

A Rigorous Proofless Approach to Linear Algebra

Murisi Tarusenga

Thursday 2nd November, 2017 09:33

1 Introduction

What follows is an attempt to present linear algebra as a system of algorithms in a manner devoid of argumentation. The functioning of these algorithms hopefully is made apparent by stating expected variable values at certain points of execution. Mathematical argumentation is circumvented by letting algorithms *show* what a proposition in an argument might have *said*.

The subset of linear algebra I intend to tackle consists of the **Smith normal form**, **determinants**, **compound matrices**, **general solutions to linear systems**, **characteristic matrices**, the rational canonical form, **block matrix multiplication**, **minimum polynomials**, **orthogonalization**, and **the spectral theorem for symmetric matrices**. To get the above done, I also have to extract the algorithms from **Sturm's theorem**, **Cauchy's bound**, **the Cauchy-Schwarz inequality**, and **the Euclidean division algorithm**.

One way to use this exposition to understand linear algebra is to go through the algorithms in order and execute each one on one or two inputs. At any rate, please be taking the following into consideration:

1. Where a proof would express generality using universal quantification, the algorithms below show generality by allowing one to choose inputs. See **algorithm 24**.
2. Where a proof would express that a proposition implies contradiction, the algorithms below merely show how certain control flows lead to absurdity. See algorithms **11**, **28**, **35**, and **52**.
3. Where a proof would use the principle of mathematical induction, the algorithms below merely use iteration/recursion and loop invariants. See algorithms **47**, **47 auxilliary**, and **52**.

Here, I would like to note that this project is largely based on the textbook Linear Algebra by Harold

Edwards. In summary, I have taken the text; removed all the exercises and exposition; removed all the proofs inessential to proving the spectral theorem for symmetric matrices; extracted and purified the algorithms used in each proof; and conjured up my own algorithms in the cases where I could not extract an algorithm.

Contents

1	Introduction	1
2	Body	2
2.1	Algorithm 1	2
2.2	Algorithm 2	3
2.3	Algorithm 3 (Smith normal form construction)	3
2.4	Algorithm 4 (Associativity verification)	4
2.5	Algorithm 5 (Extended Smith normal form construction)	4
2.6	Algorithm 6 (Inverse extended Smith normal form construction)	4
2.7	Algorithm 7	5
2.8	Algorithm 8 (Determinant calculation)	5
2.9	Algorithm 9 (Multilinearity verification)	5
2.10	Algorithm 10 (Alternation verification)	6
2.11	Algorithm 11	6
2.12	Algorithm 12	6
2.13	Algorithm 13 (Compound matrix calculation)	7
2.14	Algorithm 14 (Compound matrix of identity calculation)	7
2.15	Algorithm 15	8
2.16	Algorithm 16	8
2.17	Algorithm 17	9
2.18	Algorithm 18 (Compound matrix of matrix product calculation)	9
2.19	Algorithm 19 (Determinant equals product of diagonal entries verification)	9
2.20	Algorithm 20 (Transpose calculation) .	10

2.21	Algorithm 21 (Transpose of product verification)	10
2.22	Algorithm 22 (Determinant of transpose verification)	10
2.23	Algorithm 23 (Compound matrix of transpose verification)	10
2.24	Algorithm 24 (Linear system solution construction)	10
2.25	Algorithm 25	11
2.26	Algorithm 26	11
2.27	Algorithm 27	12
2.28	Algorithm 28	12
2.29	Algorithm 29 (Rational canonical form construction)	12
2.30	Algorithm 30	13
2.31	Algorithm 31 (Block matrix multiplication)	14
2.32	Algorithm 32	14
2.33	Algorithm 33	15
2.34	Algorithm 34 (Difference of powers)	16
2.35	Algorithm 35	16
2.36	Algorithm 36 (Bisection)	16
2.37	Algorithm 37	17
2.38	Algorithm 38 (Sturm's algorithm initialization)	18
2.39	Algorithm 39 (Change in number of sign changes verification)	18
2.40	Algorithm 40 (Cauchy's positive verification)	19
2.41	Algorithm 41 (Cauchy's alternation verification)	19
2.42	Algorithm 42 (Sturm's sign change)	19
2.43	Algorithm 43	20
2.44	Algorithm 44	20
2.45	Algorithm 45	21
2.46	Algorithm 46 (Euclidean division)	22
2.47	Algorithm 47 (Edwards' Sturm chain construction)	22
	2.47.1 Auxilliary algorithm	23
2.48	Algorithm 48	24
2.49	Algorithm 49 (Upper triangular matrix multiplication)	25
2.50	Algorithm 50 (Orthogonalization)	25
2.51	Algorithm 51 (Cauchy-Schwarz inequality)	26
2.52	Algorithm 52	26
2.53	Algorithm 53	26
2.54	Algorithm 54 (Symmetric matrix spectral algorithm initialization)	27
2.55	Algorithm 55 (Symmetric matrix spectral)	28

2 Body

2.1 Algorithm 1

Choose a $\mathcal{M}_{1,2}(\mathbb{Q}[x])$, A , and do the following:

