Structured Preconditioners for Smith Form Computations

by

Anders Cornect

A research project
presented to the University of Waterloo
in fulfillment of the
research requirement for the degree of
Master of Mathematics
in
Computational Mathematics

Waterloo, Ontario, Canada, 2026

Author's Declaration

I hereby declare that I am the sole author of this research project. This is a true copy of the project, including any required final revisions, as accepted by my examiners.

I understand that my project may be made electronically available to the public.

Abstract

We provide two contributions to the problem of preconditioning a nonsingular matrix A over $\mathbf{K}[x]$, with $\mathbf{K}$ a sufficiently large field, for easier Smith form computation. First, we show that post-multiplying A by a random unit lower triangular Toeplitz matrix will, with high probability, put its Hermite form into triangular Smith form. We then show that if one pre- (and post-) multiplies A by a random unit upper (respectively lower) triangular Toeplitz matrix, the resulting matrix will, with high probability, have the following property: For all i from 1 to n, the greatest common divisor of the $i \times i$ leading principal minor of A with $\det A$ is equal to the i^{th} determinantal divisor of A.

Acknowledgements

I would like to thank my loving family, my supportive girlfriend, and my extremely patient supervisor, who all helped to make this project possible.

Dedication

This is dedicated to my beautiful girlfriend, Cassidy.

Table of Contents

Chapter 1

Introduction

1.1 Background and Previous Work

We begin by recalling several definitions.

Definition 1.1. *A* principal ideal domain $\mathbf{R}$ *is an integral domain (a nonzero commutative ring with no zero divisors), such that every ideal* $I \in \mathbf{R}$ *is generated by a single element (i.e., every ideal is principal).*

Some examples of common ideal domains are the ring of integers $\mathbb{Z}$, or the ring of polynomials $\mathbf{K}[x]$ for a field $\mathbf{K}$. We present three important properties of principal ideal domains below without proof, as they are standard results in algebra.

Remark 1.2. *Any principal ideal domain* $\mathbf{R}$ *has the following properties:*

1. *Any two elements* $a, b \in \mathbf{R}$ *have a greatest common divisor.*
2. *An element* $p \in \mathbf{R}$ *being prime is equivalent to it being irreducible.*
3. *Any element* $a \in \mathbf{R}$ *has a unique prime factorization.*

Throughout this work, we will be using $\mathbf{R}$ to denote an arbitrary principal ideal domain, and $\mathbf{K}$ to denote an arbitrary field. We also work primarily with nonsingular matrices, and give definitions that match this case.

We also define the *Smith normal form* of a nonsingular matrix A, which is a classic result in elementary matrix theory. Recall that a matrix is called *unimodular* (over $\mathbf{R}$) if it has an inverse in $\mathbf{R}$. Then we have the following definition for the Smith normal form, adapted from the work of Newman [7] for the case where A is nonsingular.

Definition 1.3 (Newman [7, p. 26])**.** *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*

$$A = USV, \qquad S = \begin{bmatrix} s_1 & & & \\ & s_2 & & \\ & & \ddots & \\ & & & s_n \end{bmatrix}$$

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 $S = \mathrm{SNF}(A)$, and the diagonal entries s_i are called the* invariant factors *of A. For $i = 1, \ldots, n$, the product $s_i^* = s_1 s_2 \cdots s_i$ is called the i^{th}* determinantal divisor *of A.*

The determinantal divisors s_i^* of a matrix are connected to the minors of that matrix in a very important way. The i^{th} determinantal divisor of a matrix A is the greatest common divisor of all $i \times i$ minors of A.

Note that the standard version of the definition of the Smith form has the unimodular matrices U and V — which we call left and right *Smith multipliers* for A, respectively — on the left side of the equation, i.e. $UAV = S$. For our purposes, it is more convenient to have the unimodular matrices on the right; since the inverse of a unimodular matrix is itself unimodular, the definitions are equivalent up to renaming the multipliers.

Example 1.4. *Take the matrix over $\mathbf{R} = \mathbb{Z}$ given by*

$$A_{ex1} = \begin{bmatrix} -9 & -3 & -1 \\ 6 & -9 & -5 \\ 9 & 6 & 4 \end{bmatrix}.$$

Then the Smith form of A_{ex1} and two possible multipliers U and V over $\mathbb{Z}$ are given by

$$U, V = \begin{bmatrix} -1 & 0 & 0 \\ -5 & 25 & 1 \\ 4 & -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 3 & 2 \\ 0 & -13 & -9 \\ 1 & 2 & 9 \end{bmatrix} \qquad S = \begin{bmatrix} 1 & & \\ & 3 & \\ & & 48 \end{bmatrix}.$$

The Smith form is closely related to another matrix normal form, called the *Hermite normal form*; we denote the Hermite normal form of A by $\mathrm{HNF}(A)$. Note that there are multiple equivalent definitions of Hermite form, of which we will be using the upper-triangular row version.

Definition 1.5. *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.

Again we note that the standard definition of the Hermite form typically places the *Hermite multiplier* matrix W on the left-hand side of the equation. The diagonal entries of the Hermite form also have a similar property to those of the Smith form. Given the diagonal entries $h_1, h_2, \ldots, h_n$ of the Hermite form of A, 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.

