Computing the Smith form of a nonsingular integer matrix

George Labahn

Cheriton School of Computer Science
University of Waterloo

Joint work with Stavros Birmpilis and Arne Storjohann

CIRM: November 11, 2021

My thanks to Claude

Organizing:

- **International Congress on Extrapolation and Rational Interpolation** held on Jan 13-17, 1992 Tenerife, Canary Islands, Spain

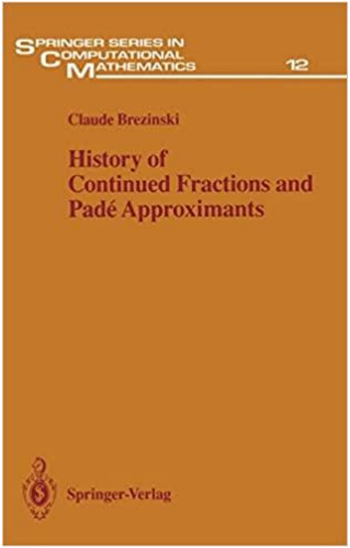
Writing:

- **History of Continued Fractions and Padé Approximants**

Scientific discussion (during coffee breaks)

Additional scientific discussion (during lunch break)

Where I learned about Prony's Method



This Talk: Smith normal form

Given

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

Return

- the Smith normal form $S = \mathrm{diag}(s_1, s_2, \ldots, s_n) \in \mathbb{Z}^{n \times n}$.
- $\{s_i\}$ are the invariant factors of A, positive, with $s_{i-1} | s_i$.

This Talk: Smith normal form

Given

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

Return

- the Smith normal form $S = \mathrm{diag}(s_1, s_2, \ldots, s_n) \in \mathbb{Z}^{n \times n}$.
- $\{s_i\}$ are the invariant factors of A, positive, with $s_{i-1} | s_i$.

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

This Talk: Smith normal form

Given

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

Return

- the Smith normal form $S = \mathrm{diag}(s_1, s_2, \ldots, s_n) \in \mathbb{Z}^{n\times n}$.
- $\{s_i\}$ are the invariant factors of A, positive, with $s_{i-1} | s_i$.

It can be obtained using unimodular row and column operations.

$$\overset{U}{\begin{bmatrix} -1 & 0 & 1 & 0 \\ 255 & 0 & -259 & 1 \\ -4548 & 1436 & 897 & 3346 \\ 26205 & -11497 & 3186 & -26829 \end{bmatrix}} \overset{A}{\begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}} \overset{V}{\begin{bmatrix} 0 & -41968 & -41970 & -36695 \\ -4 & 19731 & 19732 & 17252 \\ 0 & 167 & 167 & 146 \\ -1 & -21004 & -21005 & -18365 \end{bmatrix}}$$

$$= \overset{S}{\begin{bmatrix} 1 & & & \\ & 3 & & \\ & & 15 & \\ & & & 105 \end{bmatrix}} \quad \text{with } \det U = -1 \text{ and } \det V = 1$$

History

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

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

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

History

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

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

$$\overset{A}{\begin{bmatrix} -13 & 10 & -20 & 27 \\ 27 & 30 & 15 & 30 \\ 0 & 15 & 15 & 6 \\ -21 & 0 & -15 & 9 \end{bmatrix}} \overset{V_1}{\begin{bmatrix} 3 & 10 & 0 & 0 \\ 4 & 13 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}} = \overset{A_1}{\begin{bmatrix} 1 & 0 & -20 & 27 \\ 201 & 660 & 15 & 30 \\ 60 & 195 & 15 & 6 \\ -63 & -210 & -15 & 9 \end{bmatrix}}$$

History

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

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

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

History

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

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

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

- Problem: Exponential growth of intermediate integers

Previous work

Citation	Time complexity	Type
Kannan and Bachem (1979)	$poly(n, \log \|\|A\|\|)$	Det
Iliopoulos (1989)	$n^5(\log \|\|A\|\|)^2$	Det
Hafner and McCurley (1991)	$n^5(\log \|\|A\|\|)^2$	Det
Storjohann (ISSAC, 1996)	$n^{\omega+1} \log \|\|A\|\|$	Det
Eberly, Giesbrecht and Villard (2000)	$n^{2+\omega/2} \log \|\|A\|\|$	MC
Kaltofen and Villard (2004)	$n^{2.695594} \log \|\|A\|\|$	MC
Birmpilis, Labahn and Storjohann (ISSAC, 2020)	$n^{\omega} \log \|\|A\|\|$	LV

- Here $\omega \leq 2.3728639$ is exponent of matrix multiplication.
- Complexity is given without the extra $\log n$ and $\log \log ||A||$ factors.
- The type of the algorithms is either deterministic (Det), Monte Carlo (MC) or Las Vegas (LV).

