Anders Cornect
acornect@uwaterloo.ca

Centre for Computational Mathematics
University of Waterloo

Structured Preconditioners for Smith Form Computations

Supervised by Prof. Arne Storjohann

MMath Research Project, 2026

Outline

Smith Normal Form

Definition

Let $A \in \mathbf{R}^{n \times n}$ nonsingular. Then there exist (not necessarily unique) unimodular matrices $U, V \in \mathbf{R}^{n \times n}$ such that

$$A = USV, \qquad S = \begin{bmatrix} s_1 & & \\ & \ddots & \\ & & s_n \end{bmatrix}$$

with $s_i \mid s_{i+1}$ for all $1 \leq i < n$. The matrix S is called the *Smith normal form* of A, which we write as $S = \mathrm{SNF}(A)$.

Note that the standard definition has $UAV = S$.

Example

Take the matrix over $\mathbf{R} = \mathbb{Z}$ given by

$$A_{\text{ex1}} = \begin{bmatrix} 18 & 15 \\ 6 & 3 \end{bmatrix}. \text{ Then } \qquad \mathrm{SNF}(A_{\text{ex1}}) = \begin{bmatrix} 3 & \\ & 12 \end{bmatrix}$$

Determinantal Divisors

An important feature of the entries of the Smith normal form:

Remark

For $i = 1, \ldots, n$, the product

$$s_i^* = s_1 s_2 \cdots s_i,$$

called the i^{th} *determinantal divisor* of A, is the GCD of all $i \times i$ minors of A.

Determinantal Divisors

An important feature of the entries of the Smith normal form:

Remark

For $i = 1, \ldots, n$, the product

$$s_i^* = s_1 s_2 \cdots s_i,$$

called the i^{th} *determinantal divisor* of A, is the GCD of all $i \times i$ minors of A.

Example

Take the matrix over $\mathbf{R} = \mathbb{Z}$ given by

$$A_{\text{ex1}} = \begin{bmatrix} 18 & 15 \\ 6 & 3 \end{bmatrix}. \text{ Then } \quad \text{SNF}(A_{\text{ex1}}) = \begin{bmatrix} 3 & \\ & 12 \end{bmatrix}$$

Hermite Normal Form

Definition

For $A \in \mathbf{R}^{n \times n}$ nonsingular, there exists a (unique) unimodular $W \in \mathbf{R}^{n \times n}$ with

$$A = WH, \qquad H = \begin{bmatrix} h_1 & * & \cdots & * \\ & h_2 & \cdots & * \\ & & \ddots & \vdots \\ & & & h_n \end{bmatrix}$$

where the entries above the diagonal entry h_i are reduced modulo h_i.

Hermite Normal Form

Definition

For $A \in \mathbf{R}^{n \times n}$ nonsingular, there exists a (unique) unimodular $W \in \mathbf{R}^{n \times n}$ with

$$A = WH, \qquad H = \begin{bmatrix} h_1 & * & \cdots & * \\ & h_2 & \cdots & * \\ & & \ddots & \vdots \\ & & & h_n \end{bmatrix}$$

where the entries above the diagonal entry h_i are reduced modulo h_i.

Example

Take the matrix over $\mathbf{R} = \mathbb{Z}$ given by

$$A_{\text{ex1}} = \begin{bmatrix} 18 & 15 \\ 6 & 3 \end{bmatrix}. \text{ Then } \qquad \text{HNF}(A_{\text{ex1}}) = \begin{bmatrix} 6 & 3 \\ & 6 \end{bmatrix}.$$

Remark

The product

$$h_i^* = h_1 h_2 \cdots h_i$$

is the GCD of all $i \times i$ minors *contained in the first i columns* of A.

Remark

The product

$$h_i^* = h_1 h_2 \cdots h_i$$

is the GCD of all $i \times i$ minors *contained in the first i columns* of A.

This can be seen in the example from the previous slide.

Example

Take the matrix over $\mathbf{R} = \mathbb{Z}$ given by

$$A_{\text{ex1}} = \begin{bmatrix} 18 & 15 \\ 6 & 3 \end{bmatrix}. \text{ Then } \quad \text{HNF}(A_{\text{ex1}}) = \begin{bmatrix} 6 & 3 \\ & 6 \end{bmatrix}.$$

Triangular Smith Form

The Hermite form is historically easier to compute than the Smith form, requiring only unimodular row operations, which motivated the following definition.