Example 1.6. *Take the matrix A_{ex1} given in Example 1.4. Then its Hermite form and its multiplier W over $\mathbb{Z}$ are given by*

$$W = \begin{bmatrix} 8 & 2 & 7 \\ 1 & 0 & 1 \\ 13 & 3 & 11 \end{bmatrix}, \qquad H = \begin{bmatrix} 3 & 0 & 10 \\ & 3 & 3 \\ & & 16 \end{bmatrix}.$$

Certain input matrices enjoy the property that its Hermite form has the same diagonal as its Smith form; this is captured by Villard's [11] concept of *triangular Smith form*.

Definition 1.7 (Villard [11, Lemma 2.1])**.** *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.

Example 1.8. *Take the matrix over* $\mathbb{Z}$ *given by*

$$A_{ex2} = \begin{bmatrix} -7 & -4 & -6 \\ -1 & 5 & 0 \\ -2 & 4 & 0 \end{bmatrix}.$$

Then its Hermite and Smith forms are given by

$$H = \begin{bmatrix} 1 & 1 & 0 \\ & 3 & 6 \\ & & 12 \end{bmatrix}, \qquad S = \begin{bmatrix} 1 & & \\ & 3 & \\ & & 12 \end{bmatrix},$$

and so H *is in triangular Smith form.*

There has been much work on the problem of conditioning a matrix A such that $\mathrm{HNF}(A)$ is in triangular Smith form. It reduces the problem of computing the Smith form to computing the Hermite form, which was historically much easier. An early result by Kaltofen, Krishnamoorthy and Saunders would precondition A by multiplying it by a single, randomly chosen, unit lower triangular matrix [3]. Their particular result on preconditioning for triangular Smith form appears within another proof; we present it here as a standalone theorem.

Theorem 1.9 (Kaltofen, Krishnamoorthy, Saunders [3, Proof of Thm 3.3])**.** *For* $A \in \mathbf{K}[x]^{n \times n}$ *of degree* d*, and an* $n \times n$ *unit lower triangular matrix* R *with entries chosen uniformly at random from* $\Lambda \subset \mathbf{K}$*, let* $A' = AR$*. Then*

$$\mathbb{P}\Big[\,\mathrm{HNF}(A') \text{ is in triangular Smith form}\Big] \geq 1 - \frac{2n^3 d}{|\Lambda|}.$$

Later work continues to use the same structure of preconditioner, but computed in differerent ways. For example, the method of Villard in 1995 [11] recovers it entry-by-entry, and Mulders and Storjohann in 1998 [6] compute it column-by-column, both using deterministic methods.

1.2 Our Contributions

Theorem 1.9 is a very useful result, about which we wish to answer the following question: Is it possible to instead use a *structured* preconditioner? Using a unit lower triangular

Toeplitz matrix instead would provide us with several advantages. If A is sparse, matrix-vector products can be calculated quickly. Multiplying A by a dense matrix would cause it to lose that sparsity. However, a unit triangular Toeplitz matrix can be applied to vectors extremely easily — a unit lower triangular Toeplitz matrix-vector product is equivalent to a single truncated polynomial multiplication, as pointed out by Kaltofen and Saunders [5]:

Remark 1.10 (Kaltofen, Saunders; [5, p. 35])**.** *Application of a (unit) upper triangular Toeplitz matrix to a vector can be accomplished by polynomial multiplication, since for*

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_n \end{bmatrix} := \begin{bmatrix} 1 & & & & \\ w_2 & 1 & & & \\ w_3 & w_2 & 1 & & \\ \vdots & & \ddots & \ddots & \\ w_n & w_{n-1} & \cdots & w_2 & 1 \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ v_3 \\ \vdots \\ v_n \end{bmatrix}$$

we have

$$\left(1 + w_2 z + \cdots + w_n z^{n-1}\right)\left(v_1 + v_2 z + v_n z^{n-1}\right) \equiv y_1 + y_2 z + \cdots + y_n z^{n-1} \pmod{z^n}.$$

Therefore instead of multiplying A by a unit lower triangular Toeplitz matrix T explicitly, we can make AT itself into a black box, allowing matrix-vector products to still be calculated quickly. Toeplitz matrices can additionally be stored in a linear amount of space, and their inverses are also very easy to calculate. Preconditioning with a Toeplitz matrix, then, would be quite useful — to this end, our result on preconditioning for triangular Smith form is as follows.

Theorem 2.6. *Given a nonsingular $A \in \mathbf{K}[x]^{n \times n}$ of degree d, let*

$$T_R = \begin{bmatrix} 1 & & & & \\ r_1 & 1 & & & \\ \vdots & \vdots & \ddots & & \\ r_{n-2} & r_{n-3} & \cdots & 1 & \\ r_{n-1} & r_{n-2} & \cdots & r_1 & 1 \end{bmatrix}$$

be a unit lower triangular Toeplitz matrix with $r_1, \ldots, r_{n-1}$ selected uniformly at random

from $\Lambda \subseteq \mathbf{K}$. *If* $\bar{A} = AT_R$, *then*

$$\mathbb{P}\Big[\,\mathrm{HNF}(\bar{A}) \text{ is in triangular Smith form}\Big] \geq 1 - \frac{dn^2(n+1)}{2|\Lambda|}.$$

We then build on Theorem 2.6 to give a secondary result, which allows us to find any of the invariant factors of a matrix using only two determinants and a single GCD operation each. A preliminary definition, and then the aforementioned result, are as follows.

