

2. A Las Vegas algorithm to compute unimodular matrices $U, V \in \mathbb{Z}^{n \times n}$ such that $AV = US$ in extra time

$$O(n^\omega B(\log \|A\| + \log n) \log n).$$

3. Application: we can compute an outer product adjoint formula (\bar{V}, S, \bar{U}) for A (without further randomization) in extra time

$$O(n^\omega M(\log \|A\| + \log n) \log n).$$

$B(d)$ = cost of integer gcds, $M(d)$ = cost of integer multiplication

Further details found in:

Series of papers on fast integer matrix arithmetic:

- ▶ S. Birmpilis, G. Labahn, A. Storjohann, *Deterministic reduction of integer nonsingular linear system solving to matrix multiplication*, Proc. of ISSAC'19, July 15-18, Beijing, China, (2019), 58-65.
- ▶ S. Birmpilis, G. Labahn, A. Storjohann, *A Las Vegas Algorithm for Computing the Smith Form of a Nonsingular Integer Matrix*, Proc. of ISSAC'20, July 21-23, Kalamata, Greece, (2020).
- ▶ S. Birmpilis, G. Labahn, A. Storjohann, *A fast algorithm for computing the Smith normal form with multipliers for a nonsingular integer matrix*. Journal of Symbolic Computation, 116 (2023) 146-182
- ▶ S. Birmpilis, G. Labahn, A. Storjohann, *A softly cubic algorithm for computing the Hermite normal form of a nonsingular integer matrix*. ACM Transactions of Algorithms, (2024)

Part 3: Application

1. *Outer product adjoint formula*

- ▶ Introduced in “On the complexity of inverting integer and polynomial matrices.” [Storjohann, (2015)]
- ▶ We compute it efficiently, with just matrix multiplications.

Part 3: Application

1. *Outer product adjoint formula*

- ▶ Introduced in “On the complexity of inverting integer and polynomial matrices.” [Storjohann, (2015)]
- ▶ We compute it efficiently, with just matrix multiplications.

2. We use our *Smith multipliers* U, V such that

$$AV = US,$$

Outer product adjoint formula

Let

- ▶ a nonsingular integer matrix $A \in \mathbb{Z}^{n \times n}$,
- ▶ with Smith form $S = \text{diag}(s_1, \dots, s_n) \in \mathbb{Z}^{n \times n}$.

Outer product adjoint formula

Let

- ▶ a nonsingular integer matrix $A \in \mathbb{Z}^{n \times n}$,
- ▶ with Smith form $S = \text{diag}(s_1, \dots, s_n) \in \mathbb{Z}^{n \times n}$.

We want to compute

- ▶ an *outer product adjoint formula* (\bar{V}, S, \bar{U}) , that is, matrices $\bar{V}, \bar{U} \in \mathbb{Z}^{n \times n}$ together with the Smith form S such that

$$\begin{bmatrix} * & \cdots & * \\ \vdots & \ddots & \vdots \\ * & \cdots & * \end{bmatrix} \begin{bmatrix} s_n S^{-1} \\ \frac{s_n}{s_1} & & \\ & \ddots & \\ & & \frac{s_n}{s_n} \end{bmatrix} \begin{bmatrix} * & \cdots & * \\ \vdots & \ddots & \vdots \\ * & \cdots & * \end{bmatrix}$$

$$= s_n A^{-1} \pmod{s_n}.$$

Outer product adjoint formula

Let

- ▶ a nonsingular integer matrix $A \in \mathbb{Z}^{n \times n}$,
- ▶ with Smith form $S = \text{diag}(s_1, \dots, s_n) \in \mathbb{Z}^{n \times n}$.

We want to compute

- ▶ an *outer product adjoint formula* (\bar{V}, S, \bar{U}) , that is, matrices $\bar{V}, \bar{U} \in \mathbb{Z}^{n \times n}$ together with the Smith form S such that

$$\begin{bmatrix} * & \cdots & * \\ \vdots & \ddots & \vdots \\ * & \cdots & * \end{bmatrix} \begin{bmatrix} s_n S^{-1} \\ \frac{s_n}{s_1} & & \\ & \ddots & \\ & & \frac{s_n}{s_n} \end{bmatrix} \begin{bmatrix} * & \cdots & * \\ \vdots & \ddots & \vdots \\ * & \cdots & * \end{bmatrix} \\ = s_n A^{-1} \pmod{s_n}.$$

(If $s_n \neq |\det A|$, then the adjoint is just a scalar away.)

Compactness

So,

$$\bar{V} (s_n S^{-1}) \bar{U} = s_n A^{-1} \text{ mod } s_n.$$

Compactness

So,

$$\bar{V} (s_n S^{-1}) \bar{U} = s_n A^{-1} \text{ mod } s_n.$$

Objective

Find such \bar{V}, \bar{U} that use space linear in the size of A .