1. Let A be our working matrix.
2. If $A_{1,1} = 0$, then do the following:
 - (a) Add $A_{1,2}$ to $A_{1,1}$.
3. Then while $A_{1,2} \neq 0$, do the following:
 - (a) If $\deg(A_{1,1}) = \deg(A_{1,2})$ and $A_{1,1}$ is monic, then:
 - i. Subtract a times $A_{1,1}$ from $A_{1,2}$ where a is the leading coefficient of $A_{1,2}$.
 - (b) Otherwise, if $\deg(A_{1,1}) = \deg(A_{1,2})$ but $A_{1,1}$ is not monic, then do the following:
 - i. Add $1 - b/a$ times $A_{1,2}$ to $A_{1,1}$ where b and a are the leading coefficients of $A_{1,1}$ and $A_{1,2}$ respectively.
 - ii. Go to (3a) again.
 - (c) Otherwise, if $\deg(A_{1,1}) \neq \deg(A_{1,2})$, then do the following:
 - i. Let p and q be locations of the polynomials with the lower and higher degree respectively.
 - ii. Add $-b/ax^{\deg(p)-\deg(q)}$ times p to q where b and a are the leading coefficients of q and p respectively.
 - iii. If q becomes zero, then do the following:
 - A. Undo operation (3cii) and do the same thing again, only this time using the fraction $1 - b/ax^{\deg(p)-\deg(q)}$.
 - (d) **Verify that the degree of only one entry changed.**
 - (e) **Verify that the changed entry's degree decreased.**
4. **Verify that $A_{1,2} = 0$.**
5. If the original A was not zero, then do the following:

- (a) Verify that the body of loop (3) executed at least once.
 - (b) Verify that the last instructions executed were an instance of (3ai), (3d), then (3e).
 - (c) **Therefore verify that $A_{1,1}$ is a monic polynomial.**
6. Otherwise, do the following:
- (a) Verify that both entries were originally zero.
 - (b) **Therefore, now verify that $A_{1,1} = 0$.**
7. **Yield the tuple $\langle A \rangle$.**

2.2 Algorithm 2

Choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, A , and do the following:

1. Let A be our working matrix.
2. If the top-left entry of the matrix is zero, then do the following:
 - (a) While there are non-zero entries in the top row less its first entry, do the following:
 - i. In the first row, select the 1×2 matrix whose right entry coincides with the last non-zero entry of the first row
 - ii. Apply **algorithm 1** on this submatrix but this time adding and subtracting the entire columns instead of merely just the entries in the submatrix.
 - iii. Verify that the left and right entries of the submatrix are now non-zero and zero respectively.
 - iv. If the left entry of the submatrix coincides with the top-left entry of the matrix,
 - A. Verify that the top-left entry is now non-zero.
 - B. Go to operation (2).
 - (b) Now do the same operations as in (a), but this time with the operations themselves reflected across the matrix's diagonal. I.e. making 2×1 submatrices starting from the bottom-most non-zero row of the first column and working your way upwards.

- (c) Verify that, except for the top-left entry, the first row and the first column are zero. Now skip to operation (3).
3. While the top-left entry is non-zero, do the following:
- (a) Call operation (1a) except that at (1aivA), we instead expect that $A_{1,1}$ has a lower degree than before.
 - (b) Call operation (1b) except that at (1bivA), we instead expect that $A_{1,1}$ has a lower degree than before.
 - (c) Call operation (1c).
4. Apply **algorithm 2** to the $(m-1) \times (n-1)$ submatrix formed by removing the first row and first column from the matrix under consideration.
5. Verify that (3)'s execution leaves the first row and column unchanged.
6. **Verify that A is now a diagonal matrix.**
7. **Yield the tuple $\langle A \rangle$.**

2.3 Algorithm 3 (Smith normal form construction)

Choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, A , and do the following:

1. Apply **algorithm 2** on A .
2. If $m > 0$ and $n > 0$, then do the following:
 - (a) For j going from 2 to $\min(m, n)$, do the following:
 - i. Add row j to row 1 and let A' , a copy of A , be our working matrix.
 - ii. Apply **algorithm 1** on the submatrix of A' formed by selecting row 1 and columns 1 and j as if there were nothing in between.
 - iii. Verify that the execution of **algorithm 1** in (ii) manifested itself in a sequence of column operations to make $A'_{1,j}$ zero.
 - iv. Temporarily stepwise undo these column operations and do the following:
 - A. Verify that $A_{1,1} = p * A'_{1,1}$, where p is some implicitly constructed polynomial.