Definition (Villard, 1995)

If a nonsingular matrix $H \in \mathbf{R}^{n \times n}$ in Hermite normal form has $h_i = s_i$ for all $i = 1, \ldots, n$, then H is said to be in *triangular Smith form*.

This means that all of the information about the GCDs of the $i \times i$ minors of A are compressed into the first i columns of A.

Triangular Smith Form

The Hermite form is historically easier to compute than the Smith form, requiring only unimodular row operations, which motivated the following definition.

Definition (Villard, 1995)

If a nonsingular matrix $H \in \mathbf{R}^{n \times n}$ in Hermite normal form has $h_i = s_i$ for all $i = 1, \ldots, n$, then H is said to be in *triangular Smith form*.

This means that all of the information about the GCDs of the $i \times i$ minors of A are compressed into the first i columns of A.

Example

Take the matrix over $\mathbb{Z}$ given by

$$A_{\text{ex2}} = \begin{bmatrix} 33 & 15 \\ 9 & 3 \end{bmatrix}. \text{ Then } \operatorname{HNF}(A_{\text{ex2}}) = \begin{bmatrix} 3 & 9 \\ & 12 \end{bmatrix}, \operatorname{SNF}(A_{\text{ex2}}) = \begin{bmatrix} 3 & \\ & 12 \end{bmatrix}.$$

We have been using an arbitrary PID $\mathbf{R}$, but we are interested mainly in the case where $\mathbf{R} = \mathbf{K}[x]$, with $\mathbf{K}$ a field. The concept of GCDs, and therefore Hermite form and Smith form, extend to polynomials over a field.

We have been using an arbitrary PID $\mathbf{R}$, but we are interested mainly in the case where $\mathbf{R} = \mathbf{K}[x]$, with $\mathbf{K}$ a field. The concept of GCDs, and therefore Hermite form and Smith form, extend to polynomials over a field.

Example

Take the matrix over $\mathbf{R} = \mathbb{Z}_5[x]$ given by

$$A_{\text{ex3}} = \begin{bmatrix} x(x+3) & x(2x+1) \\ x(x+3) & x \end{bmatrix}.$$

Then we have

$$\text{HNF}(A_{\text{ex3}}) = \begin{bmatrix} x^2+3x & x \\ & x^2 \end{bmatrix}, \quad \text{SNF}(A_{\text{ex3}}) = \begin{bmatrix} x & \\ & x^3+3x^2 \end{bmatrix}.$$

Preconditioning for Triangular Smith Form

Preconditioning a matrix to be in triangular Smith form means that calculating the Smith form is reduced to calculating the Hermite form.

Preconditioning for Triangular Smith Form

Preconditioning a matrix to be in triangular Smith form means that calculating the Smith form is reduced to calculating the Hermite form.

Theorem (Kaltofen et al., 1990)

When post-multiplying an input matrix by a random unit lower triangular matrix, the resulting matrix will have the same Smith form, but (with high probability) have its Hermite form be in triangular Smith form.

Preconditioning for Triangular Smith Form

Preconditioning a matrix to be in triangular Smith form means that calculating the Smith form is reduced to calculating the Hermite form.

Theorem (Kaltofen et al., 1990)

When post-multiplying an input matrix by a random unit lower triangular matrix, the resulting matrix will have the same Smith form, but (with high probability) have its Hermite form be in triangular Smith form.

Essentially: We can reduce Smith form to Hermite form by multiplying by a **dense** unit lower triangular matrix.

Example

Recall the matrices A_{ex1} and A_{ex2} from the previous examples, given by

$$A_{\text{ex1}} = \begin{bmatrix} 18 & 15 \\ 6 & 3 \end{bmatrix} \qquad \text{HNF}(A_{\text{ex1}}) = \begin{bmatrix} 6 & 3 \\ & 6 \end{bmatrix}, \quad \text{SNF}(A_{\text{ex1}}) = \begin{bmatrix} 3 & \\ & 12 \end{bmatrix}.$$

$$A_{\text{ex2}} = \begin{bmatrix} 33 & 15 \\ 9 & 3 \end{bmatrix} \qquad \text{HNF}(A_{\text{ex2}}) = \begin{bmatrix} 3 & 9 \\ & 12 \end{bmatrix}, \text{SNF}(A_{\text{ex2}}) = \begin{bmatrix} 3 & \\ & 12 \end{bmatrix}.$$

We can see that

$$A_{\text{ex1}} \cdot \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = A_{\text{ex2}}.$$

So this matrix preconditions A_{ex1} in this way.