Definition 3.1. *A nonsingular matrix* $A \in \mathbf{R}^{n\times n}$ *has* leading Smith determinants *if*

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

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

Theorem 3.6. *Given a nonsingular* $A \in \mathbf{K}[x]^{n\times n}$ *of degree* d, *let*

$$T_L = \begin{bmatrix} 1 & l_1 & \cdots & l_{n-2} & l_{n-1} \\ & 1 & \cdots & l_{n-3} & l_{n-2} \\ & & \ddots & \vdots & \vdots \\ & & & 1 & l_1 \\ & & & & 1 \end{bmatrix}, \quad T_R = \begin{bmatrix} 1 & & & & \\ r_1 & 1 & & & \\ \vdots & \vdots & \ddots & & \\ r_{n-2} & r_{n-3} & \cdots & 1 & \\ r_{n-1} & r_{n-2} & \cdots & r_1 & 1 \end{bmatrix}$$

be unit upper (respectively, lower) triangular Toeplitz matrices with $l_1, \ldots, l_{n-1}$ *and* $r_1, \ldots, r_{n-1}$ *selected uniformly at random from* $\Lambda \subseteq \mathbf{K}$. *If* $\tilde{A} = T_L A T_R$, *then*

$$\mathbb{P}\Big[\tilde{A} \text{ has leading Smith determinants}\Big] \geq 1 - \frac{dn^2(n+1)}{|\Lambda|}.$$

The Hermite and Smith forms are canonical forms, and are therefore unaffected by field extensions. Consequently, if $\mathbf{K}$ is too small to attain a sufficiently high probability, we can work over an algebraic field extension. In the usual case where we are working over $\mathbf{R} = \mathbf{K}[x]$, the complexity added to operations over $\mathbf{K}[x]$ only grows logarithmically.

1.3 Example Application

Quickly calculating the Smith form is of use in many other applications; one example involves the *Frobenius normal form* of a matrix. To define this, we first need to understand

the concept of a *companion matrix*.

Definition 1.11. *For a monic polynomial* $f \in \mathbf{K}[x]^{n\times n}$ *with*

$$f = x^d + c_{d-1}x^{d-1} + \cdots + c_1 x + c_0,$$

its companion matrix $C_f \in \mathbf{K}^{n\times n}$ *is the matrix given by*

$$C_f = \begin{bmatrix} & & & -c_0 \\ 1 & & & -c_1 \\ & 1 & & -c_2 \\ & & \ddots & \vdots \\ & & 1 & -c_{n-1} \end{bmatrix}.$$

The Frobenius normal form is a matrix built off of these companion matrices, which is again closely related to the Smith form. It is defined as follows — note that it is defined for matrices over a *field*, not a principal ideal domain.

Definition 1.12. *For* $A \in \mathbb{K}^{n\times n}$*, there exists an invertible matrix* $V \in \mathbf{K}^{n\times n}$ *such that*

$$A = VFV^{-1}, \qquad F = \begin{bmatrix} C_{f_1} & & & \\ & C_{f_2} & & \\ & & \ddots & \\ & & & C_{f_k} \end{bmatrix},$$

where each C_{f_i} *is the companion matrix of a monic polynomial* f_i *over* $\mathbf{K}$*, and for all* $1 \le i < k$*,* $f_{i+1} \mid f_i$*. The matrix* F *is called the* Frobenius normal form *of* A*.*

The polynomials $f_1, \ldots, f_k$ in Definition 1.12 are the invariant factors of the matrix $xI - A \in \mathbf{K}[x]^{n\times n}$ [10]. This means, then, that the Frobenius form of a matrix A can be found via calculating the Smith form of the matrix $xI - A$. Therefore, by working towards improving Smith form algorithms, we are working towards a fast algorithm for the Frobenius form for the case of sparse A.

Chapter 2

Preconditioning for Triangular Smith Form

The main result of this chapter is that, to precondition a matrix such that its Hermite form is in triangular Smith form (with some probability), it suffices to post-multiply it by a single unit lower triangular Toeplitz matrix. For a nonsingular matrix A over $\mathbf{K}[x]$, where $\mathbf{K}$ is an arbitrary field, we reduce proving our main result to proving an easier condition in two ways. Firstly, we find a condition that is equivalent to A having a Hermite form that is also in triangular Smith form. Secondly, we reduce this equivalent condition to a simpler condition on primes p that divide $\det A$. This equivalent condition allows us to apply known preconditioners that work over a field to solve our problem.

The rest of this chapter is structured as follows. Section 2.1 serves to prove Theorem 2.3; this is the equivalence described above, which allows us to reduce the problem of preconditioning for triangular Smith form to preconditioning for generic rank profile. In Section 2.2, we use that equivalence to show that we can precondition a matrix for triangular Smith form using a Toeplitz matrix (as well as proving a lower bound on its probability of success) via Theorem 2.6. Note that in Section 2.1 we work over an arbitrary principal domain $\mathbf{R}$ so that our results are as general as possible. In Section 2.2, we specialize to the case $\mathbf{R} = \mathbf{K}[x]$ for an arbitrary field $\mathbf{K}$.

2.1 Reduction to Submatrix Rank Condition

We begin with some lemmas. Recall that the *row rank profile* of a matrix V is the lexicographically smallest set of indices, such that those rows of V are linearly independent.

We also use the notation $V_{i\times j}$ for the $i \times j$ leading principal submatrix of V, or simply V_i if $i = j$.