Compactness

So,

$$\bar{V} (s_n S^{-1}) \bar{U} = s_n A^{-1} \text{ mod } s_n.$$

Objective

Find such \bar{V}, \bar{U} that use space linear in the size of A .

Observation

- ▶ The i^{th} column of \bar{V} and i^{th} row of \bar{U} are scaled by $\frac{s_n}{s_i}$.
- ▶ Those entries can be taken modulo s_i since the whole equation is taken modulo s_n .

Compactness

So,

$$\bar{V} (s_n S^{-1}) \bar{U} = s_n A^{-1} \text{ mod } s_n.$$

Objective

Find such \bar{V}, \bar{U} that use space linear in the size of A .

Observation

- ▶ The i^{th} column of \bar{V} and i^{th} row of \bar{U} are scaled by $\frac{s_n}{s_i}$.
- ▶ Those entries can be taken modulo s_i since the whole equation is taken modulo s_n .

Therefore,

$$(\bar{V} \text{ cmod } S) (s_n S^{-1}) (\bar{U} \text{ rmod } S) = s_n A^{-1} \text{ mod } s_n.$$

Compactness

So,

$$\bar{V} (s_n S^{-1}) \bar{U} = s_n A^{-1} \text{ mod } s_n.$$

Objective

Find such \bar{V}, \bar{U} that use space linear in the size of A .

Observation

- ▶ The i^{th} column of \bar{V} and i^{th} row of \bar{U} are scaled by $\frac{s_n}{s_i}$.
- ▶ Those entries can be taken modulo s_i since the whole equation is taken modulo s_n .

Therefore,

$$(\bar{V} \text{ cmod } S) (s_n S^{-1}) (\bar{U} \text{ rmod } S) = s_n A^{-1} \text{ mod } s_n.$$

Conclusion

We can represent $\text{Rem}(s_n A^{-1}, s_n)$ using $O(n^2(\log \|A\| + \log n))$ bits, where explicitly we would need n times this.

Example

$$\text{Let } \begin{matrix} & A \\ \begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix} & \text{with Smith form} & \begin{matrix} S \\ \begin{bmatrix} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{bmatrix} \end{matrix} \end{matrix} .$$

Example

$$\text{Let } \begin{matrix} & A \\ \begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix} & \text{with Smith form} & \begin{matrix} S \\ \begin{bmatrix} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{bmatrix} \end{matrix} \end{matrix}.$$

Then,

$$\begin{matrix} & \bar{V} \\ \begin{bmatrix} 0 & 2 & 0 & 55 \\ 0 & 0 & 7 & 32 \\ 0 & 2 & 2 & 41 \\ 0 & 2 & 10 & 10 \end{bmatrix} & \begin{matrix} s_n S^{-1} \\ \begin{bmatrix} 105 & & & \\ & 35 & & \\ & & 7 & \\ & & & 1 \end{bmatrix} \end{matrix} & \begin{matrix} \bar{U} \\ \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 12 & 11 & 12 & 1 \\ 60 & 53 & 36 & 51 \end{bmatrix} \end{matrix} \end{matrix}$$

$$= \begin{matrix} & s_n A^{-1} \\ \begin{bmatrix} 45 & -25 & 20 & -65 \\ 303 & -180 & 165 & -419 \\ -207 & 122 & -106 & 285 \\ -240 & 145 & -130 & 335 \end{bmatrix} & \text{mod } 105. \end{matrix}$$

Example

$$\text{Let } \begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix} \text{ with Smith form } \begin{bmatrix} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{bmatrix}.$$

Then,

$$\begin{bmatrix} 2 & 0 & 55 \\ 0 & 7 & 32 \\ 2 & 2 & 41 \\ 2 & 10 & 10 \end{bmatrix} \begin{bmatrix} s_n S^{-1} & \\ & \\ & & \\ & & & 1 \end{bmatrix} \begin{bmatrix} \bar{U} & & & \\ 0 & 0 & 2 & 1 \\ 12 & 11 & 12 & 1 \\ 60 & 53 & 36 & 51 \end{bmatrix}$$

$$= \begin{bmatrix} 45 & -25 & 20 & -65 \\ 303 & -180 & 165 & -419 \\ -207 & 122 & -106 & 285 \\ -240 & 145 & -130 & 335 \end{bmatrix} \pmod{105}.$$

Another example

Let $A = \begin{bmatrix} 2 & 0 & 6 & 9 \\ 3 & 8 & 0 & 1 \\ 1 & 2 & 6 & 0 \\ 0 & 5 & 9 & 7 \end{bmatrix}$ with Smith form $S = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1566 \end{bmatrix}$.