Largest invariant factor s_n

We can use random linear system solving to find s_n.

- 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.

Largest invariant factor s_n

We can use random linear system solving to find s_n.

- 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

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

Largest invariant factor s_n

We can use random linear system solving to find s_n.

- 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

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

Largest invariant factor s_n

We can use random linear system solving to find s_n.

- 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

$$\overbrace{\begin{bmatrix} \frac{3}{7} & -\frac{5}{21} & \frac{4}{21} & -\frac{13}{21} \\ \frac{101}{35} & -\frac{12}{7} & \frac{11}{7} & -\frac{419}{105} \\ -\frac{69}{35} & \frac{122}{105} & -\frac{106}{105} & \frac{19}{7} \\ -\frac{16}{7} & \frac{29}{21} & -\frac{26}{21} & \frac{67}{21} \end{bmatrix}}^{A^{-1}} \overbrace{\begin{bmatrix} 5 & 7 \\ 5 & -3 \\ 3 & 6 \\ 2 & 3 \end{bmatrix}}^{b} = \begin{bmatrix} \frac{2}{7} & 3 \\ \frac{272}{105} & \frac{114}{5} \\ -\frac{173}{105} & -\frac{76}{5} \\ -\frac{13}{7} & -18 \end{bmatrix}$$

Largest invariant factor s_n

We can use random linear system solving to find s_n.

- 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

$$\overbrace{\begin{bmatrix} \frac{3}{7} & -\frac{5}{21} & \frac{4}{21} & -\frac{13}{21} \\ \frac{101}{35} & -\frac{12}{7} & \frac{11}{7} & -\frac{419}{105} \\ -\frac{69}{35} & \frac{122}{105} & -\frac{106}{105} & \frac{19}{7} \\ -\frac{16}{7} & \frac{29}{21} & -\frac{26}{21} & \frac{67}{21} \end{bmatrix}}^{A^{-1}} \overbrace{\begin{bmatrix} 5 & 7 \\ 5 & -3 \\ 3 & 6 \\ 2 & 3 \end{bmatrix}}^{b} = \begin{bmatrix} \frac{2}{7} & 3 \\ \frac{272}{105} & \frac{114}{5} \\ -\frac{173}{105} & -\frac{76}{5} \\ -\frac{13}{7} & -18 \end{bmatrix}$$

Eberly, Giesbrecht, Villard (2000):

- For two "small" random vectors, the probability of success is greater than $1/3$.

Largest invariant factor s_n

We can use random linear system solving to find s_n.

- 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

$$\overset{A^{-1}}{\begin{bmatrix} \frac{3}{7} & -\frac{5}{21} & \frac{4}{21} & -\frac{13}{21} \\ \frac{101}{35} & -\frac{12}{7} & \frac{11}{7} & -\frac{419}{105} \\ -\frac{69}{35} & \frac{122}{105} & -\frac{106}{105} & \frac{19}{7} \\ -\frac{16}{7} & \frac{29}{21} & -\frac{26}{21} & \frac{67}{21} \end{bmatrix}} \overset{b}{\begin{bmatrix} 5 & 7 \\ 5 & -3 \\ 3 & 6 \\ 2 & 3 \end{bmatrix}} = \begin{bmatrix} \frac{2}{7} & 3 \\ \frac{272}{105} & \frac{114}{5} \\ -\frac{173}{105} & -\frac{76}{5} \\ -\frac{13}{7} & -18 \end{bmatrix}$$

Eberly, Giesbrecht, Villard (2000):

- For two “small” random vectors, the probability of success is greater than $1/3$.

But of course this also needs to be fast enough!

Main computational tool: 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

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

Main computational tool: 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

$$A^{-1}b = \overbrace{\begin{bmatrix} \frac{8779881118476697407}{11711} \\ \frac{36103271414445948005}{23422} \\ \frac{5416863976649117543}{11711} \\ \frac{138398838659441160 65}{23422} \end{bmatrix}}^{v}$$

Main computational tool: 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

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

Main computational tool: 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

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

Main computational tool: 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

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

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

Main computational tool: 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

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

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

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

Smith form over a ring

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

Theorem

Pick $J \in \mathbb{Z}/(s)^{n\times(r+k)}$ uniformly at random. Then with probability at least

$$1 - \frac{1}{2^{k-1}}$$

the Smith form of $s_n A^{-1} J$ over $\mathbb{Z}/(s_n)$ is likely to be

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

dimension$\times$precision $\leq$ invariant

Computing the invariant factors of A: (Note: $r = n$ is too slow)