- B. Verify that $A_{1,1}$ is a factor of all $A_{2,2}, \dots, A_{j-1,j-1}$.
- C. Therefore verify that $A'_{1,1}$ is also a factor of all $A_{2,2}, \dots, A_{j-1,j-1}$.
- D. Verify that $A_{j,j} = A_{1,j} = q * A'_{1,1}$, where q is some implicitly constructed polynomial.
- E. Verify that $A'_{j,1} = r * A_{j,j} = r * A_{1,j} = rq * A'_{1,1}$, where r is some implicitly constructed polynomial.
- F. Verify that $A'_{j,j} = t * A_{j,j} = t * A_{1,j} = tq * A'_{1,1}$, where t is some implicitly constructed polynomial.
- v. Subtract rq times row 1 from row j .
- vi. Now verify that $A'_{j,1} = 0$.
- vii. Now let A be equal to our working matrix.
- (b) Call (2) in-place on the submatrix formed by removing the first row and column.
- (c) Verify that each entry on the diagonal after $A_{1,1}$ is a linear combination of multiples of $A_{1,1}$.
- (d) Therefore verify that each entry on the diagonal is still be a multiple of $A_{1,1}$.
- (e) **Let** $A_{0,0} = 1$.
- (f) **Verify that for all** $1 \leq i \leq \min(m, n)$, $A_{i,i} = u_i A_{i-1,i-1}$, **where** u_i **is a polynomial implicitly constructed above.**
- 3. **Yield the tuple** $\langle A \rangle$.

2.4 Algorithm 4 (Associativity verification)

Choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, **A**, **a** $\mathcal{M}_{n,p}(\mathbb{Q}[x])$, **B**, **and a** $\mathcal{M}_{p,q}(\mathbb{Q}[x])$, **C**. Now do the following:

1. Verify that $(AB)_{i,l} = \sum_{k=1}^n (A_{i,k} * B_{k,l})$.
2. Verify that $((AB)C)_{i,r} = \sum_{l=1}^p ((AB)_{i,l} * C_{l,r}) = \sum_{l=1}^p (\sum_{k=1}^n (A_{i,k} * B_{k,l}) * C_{l,r})$.
3. Verify that $(BC)_{k,r} = \sum_{l=1}^p (B_{k,l} * C_{l,r})$.

4. Verify that $(A(BC))_{i,r} = \sum_{k=1}^n (A_{i,k} * (BC)_{k,r}) = \sum_{k=1}^n (A_{i,k} * \sum_{l=1}^p (B_{k,l} * C_{l,r}))$.
5. Verify that $(2) = \sum_{l=1}^p (\sum_{k=1}^n (A_{i,k} * B_{k,l} * C_{l,r})) = \sum_{k=1}^n (\sum_{l=1}^p (A_{i,k} * B_{k,l} * C_{l,r})) = \sum_{k=1}^n (A_{i,k} * \sum_{l=1}^p (B_{k,l} * C_{l,r})) = (4)$.
6. **Therefore verify that** $(AB)C = A(BC)$.

2.5 Algorithm 5 (Extended Smith normal form construction)

Choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, A , and do the following:

1. Make a singleton list containing one item, the chosen matrix A .
2. Augment **algorithm 3** so that each time a polynomial x times a column i is added onto column j , an $n \times n$ matrix that only has 1s on its diagonal, and such that the only non-zero entry off its diagonal is x at position (i, j) , is appended onto the list.
3. Also augment **algorithm 3** so that each time a polynomial x times a row i is added onto row j , an $n \times n$ matrix that only has 1s on its diagonal, and such that the only non-zero entry off its diagonal is x at position (j, i) , is prepended onto the list.
4. Now run **algorithm 3** on the matrix A . Let the tuple $\langle D \rangle$ receive the result.
5. Verify that D is a diagonal matrix.
6. **Verify that** D **equals the product, in-order, of the matrices in the list.**
7. Let M be the product of the sublist whose entries are all those that precede A .
8. Let N be the product of the sublist whose entries are all those that follow the original A .
9. **Verify that** $D = MAN$.
10. **Yield the tuple** $\langle D, M, N \rangle$.

2.6 Algorithm 6 (Inverse extended Smith normal form construction)

Choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, A , and do the following:

1. Run **algorithm 3** on matrix A to get the matrix D .
2. Now, starting work with the matrix D , iterate through the row and column operations of **algorithm 3** starting from the last and ending with the first:
 - (a) If the current operation adds polynomial x times column i to column j , then add $-x$ times column i from column j from our working matrix.
 - (b) If the current operation adds polynomial x times row i to row j , then add $-x$ times row i from row j from our working matrix.
3. Verify that our working matrix now equals A .
4. Make a singleton list containing one item, the original matrix D .
5. Augment (2) in a way analogous to how **algorithm 5** augmented **algorithm 3**, but this time with the list provided in (4).
6. Now run augmented (2).
7. **Verify that A equals the product, in-order, of the matrices in the list.**
8. Let M^{-1} be the product of the sublist whose entries are all those that precede D .
9. Let N^{-1} be the product of the sublist whose entries are all those that follow D .
10. **Verify that $A = M^{-1}DN^{-1}$.**
11. **Yield the tuple $\langle M^{-1}, D, N^{-1} \rangle$.**

2.7 Algorithm 7

Choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, A , and do the following:

1. Run **algorithm 6** with A as the choice matrix.
2. Now, starting work with the matrix I_n , the $n \times n$ matrix with only 1s on the diagonal, do the following operations:
 - (a) Apply in-order the column operations that were applied on A
 - (b) Then apply in-order the column operations that were applied on D
3. Verify that the application of operation (2) leaves I_n unchanged.