Another example

Let $A = \begin{bmatrix} 2 & 0 & 6 & 9 \\ 3 & 8 & 0 & 1 \\ 1 & 2 & 6 & 0 \\ 0 & 5 & 9 & 7 \end{bmatrix}$ with Smith form $S = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1566 \end{bmatrix}$.

Then,

$$\begin{bmatrix} \bar{V} \\ 0 & 0 & 0 & 834 \\ 0 & 0 & 0 & 363 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 858 \end{bmatrix} \begin{bmatrix} s_n S^{-1} \\ 1566 & & & \\ & 1566 & & \\ & & 1566 & \\ & & & 1 \end{bmatrix} \begin{bmatrix} \bar{U} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1557 & 1493 & 237 & 22 \end{bmatrix}$$

$$= \begin{bmatrix} s_n A^{-1} \\ 324 & 192 & 342 & -444 \\ -135 & 123 & -99 & 156 \\ -9 & -73 & 237 & 22 \\ 108 & 6 & -234 & 84 \end{bmatrix} \pmod{1566}.$$

Another example

$$\text{Let } \begin{matrix} & A \\ \begin{bmatrix} 2 & 0 & 6 & 9 \\ 3 & 8 & 0 & 1 \\ 1 & 2 & 6 & 0 \\ 0 & 5 & 9 & 7 \end{bmatrix} & \text{with Smith form } \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1566 \end{bmatrix}. \end{matrix}$$

Then,

$$\begin{matrix} & \bar{V} \\ \begin{bmatrix} 834 \\ 363 \\ 1 \\ 858 \end{bmatrix} & \begin{bmatrix} 60 & 53 & 36 & 51 \end{bmatrix} \\ & \bar{U} \end{matrix}$$
$$= \begin{bmatrix} 324 & 192 & 342 & -444 \\ -135 & 123 & -99 & 156 \\ -9 & -73 & 237 & 22 \\ 108 & 6 & -234 & 84 \end{bmatrix} \text{mod } 1566.$$

$s_n A^{-1}$

Another example

$$\text{Let } \begin{matrix} & A \\ \begin{bmatrix} 2 & 0 & 6 & 9 \\ 3 & 8 & 0 & 1 \\ 1 & 2 & 6 & 0 \\ 0 & 5 & 9 & 7 \end{bmatrix} & \text{with Smith form } \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1566 \end{bmatrix}. \end{matrix}$$

Then,

$$\text{Rem}_s \left(\begin{matrix} \bar{V} \\ \begin{bmatrix} 834 \\ 363 \\ 1 \\ 858 \end{bmatrix} \\ \bar{U} \\ [60 \quad 53 \quad 36 \quad 51], 1566 \end{matrix} \right)$$

$$= \begin{matrix} s_n A^{-1} \\ \begin{bmatrix} 324 & 192 & 342 & -444 \\ -135 & 123 & -99 & 156 \\ -9 & -73 & 237 & 22 \\ 108 & 6 & -234 & 84 \end{bmatrix} \end{matrix}.$$

Computation

Given

- ▶ the Smith form $S = \text{diag}(s_1, \dots, s_n)$ of A , and
- ▶ unimodular matrices $U, V \in \mathbb{Z}^{n \times n}$ such that

$$AV = US.$$

Computation

Given

- ▶ the Smith form $S = \text{diag}(s_1, \dots, s_n)$ of A , and
- ▶ unimodular matrices $U, V \in \mathbb{Z}^{n \times n}$ such that

$$AV = US.$$

Then, the outer adjoint formula given by (V, S, U^{-1}) since

$$V (s_n S^{-1}) (U^{-1}) = s_n A^{-1} \text{ mod } s_n,$$

Use $((V \mathbf{c} \text{ mod } S), (s_n S^{-1}), (U^{-1} \mathbf{r} \text{ mod } S))$ for a good size.

Computation

Given

- ▶ the Smith form $S = \text{diag}(s_1, \dots, s_n)$ of A , and
- ▶ unimodular matrices $U, V \in \mathbb{Z}^{n \times n}$ such that

$$AV = US.$$

Then, the outer adjoint formula given by (V, S, U^{-1}) since

$$V (s_n S^{-1}) (U^{-1}) = s_n A^{-1} \text{ mod } s_n,$$

Use $((V \mathbf{c} \text{ mod } S), (s_n S^{-1}), (U^{-1} \mathbf{r} \text{ mod } S))$ for a good size.

Finally, we can compute $(U^{-1} \mathbf{r} \text{ mod } S)$ with high-order lifting in (softly) matrix multiplication time

$$O(n^\omega M(\log \|A\| + \log n) \log n).$$