Lemma 2.1. *Let $V \in \mathbf{K}^{m\times n}$ be a matrix, and let V' be the matrix that results from adding some number of rows of V to* later *rows of V. Then V and V' have the same row rank profile.*

Proof. It suffices to show that, for arbitrary indices i, j with $1 \le i < j \le m$ and $c \in \mathbb{Z}$, adding c times row i to row j does not change whether row j is linearly independent from the lexicographically smallest set of linearly independent rows before it, i.e., the rank profile of the rows 1 to $j - 1$.

Suppose V' is equal to V, but with row r_j replaced by $r_j + cr_i$, and suppose

$$\mathcal{I} = \{i_1, i_2, \ldots, i_\ell\} \subset \{1, 2, \ldots, j-1\}$$

is the row rank profile of the rows $\{r_1, r_2, \ldots, r_{j-1}\}$.

If $\mathcal{I} \cup \{r_j\}$ was linearly independent, we have two cases. If $r_i \in \mathcal{I}$, then $\mathcal{I} \cup \{r_j + cr_i\}$ is automatically still linearly independent. Otherwise, suppose $r_i \notin \mathcal{I}$. Then it must be that $r_i \in \operatorname{span}\mathcal{I}$. Therefore if $\mathcal{I} \cup \{r_j + cr_i\}$ was linearly dependent, we would have $r_j + cr_i - cr_i = r_j \in \operatorname{span}\mathcal{I}$, a contradiction, and $\mathcal{I} \cup \{r_j\}$ is still linearly independent.

Otherwise if $S \cup \{r_j\}$ was linearly dependent, we have the same cases. In either case, however, we have $r_i \in \operatorname{span} S$. Then since $r_j \in \operatorname{span} S$, $r_j + cr_i \in \operatorname{span} S$ as well, so $S \cup \{r_j + cr_i\}$ is still linearly dependent and the desired result follows. □

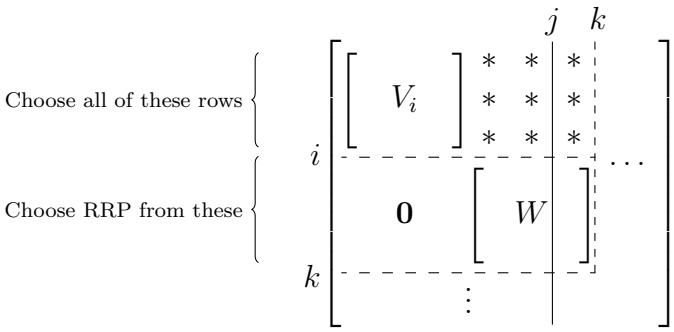
Lemma 2.2. *Let $V \in \mathbf{K}^{n\times n}$ be a matrix, and let $i, j, k \in \mathbb{Z}$ satisfy $0 \le i < j < k \le n$. If V_i and V_k are nonsingular over $\mathbf{K}$, then the row rank profile of $V_{n\times j}$ is given by*

$$\{1, 2, \ldots, i\} \cup S$$

where $S \subset \{i + 1, i + 2, \ldots, k\}$ is a subset of size $j - i$.

Proof. Since V_i has full rank modulo p, we can add linear combinations of the first i rows of V to the later $k - i$ rows, such that all of the entries of those later rows in the first i columns are 0. This leaves a $(k-i)\times(k-i)$ matrix to the right of these zeroed-out entries,

which we will call W. The result is a matrix that looks like Matrix 2.1, which we call V'.



(2.1)

Since V_i is nonsingular over $\mathbf{K}$, all of the first i rows of $V'_{n\times j}$ are included in its row rank profile. Now, since V_k has full rank, so does W. Therefore the first $j-i$ columns of W also have full rank, i.e., rank $j-i$. It follows that there exists a nonzero $(j-i)\times(j-i)$ minor in the first $j-i$ columns of W. Of these minors, choose the one with the lexicographically smallest set of row indices.

The first i rows of $V'_{n\times j}$, along with the subset of the next $j-i$ rows described above, form a linearly independent set, since V_k has full rank and we only performed row operations *within* that submatrix. Since we chose the lexicographically smallest row index at every point, this is actually the row rank profile of $V'_{n\times j}$. By Lemma 2.1, it is also the row rank profile of $V_{n\times j}$. □

Using these lemmas, we provide a necessary and sufficient condition on our unimodular Smith multiplier matrix V, for HNF(A) to be in triangular Smith form. As mentioned, we present the result as a condition for a prime p to have the correct order in the diagonal entries of HNF(A). The result follows from applying this condition for all primes $p \mid \det A$.

To this end, for $p \in \mathbf{R}$ a prime, we focus only on the order of p in the diagonal entries of HNF(A) and SNF(A). This then gives us the following theorem, where the first condition can be thought of as HNF(A) being in triangular Smith form, with respect to the prime p.

Theorem 2.3. *Let $A \in \mathbf{R}^{n\times n}$ nonsingular with $H = \mathrm{HNF}(A)$, $S = \mathrm{SNF}(A)$, and unimodular matrices U and V such that $A = USV$. For any prime $p \in \mathbf{R}$, the following are equivalent.*

1. *The order of p in each diagonal entry of H is the same as the order of p in the corresponding diagonal entry of S.*
2. *For each $1 \le i < n$ such that the order of p in $S_{i,i} \neq$ the order of p in $S_{i+1,i+1}$, V_i has full rank modulo p.*

Proof. Let H^p and S^p be the matrices consisting of the highest powers of p dividing the corresponding entries in H and S, respectively. In the following proof, let $h_i := H^p_{i,i}$ and $h_i^* = \prod_{j=1}^{i} h_i$, similarly for s_i and s_i^*. Write $s_1 = p^{\alpha_1} \le s_2 = p^{\alpha_2} \le \cdots \le s_n = p^{\alpha_n}$.