4. Verify that $(I_n N)N^{-1}$ evaluates to the same matrix produced by (2).
5. **Therefore verify that $(I_n N)N^{-1} = I_n$.**
6. **Therefore, using **algorithm 4**, verify that $I_n = (I_n N)N^{-1} = I_n(NN^{-1}) = NN^{-1}$.**

Using similar computations, verify that $N^{-1}N = I_n$, and that $MM^{-1} = M^{-1}M = I_m$.

2.8 Algorithm 8 (Determinant calculation)

Choose a $\mathcal{M}_{m,m}(\mathbb{Q}[x])$, A , and do the following:

1. If m equals 0, then do the following:
 - (a) **Yield the tuple $\langle 1 \rangle$.**
2. Otherwise, do the following:
 - (a) Let a be the sum of m terms where, counting from $i = 0$, the i^{th} term is $((-1)^i A_{i,1})$ times the result of applying **algorithm 8** on the submatrix formed by removing the first column and i^{th} row from A .
 - (b) **Yield the tuple $\langle a \rangle$.**

We will use the notation $\det_{I,J}(A)$ to refer to the invocation of **algorithm 8** on the square submatrix created by selecting the sequence of rows I and the sequence of columns J from A . If neither I nor J are specified, then the invocation shall happen directly on A .

2.9 Algorithm 9 (Multilinearity verification)

Choose a $\mathbb{Q}[x]$ p . Choose two $\mathcal{M}_{m,1}(\mathbb{Q}[x])$ s, B and C . Choose a $\mathcal{M}_{m,m}(\mathbb{Q}[x])$, A , such that its i^{th} column is $B + pC$. Now do the following:

1. Considering every element of A to be a unit, verify that fully expanding out $\det(A)$ yields an alternating sum of $m!$ terms, where each term is the product of m entries of A , where each entry has a distinct row and distinct column.
2. Distribute out the entries of the i^{th} column occurring in this alternating sum.
3. Verify that the outcome of (2) is $m! * 2$ terms.

4. Reorder the terms so that the currently odd ones come first and the currently even ones come last.
5. Verify that $\det(A) = \det(A') + \det(A'')$ where A' is A with the i^{th} column replaced by B and A'' is A with the i^{th} column replaced by pC .
6. Reorder the factors of each term in $\det(A'')$ to bring p to the front.
7. Now verify that the $\det(A'') = p \det(A''')$, where A''' is A with the i^{th} column replaced by C .
8. **Therefore verify that** $\det(A) = \det(A') + p \det(A''')$.

Make an analogous algorithm for cases when a given row is the sum of two $1 \times m$ matrices.

2.10 Algorithm 10 (Alternation verification)

Choose a $\mathcal{M}_{m,m}(\mathbb{Q}[x])$, A . Choose a row $1 < i \leq m$. Let A' be A with rows $i-1$ and i swapped. Now do the following:

1. Fully expand out $\det A$ into $m!$ terms and then do the same for $\det A'$.
2. For each of the $m!$ ways to select m rows from A , let $r = (r_1, r_2, \dots, r_m)$ be the rows selected corresponding to the columns $1, 2, \dots, m$ respectively, and do the following:
 - (a) Verify that the values selected by r in A are the same as the values selected by r' in A' , where r' is obtained by swapping the values $i-1$ and i in the sequence r .
 - (b) Execute **algorithm 8** on A , and consider the execution path that produces the term corresponding to the row selections r . Ditto for A' and r' .
 - (c) Let k be the lesser of the indices of the values $i-1$ and i in the sequence r .
 - (d) Verify that the signs attached to $A_{r_1,1}, \dots, A_{r_{k-1},k-1}$ are the same as the signs attached to $A'_{r'_1,1}, \dots, A'_{r'_{k-1},k-1}$.
 - (e) Verify that indices r_k and r'_k identify adjacent rows in the remaining respective submatrices of A and A' .
 - (f) Therefore verify that the signs then attached to A_{r_k} and $A'_{r'_k}$ are opposite.
3. Therefore verify that every term in the full expansion of $\det(A)$ corresponds to a unique negated version of itself in the full expansion of $\det(A')$.
4. **Therefore verify that** $\det(A') = -\det(A)$.

Make a simpler algorithm to verify that column swaps cause sign alternations.

2.11 Algorithm 11

Choose integers $1 < i \leq m$. Choose a $\mathcal{M}_{m,m}(\mathbb{Q}[x])$, A , such that columns $i-1$ and i are the same. Now do the following:

1. If $\det(A) \neq 0$, then do the following:
 - (a) Let A' be A with columns i and $i-1$ swapped.
 - (b) Verify that A' equals A .
 - (c) Therefore verify that $\det(A') = \det(A)$.
 - (d) Using **algorithm 10**, also verify that $\det(A') = -\det(A)$.
 - (e) **Abort algorithm.**
2. Otherwise, do the following:
 - (a) **Verify that** $\det(A) = 0$.

Make an analogous algorithm to verify that matrix choices with repeated rows yield determinants equal to zero.