We wish to use structured matrices — for example, a *Toeplitz* matrix.

Dense Matrix:

$$\begin{bmatrix} 1 & & & & & & \\ * & 1 & & & & & \\ * & * & 1 & & & & \\ * & * & * & 1 & & & \\ \vdots & \vdots & & \vdots & \ddots & & \\ * & * & \cdots & * & * & 1 & \\ * & * & \cdots & * & * & * & 1 \end{bmatrix}$$

Toeplitz Matrix:

$$\begin{bmatrix} 1 & & & & & & \\ \alpha_1 & 1 & & & & & \\ \alpha_2 & \alpha_1 & 1 & & & & \\ \alpha_3 & \alpha_2 & \alpha_1 & 1 & & & \\ \vdots & \vdots & & \vdots & \ddots & & \\ \alpha_{n-2} & \alpha_{n-3} & \cdots & \alpha_2 & \alpha_1 & 1 & \\ \alpha_{n-1} & \alpha_{n-2} & \cdots & \alpha_3 & \alpha_2 & \alpha_1 & 1 \end{bmatrix}$$

Why?

We wish to use structured matrices — for example, a *Toeplitz* matrix.

Dense Matrix:

$$\begin{bmatrix} 1 & & & & & & \\ * & 1 & & & & & \\ * & * & 1 & & & & \\ * & * & * & 1 & & & \\ \vdots & \vdots & & \vdots & \ddots & & \\ * & * & \cdots & * & * & 1 & \\ * & * & \cdots & * & * & * & 1 \end{bmatrix}$$

Toeplitz Matrix:

$$\begin{bmatrix} 1 & & & & & & \\ \alpha_1 & 1 & & & & & \\ \alpha_2 & \alpha_1 & 1 & & & & \\ \alpha_3 & \alpha_2 & \alpha_1 & 1 & & & \\ \vdots & \vdots & & \vdots & \ddots & & \\ \alpha_{n-2} & \alpha_{n-3} & \cdots & \alpha_2 & \alpha_1 & 1 & \\ \alpha_{n-1} & \alpha_{n-2} & \cdots & \alpha_3 & \alpha_2 & \alpha_1 & 1 \end{bmatrix}$$

Why?

Dense Matrix:

- Must choose $\Theta\left(n^2\right)$ random matrix entries.

Toeplitz Matrix:

- Only requires $\Theta\left(n\right)$ random entries.

We wish to use structured matrices — for example, a *Toeplitz* matrix.

Dense Matrix:

$$\begin{bmatrix} 1 & & & & & & \\ * & 1 & & & & & \\ * & * & 1 & & & & \\ * & * & * & 1 & & & \\ \vdots & \vdots & & \vdots & \ddots & & \\ * & * & \cdots & * & * & 1 & \\ * & * & \cdots & * & * & * & 1 \end{bmatrix}$$

Toeplitz Matrix:

$$\begin{bmatrix} 1 & & & & & & \\ \alpha_1 & 1 & & & & & \\ \alpha_2 & \alpha_1 & 1 & & & & \\ \alpha_3 & \alpha_2 & \alpha_1 & 1 & & & \\ \vdots & \vdots & & \vdots & \ddots & & \\ \alpha_{n-2} & \alpha_{n-3} & \cdots & \alpha_2 & \alpha_1 & 1 & \\ \alpha_{n-1} & \alpha_{n-2} & \cdots & \alpha_3 & \alpha_2 & \alpha_1 & 1 \end{bmatrix}$$

Why?

Dense Matrix:

- Must choose $\Theta\left(n^2\right)$ random matrix entries.
- Matrix-vector multiplication takes $\Theta\left(n^2\right)$ operations.

Toeplitz Matrix:

- Only requires $\Theta\left(n\right)$ random entries.
- Easy $\Theta\left(n \log n \log\log n\right)$ matrix-vector products, good for sparse A.

We wish to use structured matrices — for example, a *Toeplitz* matrix.