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

dimension × precision ≤ invariant

Computing the invariant factors of A:

$$\left[\begin{array}{cccccccccc|c}
* &&&&&&&&&& \\
& \ddots &&&&&&&&& \\
&& * &&&&&&&& \\
&&& * &&&&&&& \\
&&&& * &&&&&& \\
&&&&& * &&&&& \\
&&&&&& * &&&& \\
&&&&&&& * &&& \\
&&&&&&&& * && \\
\hline
&&&&&&&&&& s_n
\end{array}\right] \bmod s_n$$

dimension × precision ≤ invariant

Computing the invariant factors of A:

$$
\left[\begin{array}{ccccccc|cc|c}
* & & & & & & & & & \\
 & \ddots & & & & & & & & \\
 & & * & & & & & & & \\
 & & & * & & & & & & \\
 & & & & * & & & & & \\
 & & & & & * & & & & \\
 & & & & & & * & & & \\
\hline
 & & & & & & & s_{n-2} & & \\
 & & & & & & & & s_{n-1} & \\
\hline
 & & & & & & & & & s_n
\end{array}\right]
\quad \bmod s_{n-1}
$$

Computing the invariant factors of A:

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

Example

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

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

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

Example

$$B_0 =$$

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

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

Example

$$B_1 =$$

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

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

Example

$$B_1 =$$

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

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

Example

$$B_1 :=$$

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

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

Example

$$B_1 =$$

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

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

Example

$$B_2 =$$

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

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

Example

$$B_2 :=$$

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

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

Example

$$B_3 :=$$

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

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

Example

$$B_3 :=$$

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

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

Construction of a Smith massager

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

Construction of a Smith massager

- Augment A with I_n.

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

Construction of a Smith massager

- Augment A with I_n.

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

Conditioner matrix $\begin{bmatrix} I_n & \\ C & I_n \end{bmatrix}$.

Construction of a Smith massager

- Augment A with I_n.

Massager $\begin{bmatrix} I_n & M \\ & T \end{bmatrix}$.

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

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

Conditioner matrix $\begin{bmatrix} I_n & \\ C & I_n \end{bmatrix}$.

Construction of a Smith massager

- Augment A with I_n.

Massager $\begin{bmatrix} I_n & M \\ & T \end{bmatrix}$.

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

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

Conditioner matrix $\begin{bmatrix} I_n & \\ C & I_n \end{bmatrix}$.

- If the product is unimodular, then S is the Smith form of A.

Conclusions

- Smith form computation in

$$O(n^3(\log n + \log ||A||)^2(\log n)^2)$$

bit operations using standard integer and matrix arithmetic.

- $\tilde{O}(n^\omega \log ||A||)$ using fast integer and matrix multiplication

The algorithm is Las Vegas:

- either the correct Smith form is returned,
- or "fail" with probability $< 1/2$.

Conclusions

- Smith form computation in

$$O(n^3(\log n + \log ||A||)^2(\log n)^2)$$

  bit operations using standard integer and matrix arithmetic.

- $\tilde{O}(n^\omega \log ||A||)$ using fast integer and matrix multiplication

The algorithm is Las Vegas:

- either the correct Smith form is returned,
- or "fail" with probability $< 1/2$.

In addition:

- We use Smith massager to obtain unimodular multiplier matrices $U, V \in \mathbb{Z}^{n\times n}$ such that $AV = US$.

Conclusions

- Smith form computation in

$$O(n^3(\log n + \log ||A||)^2(\log n)^2)$$

  bit operations using standard integer and matrix arithmetic.

- $\tilde{O}(n^\omega \log ||A||)$ using fast integer and matrix multiplication

The algorithm is Las Vegas:

- either the correct Smith form is returned,
- or "fail" with probability $< 1/2$.

In addition:

- We use Smith massager to obtain unimodular multiplier matrices $U, V \in \mathbb{Z}^{n \times n}$ such that $AV = US$.

Finally: Congratulations Claude on your 80^{th} birthday.

Further details found in:

Series of papers on fast integer matrix arithmetic:

- S. Birmpilis, G. L., 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. L., 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. L., A. Storjohann, *A fast algorithm for computing the Smith normal form with multipliers for a nonsingular integer matrix*. Submitted to Journal of Symbolic Computation
- S. Birmpilis, G. L., A. Storjohann, *A softly cubic algorithm for computing the Hermite normal form of a nonsingular integer matrix*. In preparation.