2.12 Algorithm 12

Choose integers $1 \leq i \leq m$. Choose an integer $0 < j \leq m-i$. Choose a $\mathcal{M}_{m,m}(\mathbb{Q}[x])$, A . Let A'

be A but with column i moved j places. Now do the following:

1. Let $A_i = A$.
2. For $k = i + 1$ to $k = i + j$, do the following:
 - (a) Let A_k be obtained by swapping columns $k - 1$ and k of A_{k-1} .
 - (b) Using **algorithm 10**, verify that $\det(A_k) = -\det(A_{k-1})$.
3. Verify that $A' = A_{i+j}$.
4. **Therefore verify that** $\det(A') = \det(A_{i+j}) = (-1)^1 \det(A_{i+j-1}) = \dots = (-1)^j \det(A_i) = (-1)^j \det(A)$.

Make an analogous algorithm that verifies that $\det(A') = (-1)^j \det(A)$ when a non-positive integer, j , is chosen.

Also make an analogous algorithm that does the verification for moved rows.

2.13 Algorithm 13 (Compound matrix calculation)

Choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, A , and choose an integer $0 \leq k \leq \min(m, n)$. Yield a tuple comprising the $\binom{m}{k} \times \binom{n}{k}$ matrix constructed as follows:

1. The rows are labeled by the colexicographically sorted list of increasing length- k sequences whose elements are picked from the first m positive integers.
2. The columns are labeled by the colexicographically sorted list of increasing length- k sequences whose elements are picked from the first n positive integers.
3. For each row label I : For each column label J : Let the entry at position (I, J) be $\det_{I,J}(A)$.

We will use the notation $C_k(A)$ to refer to an invocation of **algorithm 13 on the matrix A .**

2.14 Algorithm 14 (Compound matrix of identity calculation)

Choose two integers $0 \leq k \leq m$. To evaluate $C_k(I_m)$, iterate through all its entries and do the following:

1. **Algorithm 13** requires us to form a submatrix B of A using the rows listed in the row label, and the columns listed in the column label.
2. If the entry is diagonal, then do the following:
 - (a) Verify that the k column indices we just selected from I_m are the same as the k rows indices we just selected from I_m .
 - (b) Therefore verify that the diagonal positions of B correspond to diagonal positions of I_m .
 - (c) Therefore verify that the diagonal positions of B are 1s.
 - (d) Also verify that the non-diagonal positions of B correspond to a non-diagonal entry of I_m .
 - (e) Therefore verify that the non-diagonal positions of B are 0.
 - (f) Therefore verify that $B = I_k$.
 - (g) **Therefore using **algorithm 8**, verify that $\det(B) = 1$.**
3. Otherwise, do the following:
 - (a) Verify that the k column indices we just selected from I_m are different from the k row indices that we just selected from I_m .
 - (b) Let i be a selected row index that is not also a column index.
 - (c) Iterate through the columns of the row in the submatrix B that corresponds to row i of I_m and do the following:
 - i. Let j be the column index of I_m to which this column corresponds.
 - ii. Using (3b), verify that $i \neq j$.
 - iii. Verify that $(I_m)_{i,j} = 0$.
 - iv. Therefore verify that this entry is 0.
 - (d) Verify that the row in the submatrix B that corresponds to row i of I_m is entirely zero.
 - (e) **Therefore using **algorithm 8**, verify that $\det(B) = 0$.**
4. **Therefore verify that $C_k(I_m) = I_{\binom{m}{k}}$.**

2.15 Algorithm 15

Choose an integer $1 \leq k \leq \min(m, n)$. Choose a $\mathcal{M}_{m,m}(\mathbb{Q}[x])$, A , whose diagonal entries are 1s, and such that the only entry off the diagonal is the $\mathbb{Q}[x]$ p at (i, j) . Also choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, B . To evaluate $C_k(AB)$, do the following:

1. Verify that AB equals B , but with its row i having p times B 's row j added to it.
2. Go through the row labels, I , of $C_k(AB)$ and do the following:

(a) If $i \notin I$, then do the following:

- i. For $l \in I$: For $j = 1$ to $j = n$: Verify that $(AB)_{l,j} = B_{l,j}$.
- ii. Therefore for each column label J , verify that $C_k(AB)_{I,J} = \det_{I,J}(AB) = \det_{I,J}(B) = C_k(B)_{I,J}$.
- iii. **Therefore verify that row I of $C_k(AB)$ equals row I of $C_k(B)$.**

(b) Otherwise, if $i \in I$, then:

- i. Let I' be I but with an in-place replacement of i by j .
- ii. For each column label J : Using **algorithm 9**, verify that $C_k(AB)_{I,J} = \det_{I,J}(AB) = \det_{I,J}(B) + p * \det_{I',J}(B)$.
- iii. Let l be the signed number of places that the j introduced above needs to be moved in order to make I' a non-increasing sequence.
- iv. Let I'' be obtained from I' by moving the integer j in I' by l places.
- v. For each column label J : Using **algorithm 12**, verify that $\det_{I',J}(B) = (-1)^l \det_{I'',J}(B)$.
- vi. Therefore for each column label J : Verify that $C_k(AB)_{I,J} = \det_{I,J}(B) + p * \det_{I',J}(B) = \det_{I,J}(B) + (-1)^l p * \det_{I'',J}(B)$.
- vii. If $j \notin I$, then do the following:

- A. Verify that I'' is a decreasing sequence.