Firstly, we simplify the proof by noting the following. Write $U^{-1}A = SV$. Since HNF is invariant under left-multiplication by unimodular matrices, $\mathrm{HNF}(U^{-1}A) = \mathrm{HNF}(A)$. Since the conditions of the theorem are only on V and $\mathrm{HNF}(A)$, we can treat $U^{-1}A$ as our matrix A. In other words, assume without loss of generality that $U = I$, and so $A = SV$.

$1 \Rightarrow 2$: We proceed by proving the contrapositive. Suppose there exists an i such that $\alpha_i \neq \alpha_{i+1}$, but V_i is rank deficient mod p. It suffices to show that $h_i^* \neq s_i^*$, i.e., all principal $i \times i$ submatrices contained in $A_{n\times i}$ have determinant divisible by some power of p greater than $p^{\alpha_1+\alpha_2+\cdots+\alpha_i}$.

By assumption, $\det V_i = pD$ for some $D \in \mathbf{R}$ (with D possibly equal to 0). Therefore the determinant of $A_i = (SV)_i$ is

$$p^{\alpha_1}p^{\alpha_2}\cdots p^{\alpha_i} \cdot pD = p^{\alpha_1+\cdots+\alpha_i+1}D,$$

which satisfies the desired condition. Any other submatrix formed using the rows r_1, r_2, $\ldots$, r_i must have at least one row with index greater than i; label them such that $r_1 \ge 1$, $\ldots$, $r_{i-1} \ge i-1$, $r_i > i$. If the determinant of this submatrix of V is D', then the determinant of the corresponding submatrix of $A = SV$ is

$$p^{\alpha_{r_1}}p^{\alpha_{r_2}}\cdots p^{\alpha_{r_i}}D' = p^{\alpha_{r_1}+\alpha_{r_2}+\cdots+\alpha_{r_i}}D'.$$

Note that because of our choice of i, $r_i > i$ means that $\alpha_{r_i} > \alpha_i$. Then since $\alpha_{r_1}+\cdots+\alpha_{r_i} > \alpha_1+\cdots+\alpha_i$, this determinant also satisfies the desired condition, and the implication follows.

$2 \Rightarrow 1$: Suppose V satisfies condition 2. If there is no such i with $\alpha_i \neq \alpha_{i+1}$, then the Smith form of A has only a single unique entry, i.e. $S = sI$ for some $s \in \mathbf{R}$. Then $A = SV = sV$, meaning the Hermite form of A is just $sI = S$, and condition 1 is satisfied.

Otherwise, consider every index i such that $\alpha_i \neq \alpha_{i+1}$; label them $\delta_1 < \delta_2 < \cdots < \delta_m$. For every $j = 1, 2, \ldots, n$, we know that $S^p_{j,j} \mid H^p_{j,j}$. Therefore we wish to show that for each j, we can find a $j \times j$ principal submatrix in $(SV)_{n \times j}$ whose determinant has the same order of p as $S^p_{j,j}$. Since $A = SV$, it follows that $H^p_{j,j} \mid S^p_{j,j}$ for all j, and so $H^p_{j,j} = S^p_{j,j}$, as desired.

Suppose $j \in \{\delta_1, \delta_2, \ldots, \delta_m, n\}$. Then

$$\det (SV)_j = s_1 \cdots s_j \det V_j = s_J^* \cdot \det V_j$$

and since $\det V_j$ is nonzero mod p, this matrix satisfies the desired condition.

Suppose instead that $j \notin \{\delta_1, \delta_2, \delta_m, n\}$. For convenience, label $\delta_0 = 0$ and $\delta_{m+1} = n$. Then we see that $\delta_{l-1} < j < \delta_l$ for some $0 < l \leq m + 1$. We want to show that, in fact, the minor that corresponds to the row rank profile of the first j columns of SV actually satisfies the desired property. By Lemma 2.2, the RRP of this matrix over $\mathbf{R}/(p)$ consists of the first δ_{l-1} rows of $V_{n \times j}$, plus a set of size $j - \delta_{l-1}$ selected from rows from $\delta_{l-1} + 1$ to δ_l.

Denote by Δ the determinant of the submatrix corresponding to the RRP of $V_{j \times n}$, with $\gcd(\Delta, p) = 1$. Because of the way the rows of this RRP were selected, combined with the fact that $\alpha_{\delta_{l-1}+1} = \cdots = \alpha_j = \cdots = \alpha_{\delta_l}$, the determinant of the corresponding submatrix of $A = SV$ is

$$\begin{aligned} s_1 \cdots s_{\delta_{l-1}} s_{\delta_{l-1}+1} \cdots s_j \Delta &= s_1 \cdots s_j \Delta \\ &= s_j^* \cdot \Delta, \end{aligned}$$

as desired. The implication, and thus the equivalence we wished to prove, follows.