Dense Matrix:

$$\begin{bmatrix} 1 & & & & & & \\ * & 1 & & & & & \\ * & * & 1 & & & & \\ * & * & * & 1 & & & \\ \vdots & \vdots & & \vdots & \ddots & & \\ * & * & \cdots & * & * & 1 & \\ * & * & \cdots & * & * & * & 1 \end{bmatrix}$$

Toeplitz Matrix:

$$\begin{bmatrix} 1 & & & & & & \\ \alpha_1 & 1 & & & & & \\ \alpha_2 & \alpha_1 & 1 & & & & \\ \alpha_3 & \alpha_2 & \alpha_1 & 1 & & & \\ \vdots & \vdots & & \vdots & \ddots & & \\ \alpha_{n-2} & \alpha_{n-3} & \cdots & \alpha_2 & \alpha_1 & 1 & \\ \alpha_{n-1} & \alpha_{n-2} & \cdots & \alpha_3 & \alpha_2 & \alpha_1 & 1 \end{bmatrix}$$

Why?

Dense Matrix:

- Must choose $\Theta\left(n^2\right)$ random matrix entries.
- Matrix-vector multiplication takes $\Theta\left(n^2\right)$ operations.

Toeplitz Matrix:

- Only requires $\Theta\left(n\right)$ random entries.
- Easy $\Theta\left(n \log n \log\log n\right)$ matrix-vector products, good for sparse A.
- Existing research conditioning with Toeplitz matrices.

It is known that unit triangular Toeplitz matrices can be used to precondition for **generic rank profile** (all square leading principal submatrices are nonsingular).

It is known that unit triangular Toeplitz matrices can be used to precondition for **generic rank profile** (all square leading principal submatrices are nonsingular).

Theorem (Kaltofen and Saunders, 1991)

When post-multiplying a nonsingular matrix by a random unit lower triangular Toeplitz matrix, the product will (with high probability) have generic rank profile.

Recall: $A = USV$ with S in Smith form, U, V unimodular. We show that for the Hermite form of A to be in triangular Smith form, it suffices to ensure that the Smith multiplier V has generic rank profile.

Recall: $A = USV$ with S in Smith form, U, V unimodular. We show that for the Hermite form of A to be in triangular Smith form, it suffices to ensure that the Smith multiplier V has generic rank profile.

Our first main result is to show that Toeplitz matrices are sufficient preconditioners for triangular Smith form:

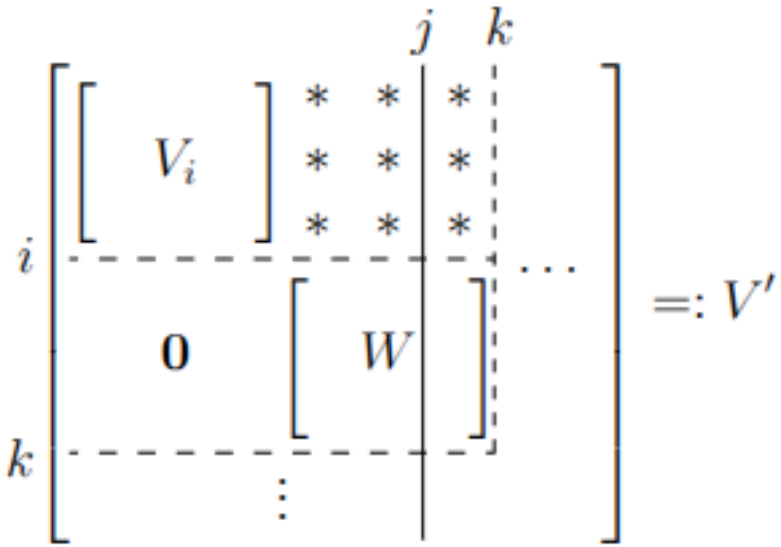
Theorem (Main Result #1)

When post-multiplying an input matrix by a random unit lower triangular **Toeplitz** *matrix, the resulting matrix will have the same Smith form, but have its Hermite form be in triangular Smith form with probability at least*

$$1 - \frac{dn^2(n+1)}{2|S|}.$$

The essence of the proof is as follows.

Firstly, we consider all irreducibles $p \in \mathbf{K}[x]$ that divide $\det A$. For arbitrary p, we find a condition on V that is equivalent to the Hermite form being in triangular Smith form with respect to p.