- B. Verify that I'' is a row label of $C_k(B)$.

- C. Therefore for each column label J : Verify that $C_k(AB)_{I,J} = \det_{I,J}(B) + (-1)^l p * \det_{I'',J}(B) = C_k(B)_{I,J} + (-1)^l p * C_k(B)_{I'',J}$.

- D. **Therefore verify that row I of $C_k(AB)$ is row I of $C_k(B)$ plus $(-1)^l p$ times row I'' added to it.**

viii. Otherwise if $j \in I$, do the following:

- A. Verify that the sequence I'' contains two consecutive j s.

- B. Using **algorithm 11**, verify that $\det_{I'',J}(B) = 0$.

- C. Therefore verify that $C_k(AB)_{I,J} = \det_{I,J}(B) = C_k(B)_{I,J}$.

- D. **Therefore verify that row I of $C_k(AB)$ is row I of $C_k(B)$.**

3. Let D be the matrix of row operations implicitly applied in (2).

4. **Verify that $C_k(AB) = DC_k(B)$.**

2.16 Algorithm 16

Choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, A , that only has entries on the diagonal. Also choose a $\mathcal{M}_{n,n}(\mathbb{Q}[x])$, B . Also choose an integer $0 \leq k \leq \min(m, n)$. To evaluate $C_k(AB)$, do the following:

1. Verify that AB equals the top $m \times n$ submatrix of B with each row i multiplied by $A_{i,i}$.
2. Go through the row labels, I , of $C_k(AB)$ and do the following:

(a) Let $(r_1, r_2, \dots, r_k) = I$.

(b) If $r_k \leq n$, then do the following:

- i. Using **algorithm 13**, verify that every element of I is less than or equal to n .

ii. Let $A_0 = A$.

iii. For $i = 1$ to $i = k$: Let A_i equal A_{i-1} but with position (r_i, r_i) set to 1.

iv. For each column label J : Repeatedly using **algorithm 9**, verify that $C_k(AB)_{I,J} = \det_{I,J}(AB) =$

$$\begin{aligned}
\det_{I,J}(A_0B) &= A_{r_1,r_1} \det_{I,J}(A_1B) = \\
&A_{r_1,r_1} A_{r_2,r_2} \det_{I,J}(A_2B) = \cdots = \\
&A_{r_1,r_1} A_{r_2,r_2} \cdots A_{r_k,r_k} \det_{I,J}(A_kB) = \\
&A_{r_1,r_1} A_{r_2,r_2} \cdots A_{r_k,r_k} \det_{I,J}(B) = \\
&A_{r_1,r_1} A_{r_2,r_2} \cdots A_{r_k,r_k} C_k(B)_{I,J}.
\end{aligned}$$

- v. Therefore verify that row I of $C_k(AB)$ is $A_{r_1,r_1} A_{r_1,r_1} \cdots A_{r_k,r_k}$ times row I of $C_k(B)$.

(c) Otherwise if $r_k > n$, then do the following:

- i. Verify that row r_k of A is zero.
 - ii. Therefore verify that row r_k of AB is zero.
 - iii. Therefore verify that the last row of the submatrix obtained by selecting rows I from AB is zero.
 - iv. Therefore using **algorithm 8**, for each column label J : verify that $C_k(AB)_{I,J} = 0$.
 - v. Therefore verify that row I of $C_k(AB)$ is zero.
3. Let D be the matrix of row operations implicitly applied in (2).
 4. Verify that D is diagonal.
 5. Verify that $C_k(AB) = DC_k(B)$.

2.17 Algorithm 17

Choose an integer $1 \leq k \leq \min(m, n)$. Choose a $\mathcal{M}_{m,m}(\mathbb{Q}[x])$, A , whose diagonal entries are 1s, and such that the only entry off the diagonal is the $\mathbb{Q}[x]$ p at (i, j) . Also choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, B . Now do the following:

1. Execute **algorithm 15** on matrices A and I_m . Let D be the matrix constructed.
2. Verify that $C_k(AI_m) = DC_k(I_m)$.
3. Using **algorithm 14**, verify that $C_k(A) = C_k(AI_m) = DC_k(I_m) = DI_{\binom{m}{k}} = D$.
4. Execute **algorithm 15** on matrices A and B . Let D' be the matrix constructed.
5. Verify that $C_k(AB) = D'C_k(B)$.
6. Verify that $D' = D = C_k(A)$.

7. Therefore verify that $C_k(AB) = C_k(A)C_k(B)$.

Make an analogous algorithm to verify that $C_k(BA) = C_k(B)C_k(A)$.

Using **algorithm 16**, make an algorithm similar to above but that works when a diagonal matrix of $\mathbb{Q}[x]$ s, A , is instead chosen.