□

2.2 Conditioning and Probability Bound

Using the equivalence of the conditions in Theorem 2.3, we derive a lower bound on the probability of the product of A and a unit triangular Toeplitz matrix having its Hermite form in triangular Smith form. Again, we begin with a lemma.

Lemma 2.4 (Kalofen and Saunders [5]). *Let $V \in \mathbf{K}[x]^{n\times n}$, $p \in \mathbf{K}$ be prime, and Λ be a subset of the field $\mathbf{K}$. If $\bar{V}$ is the matrix that results from post-multiplying V by a unit lower triangular Toeplitz matrix with entries chosen uniformly at random from Λ, then*

$$\mathbf{P}\Big[\bar{V} \text{ does not have generic rank profile over } \mathbf{K}[x]/(p)\Big] \leq \frac{n(n+1)}{2|\Lambda|}.$$

Proof. Follows from the proof of Theorem 2 of Chapter 4 of Kaltofen and Saunders [5] based on the Schwartz-Zippel lemma, working over the field $\mathbf{K}[x]/(p)$. The result comes from replacing the random pre-multiplied conditioning matrix with the identity matrix, and supposing A is nonsingular, as alluded to in Chen et al [1]. Replacing the left preconditioning matrix with the identity matrix eliminates the indeterminants that were in that matrix, and decreases the degree of the resulting polynomial by half. This introduces an extra factor of 2 in the denominator of the calculated probability. □

Lemma 2.5. *If $A \in \mathbf{K}[x]^{n\times n}$ has degree d, the prime factorization of $\det A$ has at most dn distinct primes.*

Proof. This follows from the Leibniz formula for the determinant,

$$\det A = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{\sigma(i)i}.$$

Since each summand on the right hand side is a product of n polynomials of degree at most d, $\det A$ has degree at most dn, and therefore has at most dn distinct prime factors. □

Theorem 2.6. *Given a nonsingular $A \in \mathbf{K}[x]^{n\times n}$ of degree d, let*

$$T_R = \begin{bmatrix} 1 & & & & \\ r_1 & 1 & & & \\ \vdots & \vdots & \ddots & & \\ r_{n-2} & r_{n-3} & \cdots & 1 & \\ r_{n-1} & r_{n-2} & \cdots & r_1 & 1 \end{bmatrix}$$

be a unit lower triangular Toeplitz matrix with $r_1, \ldots, r_{n-1}$ selected uniformly at random from $\Lambda \subseteq \mathbf{K}$. If $\bar{A} = AT_R$, then

$$\mathbb{P}\Big[\operatorname{HNF}(\bar{A}) \text{ is in triangular Smith form}\Big] \geq 1 - \frac{dn^2(n+1)}{2|\Lambda|}.$$

Proof. We note first that, if H has the same power of p in all its diagonal entries as S does for all $p \mid \det A$, then H is in triangular Smith form. For any prime q that does not divide $\det A$, q also cannot divide h_i or s_i for any i. Therefore if the order of p in h_i is the same as the order of p in s_i for all $p \mid \det A$, h_i and s_i are equal.

Now, suppose $\det A = p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}$ is the prime factorization of $\det A$. If V has generic rank profile mod p_i, clearly it satisfies condition 2 of Theorem 2.3. Note that $A = USV$, $AT_R = (USV)T_R = US(VT_R)$, and so VT_R is a unimodular right Smith form multiplier for AT_R. By Lemma 2.4, the probability that VT_R *does not* have generic rank profile mod p_i for any p_i is at most

$$\frac{n(n+1)}{2|\Lambda|}.$$

Since $t \leq dn$ by Lemma 2.5, by the union bound, our probability that VT_R does not have generic rank profile for every p_i is at most

$$dn \cdot \left(\frac{n(n+1)}{2|\Lambda|} \right) = \frac{dn^2(n+1)}{2|\Lambda|},$$

and so by Theorem 2.3, taking the complement of this probability gives our desired result. □

The probability estimate in Theorem 2.6 is likely a very pessimistic bound, since instead of conditioning V precisely to fulfill Condition (2), we aim for the stronger condition of V having generic rank profile. This allows us to use classical results for preconditioning matrices to have generic rank profile, i.e., that of Kaltofen and Saunders [5].

Chapter 3

Preconditioning for Leading Smith Determinants

Using a similar framework to that of Theorem 2.6, we provide a result for conditioning matrices such that calculating their determinantal divisors is reduced to calculating a single GCD of two determinants. The rest of this chapter is structured similarly to Chapter 2. Section 3.1 culminates in Lemma 3.4. This lemma allows us to precondition a nonsingular matrix $A \in \mathbf{R}^{n\times n}$, with $\mathbf{R}$ a principal ideal domain, such that the determinantal divisors of A can be easily calculated *if* $\mathrm{HNF}(A)$ is in triangular Smith form. After preconditioning, any determinantal divisor s_i^* of A can be found by taking the GCD of $\det A$ with the leading principal $i \times i$ minor of A.

In Section 3.2, we build on the main result from Chapter 2 (i.e. Theorem 2.6) as well as the work of the previous section, specializing to the case where $\mathbf{R} = \mathbf{K}[x]$ for a field $\mathbf{K}$. We show in Theorem 3.6 that any nonsingular $A \in \mathbf{K}[x]^{n\times n}$ can be preconditioned such that its determinantal divisors have the property described in the previous paragraph, by pre- and post- multiplying by a unit lower upper and lower triangular Toeplitz matrix, respectively. We also give a lower bound on the probability of success of this preconditioning.