For this condition to be satisfied for all p, it suffices for V to have generic rank profile over $\mathbf{K}[x]/(p)$ for all p.

Theorem (Main Result #1)

When post-multiplying an input matrix by a random unit lower triangular **Toeplitz** *matrix, the resulting matrix will have the same Smith form, but have its Hermite form be in triangular Smith form with probability at least*

$$1 - \frac{dn^2(n+1)}{2|S|}.$$

If the field $\mathbf{K}$ is too small to produce a sufficiently high probability (consider working over $\mathbb{Z}_2[x]$), we can work over a field extension.

Theorem (Main Result #1)

When post-multiplying an input matrix by a random unit lower triangular **Toeplitz** *matrix, the resulting matrix will have the same Smith form, but have its Hermite form be in triangular Smith form with probability at least*

$$1 - \frac{dn^2(n+1)}{2|S|}.$$

If the field $\mathbf{K}$ is too small to produce a sufficiently high probability (consider working over $\mathbb{Z}_2[x]$), we can work over a field extension.

Thankfully, the Smith and Hermite forms are **canonical forms**, and therefore do not change under field extensions.

The following definition is important for the statement of Main Result #2:

Definition

A nonsingular matrix $A \in \mathbb{R}^{n \times n}$ has *leading Smith determinants* if

$$\gcd(\det A_i, \det A) = s_i^*$$

for all $i = 1, \ldots, n$.

The following definition is important for the statement of Main Result #2:

Definition

A nonsingular matrix $A \in \mathbb{R}^{n \times n}$ has *leading Smith determinants* if

$$\gcd(\det A_i, \det A) = s_i^*$$

for all $i = 1, \ldots, n$.

Matrices with this property are used in, for example, the Smith form algorithm of Storjohann and Labahn, 1997.

The following definition is important for the statement of Main Result #2:

Definition

A nonsingular matrix $A \in \mathbb{R}^{n \times n}$ has *leading Smith determinants* if

$$\gcd(\det A_i, \det A) = s_i^*$$

for all $i = 1, \ldots, n$.

Matrices with this property are used in, for example, the Smith form algorithm of Storjohann and Labahn, 1997.
Recall that $A = WH$ with H in Hermite form W unimodular. We show that, for a matrix to have leading Smith determinants, it suffices that:

- H is in triangular Smith form (see Result #1),
- W has generic rank profile.

Using our other main result, combined with the generic rank profile result by Kaltofen and Saunders, 1991, we can precondition for leading Smith determinants.

Using our other main result, combined with the generic rank profile result by Kaltofen and Saunders, 1991, we can precondition for leading Smith determinants.

Theorem (Main Result #2)

When pre- (and post-) multiplying an input matrix by a random unit upper (respectively lower) triangular **Toeplitz** *matrix, the resulting matrix will have leading Smith determinants with probability at least*

$$1 - \frac{dn^2(n+1)}{|S|}.$$

To conclude:

- Instead of a dense matrix, one can use structured matrix preconditioners to aid in Smith form computation.
- This can be especially useful when the input matrix is sparse.
- It may also be useful in other applications, such as calculating the *Frobenius normal form* of a sparse matrix, which can be done through calculating the Smith form.

Thank You!

References I

[1] Erich Kaltofen, M.S. Krishnamoorthy, and B. David Saunders. "Parallel algorithms for matrix normal forms". In: *Linear Algebra and its Applications* 136 (1990), pp. 189–208. ISSN: 0024-3795. DOI: https://doi.org/10.1016/0024-3795(90)90028-B.

[2] Erich Kaltofen and David Saunders. "On Wiedemann's Method of Solving Sparse Linear Systems.". In: *Lecture Notes in Computer Science*. Vol. 539. Oct. 1991, pp. 29–38. ISBN: 978-3-540-54522-4. DOI: 10.1007/3-540-54522-0_93.

[3] A. Storjohann and G. Labahn. "A Fast Las Vegas Algorithm for Computing the Smith Normal Form of a Polynomial Matrix". In: *Linear Algebra and its Applications* 253 (1997), pp. 155–173.

[4] Gilles Villard. "Generalized Subresultants for Computing the Smith Normal Form of Polynomial Matrices". In: *Journal of Symbolic Computation* 20.3 (1995), pp. 269–286. ISSN: 0747-7171. DOI: https://doi.org/10.1006/jsco.1995.1050.