2.18 Algorithm 18 (Compound matrix of matrix product calculation)

Choose integers $0 \leq k \leq \min(m, n, p)$. Choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, A . Also choose a $\mathcal{M}_{n,p}(\mathbb{Q}[x])$, B . Now do the following:

1. Execute **algorithm 6** on A . Let M^{-1}_i be the i^{th} element of the sublist corresponding to M and N^{-1}_i be the i^{th} element of the sublist corresponding to N .
2. Verify that $A = M^{-1}_1 \cdots M^{-1}_m D N^{-1}_1 \cdots N^{-1}_n$.
3. Using repeated applications of **algorithm 17**, verify that $C_k(AB) = C_k(M^{-1}_1 \cdots M^{-1}_m D N^{-1}_1 \cdots N^{-1}_n B) = C_k(M^{-1}_1) \cdots C_k(M^{-1}_m) * C_k(D) * C_k(N^{-1}_1) \cdots C_k(N^{-1}_n) C_k(B) = C_k(M^{-1}_1 \cdots M^{-1}_m D N^{-1}_1 \cdots N^{-1}_n) C_k(B) = C_k(A) C_k(B)$.

2.19 Algorithm 19 (Determinant equals product of diagonal entries verification)

Choose a $\mathcal{M}_{m,m}(\mathbb{Q}[x])$, A . Now do the following:

1. Execute **algorithm 6** on A . Let M^{-1}_i be the i^{th} element of the sublist corresponding to M and N^{-1}_i be the i^{th} element of the sublist corresponding to N .
2. Verify that $A = M^{-1}_1 \cdots M^{-1}_m D N^{-1}_1 \cdots N^{-1}_n$.
3. Using **algorithm 8** and **algorithm 18**, verify that $\det(A) = C_m(A) = C_m(M^{-1}_1 \cdots M^{-1}_m D N^{-1}_1 \cdots N^{-1}_n) = C_m(M^{-1}_1) \cdots C_m(M^{-1}_m) C_m(D) C_m(N^{-1}_1) \cdots C_m(N^{-1}_n) = 1 \cdots 1 C_m(D) 1 \cdots 1 = C_m(D) = \det(D)$.

4. Using **algorithm 8**, verify that $\det(D)$ is the product of the diagonal entries of D .

2.20 Algorithm 20 (Transpose calculation)

Choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, A , and do the following:

1. Make an $n \times m$ matrix, A^T .
2. For $i = 1$ to $i = n$:
 - (a) For $j = 1$ to $j = m$:
 - i. Let $A^T_{i,j} = A_{j,i}$.
3. Yield the tuple $\langle A^T \rangle$.

The notation A^T shall be used to refer to the result of invoking **algorithm 20** on a matrix A .

2.21 Algorithm 21 (Transpose of product verification)

Choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, A , and a $\mathcal{M}_{n,k}(\mathbb{Q}[x])$, B . Now do the following:

1. Verify that $B^T A^T$ and $(AB)^T$ have dimensions $k \times m$.
2. For $i = 1$ to $i = k$:
 - (a) For $j = 1$ to $j = m$:
 - i. Using **algorithm 20**, verify that $(B^T A^T)_{i,j} = \sum_{l=0}^n B_{l,i} A_{j,l} = \sum_{l=0}^n A_{j,l} B_{l,i} = (AB)_{j,i} = ((AB)^T)_{i,j}$.
3. Therefore verify that $B^T A^T = (AB)^T$.

2.22 Algorithm 22 (Determinant of transpose verification)

Choose a $\mathcal{M}_{m,m}(\mathbb{Q}[x])$, A . Now do the following:

1. Execute **algorithm 6** on A . Let M^{-1}_i be the i^{th} element of the sublist corresponding to M and N^{-1}_i be the i^{th} element of the sublist corresponding to N .
2. Verify that $A = M^{-1}_1 \cdots M^{-1}_m D N^{-1}_1 \cdots N^{-1}_n$.

3. Therefore using **algorithms 19 and 20**, verify that $\det(A^T) = \det((M^{-1}_0 \cdots M^{-1}_m D N^{-1}_0 \cdots N^{-1}_n)^T) = \det((N^{-1}_n)^T \cdots (N^{-1}_0)^T D^T (M^{-1}_m)^T \cdots (M^{-1}_0)^T) = \det(D^T) = \det(D) = \det(M^{-1}_1 \cdots M^{-1}_m D N^{-1}_1 \cdots N^{-1}_n) = \det(A)$.

2.23 Algorithm 23 (Compound matrix of transpose verification)

Choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, A , and an integer $0 \leq k \leq \min(m, n)$. Now do the following:

1. Compute the value $C_k(A^T)$.
2. For each row label I of $C_k(A^T)$, do the following:
 - (a) For each column label J of $C_k(A^T)$, do the following:
 - i. Let B be a submatrix of A^T formed by selecting the rows I and the columns J .
 - ii. Using **algorithm 22**, verify that $(C_k(A^T))_{I,J} = \det_{I,J}(A^T) = \det(B) = \det(B^T) = \det_{J,I}(A) = (C_k(A))_{J,I}$.
3. Therefore verify that $(C_k(A))^T = (C_k(A^T))$.