3.1 Reduction to Rank Profile Condition

We begin with a definition. Recall that we use $A_{i\times j}$ to denote the $i \times j$ leading principal submatrix of A, or simply A_i if $i = j$.

Definition 3.1. *A nonsingular matrix $A \in \mathbf{R}^{n\times n}$ has* leading Smith determinants *if*

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

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

Intuitively, this means that A is perturbed such that all of the necessary information for the GCD of the $i \times i$ minors of A are contained in the leading principal $i \times i$ minor. This makes any of the values s_i^* very easy to compute, requiring only a single $i \times i$ determinant (if $\det A$ has already been calculated), and a gcd of two polynomials with degrees at most $i \deg A$ and $n \deg A$, respectively. The 1997 Smith form algorithm of Labahn and Storjohann [9], for example, works by randomly perturbing matrices to satisfy this condition with some probability.

We start by essentially reusing Lemma 2.4, with a slight modification.

Lemma 3.2 (Kalofen and Saunders [5])**.** *Let $V \in \mathbf{K}[x]^{n\times n}$, $p \in \mathbf{K}$ be prime, and Λ be a subset of the field $\mathbf{K}$. If $\bar{V}$ is the matrix that results from pre-multiplying V by a unit upper triangular Toeplitz matrix with entries chosen uniformly at random from Λ, then*

$$\mathbf{P}\Big[\bar{V} \text{ does not have generic rank profile over } \mathbf{K}[x]/(p)\Big] \leq \frac{n(n+1)}{2|\Lambda|}.$$

Proof. Follows directly from taking the transpose of the matrices in Lemma 2.4. □

We now reduce the condition of having leading Smith determinants, to a condition on individual primes $p \in \mathbf{R}$, similarly to the proof of Theorem 2.6. We claim the following:

Lemma 3.3. *For $A \in \mathbf{R}^{n\times n}$, let $i \in \{1, \ldots, n\}$ be fixed. If for all primes $p \in \mathbf{R}$ such that $p \mid \det A$, the order of p in $\det A_i$ is the same as the order of p in s_i^*, then* $\gcd(\det A_i, \det A) = s_i^*$.

Proof. Since $s_i^* \mid \det A$, this follows directly from basic properties of the GCD. □

Recall that for any $A \in \mathbf{R}^{n\times n}$, there exists $W, H \in \mathbf{R}^{n\times n}$ with W unimodular, H in Hermite normal form, and $A = WH$. Our final lemma defines a condition on W, that is sufficient for A to satisfy the condition of Lemma 3.3 for a particular prime p.

Lemma 3.4. *Let $A \in \mathbf{R}^{n\times n}$ be nonsingular with the property that $H = \mathrm{HNF}(A)$ is in triangular Smith form, and let W be the unique unimodular matrix such that $A = WH$. Then for any prime $p \in \mathbf{R}$, the following are equivalent.*

1. *W has generic rank profile over $\mathbf{R}/(p)$.*
2. *For all $i = 1, \ldots, n$, the order of p in $\det A_i$ is the same as the order of p in s_i^*.*

Proof. For any $i \in \{1, \ldots, n\}$, we can rewrite W, H and A as block matrices, as follows.

$$\underbrace{\begin{bmatrix} W_i & * \\ * & * \end{bmatrix}}_{W} \underbrace{\begin{bmatrix} H_i & * \\ 0 & * \end{bmatrix}}_{H} = \underbrace{\begin{bmatrix} W_i H_i & * \\ * & * \end{bmatrix}}_{A}$$

So $A_i = W_i H_i$, and therefore $\det A_i = \det W_i \cdot \det H_i$. But $\det H_i = h_1 h_2 \cdots h_i = h_i^* = s_i^*$, since H is in triangular Smith form. From this, it is easy to see that the order of p in $\det A_i$ is the same as the order of p in s_i^* if and only if $\det W_i$ contains no factor of p, thus proving the equivalence. □

3.2 Conditioning and Probability Bound

The following result shows that pre-multiplication by a unit upper triangular Toeplitz matrix suffices to condition a matrix for leading Smith determinants, *provided that* the Hermite form of the original matrix is in triangular Smith form.

Theorem 3.5. *Given a nonsingular $A \in \mathbf{K}[x]^{n\times n}$ of degree d whose Hermite normal form H is in triangular Smith form, let*

$$T_L = \begin{bmatrix} 1 & l_1 & \ldots & l_{n-2} & l_{n-1} \\ & 1 & \ldots & l_{n-3} & l_{n-2} \\ & & \ddots & \vdots & \vdots \\ & & & 1 & l_1 \\ & & & & 1 \end{bmatrix}$$

be a unit upper triangular Toeplitz matrix with $l_1, \ldots, l_{n-1}$ selected uniformly at random from $\Lambda \subseteq \mathbf{K}$. If $\bar{A} = T_L A$, then

$$\mathbb{P}\Big[\bar{A} \text{ has leading Smith determinants}\Big] \geq 1 - \frac{dn^2(n+1)}{2|\Lambda|}.$$

Proof. Note that $T_L A = T_L(WH) = (T_L W)H$, where W is the unique unimodular Hermite multiplier matrix for A. So, $T_L W$ is the unique unimodular Hermite multiplier matrix for $T_L A$. By Lemma 3.2, for each p with $p \mid \det A$, $T_L W$ has generic rank profile over $\mathbb{R}/(p)$ with probability at least

$$1 - \frac{n(n+1)}{2|\Lambda|}.$$

By Lemma 2.5, there can be at most dn unique primes that divide $\det A$. Therefore by the union bound, the probability that $T_L W$ has generic rank profile over $\mathbf{R}/(p)$ for all p is at least

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

By Lemmas 3.3 and 3.4, $T_L W$ having generic rank profile over $\mathbf{R}/(p)$ for all p means that $\gcd(\det A_i, \det A) = s_i^*$ for all i, and therefore A has leading Smith determinants. □

Because of Theorem 2.6, we can easily precondition A on the right so that it satisfies the triangular Smith form condition of Theorem 3.5, while still ensuring we can use another preconditioner on the left. Our final theorem is an easy corollary of these two results.

Theorem 3.6. *Given a nonsingular $A \in \mathbf{K}[x]^{n\times n}$ of degree d, let*

$$T_L = \begin{bmatrix} 1 & l_1 & \cdots & l_{n-2} & l_{n-1} \\ & 1 & \cdots & l_{n-3} & l_{n-2} \\ & & \ddots & \vdots & \vdots \\ & & & 1 & l_1 \\ & & & & 1 \end{bmatrix}, \quad T_R = \begin{bmatrix} 1 & & & & \\ r_1 & 1 & & & \\ \vdots & \vdots & \ddots & & \\ r_{n-2} & r_{n-3} & \cdots & 1 & \\ r_{n-1} & r_{n-2} & \cdots & r_1 & 1 \end{bmatrix}$$

be unit upper (respectively, lower) triangular Toeplitz matrices with $l_1, \ldots, l_{n-1}$ and $r_1, \ldots, r_{n-1}$ selected uniformly at random from $\Lambda \subseteq \mathbf{K}$. If $\tilde{A} = T_L A T_R$, then

$$\mathbb{P}\Big[\tilde{A} \text{ has leading Smith determinants}\Big] \geq 1 - \frac{dn^2(n+1)}{|\Lambda|}.$$

Proof. Follows directly from applying the union bound to the probabilities in Theorems 2.6 and 3.5. □

Chapter 4

Conclusion

We have shown that, to precondition a nonsingular matrix A over a principal ideal domain such that its Hermite form and Smith form have the same diagonal entries, it suffices to post-multiply A by a random unit triangular Toeplitz matrix. We have also shown that multiplying by two random unit triangular Toeplitz matrices are enough to condition A to have principal leading minors whose GCDs with $\det A$ are the invariant factors of A.

Since so much of the theory behind our main results rely on the assumption that A is nonsingular, the singular case would likely require a very different approach. The more general case of the probability bound from Kaltofen and Saunders [5] used in the proof of Theorem 2.6 also holds for singular A, if two preconditioning matrices are used. However, the proof of Theorem 2.3 completely breaks down, among others. Therefore, it would be interesting to see how these results hold up without that assumption.

Additionally, as stated, the probability bound in Theorem 2.6 is likely very pessimistic, as we precondition for the stronger condition of the right Smith multiplier having generic rank profile modulo each p. It is quite possible that a tighter bound can be placed on this probability via other methods.

References

[1] Li Chen, Wayne Eberly, Erich Kaltofen, B. David Saunders, William J. Turner, and Gilles Villard. Efficient matrix preconditioners for black box linear algebra. *Linear Algebra and its Applications*, 343-344:119–146, 2002. Special Issue on Structured and Infinite Systems of Linear equations.

[2] Wayne Eberly. Black box Frobenius decompositions over small fields. In *Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation*, ISSAC '00, page 106–113, New York, NY, USA, 2000. Association for Computing Machinery.

[3] Erich Kaltofen, M.S. Krishnamoorthy, and B. David Saunders. Parallel algorithms for matrix normal forms. *Linear Algebra and its Applications*, 136:189–208, 1990.

[4] Erich Kaltofen, Mukkai Krishnamoorthy, and David Saunders. Fast parallel computation of Hermite and Smith forms of polynomial matrices*. *SIAM Journal on Algebraic Discrete Methods*, 8:683–690, 12 1987.

[5] Erich Kaltofen and David Saunders. On Wiedemann's method of solving sparse linear systems. In *Lecture Notes in Computer Science*, volume 539, pages 29–38, 10 1991.

[6] Thom Mulders and Arne Storjohann. The modulo N extended GCD problem for polynomials. In *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation*, ISSAC '98, page 105–112, New York, NY, USA, 1998. Association for Computing Machinery.

[7] Morris Newman. *Integral matrices*, volume 45. Academic Press, 1972.

[8] Arne Storjohann. On the complexity of inverting integer and polynomial matrices. *Comput. Complex.*, 24(4):777–821, December 2015.

[9] Arne Storjohann and George Labahn. A fast Las Vegas algorithm for computing the Smith normal form of a polynomial matrix. *Linear Algebra and its Applications*, 253:155—173, 1997.

[10] Gilles Villard. Fast parallel computation of the Smith normal form of polynomial matrices. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, ISSAC '94, page 312–317, New York, NY, USA, 1994. Association for Computing Machinery.

[11] Gilles Villard. Generalized subresultants for computing the Smith normal form of polynomial matrices. *Journal of Symbolic Computation*, 20(3):269–286, 1995.