2.24 Algorithm 24 (Linear system solution construction)

Choose a $\mathcal{M}_{m,n}(\mathbb{Q})$, A , and a $\mathcal{M}_{m,p}(\mathbb{Q})$, B . Now do the following:

1. Execute **algorithm 6** on A and let $\langle M^{-1}, D, N^{-1} \rangle$ receive the result.
2. Verify that $A = M^{-1} D N^{-1}$.
3. Verify that M^{-1} , D , and N^{-1} contain only rational entries.
4. If the indices of the rows of D that are entirely zero are also the indices of the rows of MB that are entirely zero, then:
 - (a) Let C be an $n \times p$ matrix with its i^{th} row given as follows:
 - i. If $D_{i,i} \neq 0$, then do the following:
 - A. Let row i be row i of MB divided by $D_{i,i}$.

ii. Otherwise, do the following:

A. Choose p rational numbers to fill up the row.

- (b) Verify that $DC = MB$.
- (c) Let E be NC .
- (d) Therefore using **algorithm 7**, verify that $AE = M^{-1}DN^{-1}E = M^{-1}DN^{-1}NC = M^{-1}DI_nC = M^{-1}DC = M^{-1}MB = I_mB = B$.
- (e) Yield the tuple $\langle E \rangle$.

The notation $A \setminus B$ shall be used to refer to the result, E , of invoking **algorithm 24** on matrices A and B .

Make an analogous algorithm that yields an F such that $FA = B$. The notation B/A shall be used to refer to the F yielded by invoking this algorithm.

2.25 Algorithm 25

Choose two $\mathcal{M}_{m,m}(\mathbb{Q})$ s, A and B , such that $AB = I_m$. Now do the following:

1. Execute **algorithm 6** on B and let $\langle M^{-1}, D, N^{-1} \rangle$ receive the result.
2. Verify that $B = M^{-1}DN^{-1}$.
3. If D has a zero on its diagonal, then do the following:
 - (a) Using **algorithm 19**, verify that $\det(I_m) = \det(AB) = \det(A)\det(B) = \det(A)\det(D) = \det(A) * 0 = 0$.
 - (b) Using **algorithm 8**, verify that $\det(I_m) = 1^m = 1$.
 - (c) Verify that $0 = 1$.
 - (d) **Abort algorithm.**
4. Otherwise do the following:
 - (a) Verify that D does not have a zero on its diagonal.
 - (b) Verify that $B \setminus I_m = I_m(B \setminus I_m) = AB(B \setminus I_m) = A(B(B \setminus I_m)) = AI_m = A$.
 - (c) Therefore verify that $BA = B(B \setminus I_m) = I_m$.

2.26 Algorithm 26

Choose $\mathcal{M}_{m,m}(\mathbb{Q}[x])$ s, $\langle B, M, M^{-1}, A, N^{-1}, N \rangle$, such that:

1. B and A are $\mathcal{M}_{m,m}(\mathbb{Q})$ s.
2. $MM^{-1} = I_m$.
3. $N^{-1}N = I_m$.
4. $xI_m - B = M(xI_m - A)N$.

and do the following:

1. Post-multiply both sides of (3) by N^{-1} .
2. Verify that $(xI_m - B)N^{-1} = M(xI_m - A)NN^{-1} = M(xI_m - A)I_m = M(xI_m - A)$.
3. Let $M_0x^b + M_1x^{b-1} + \dots + M_bx^0 = M$, where the M_i are rational matrices.
4. Now let $R_1 = B^bM_0 + B^{b-1}M_1 + \dots + B^0M_b$.
5. Verify that $M - R_1 = (xI_m - B)\sum_{k=1}^b(x^{k-1}I_mB^0 + x^{k-2}I_mB^1 + \dots + x^0I_mB^{k-1})M_k$.
6. Let $Q_1 = \sum_{k=1}^b(x^{k-1}I_mB^0 + x^{k-2}I_mB^1 + \dots + x^0I_mB^{k-1})M_k$.
7. Verify that $M = (xI_m - B)Q_1 + R_1$.
8. Let $N^{-1}_0x^a + N^{-1}_1x^{a-1} + \dots + N^{-1}_ax^0 = N^{-1}$ where the N^{-1}_j are rational matrices.
9. Let $R_2 = N^{-1}_0A^a + N^{-1}_1A^{a-1} + \dots + N^{-1}_aA^0$.
10. Verify that $N^{-1} - R_2 = \sum_{k=1}^a N^{-1}_k(x^{k-1}I_mA^0 + x^{k-2}I_mA^1 + \dots + x^0I_mA^{k-1})(xI_m - A)$.
11. Let $Q_2 = \sum_{k=1}^a N^{-1}_k(x^{k-1}I_mA^0 + x^{k-2}I_mA^1 + \dots + x^0I_mA^{k-1})$.
12. Verify that $N^{-1} = Q_2(xI_m - A) + R_2$.
13. By substituting M and N^{-1} into (2), verify that $(xI_m - B)(Q_2(xI_m - A) + R_2) = ((xI_m - B)Q_1 + R_1)(xI_m - A)$.
14. By rearranging both sides, verify that $(xI_m - B)(Q_2 - Q_1)(xI_m - A) = R_1(xI_m - A) - (xI_m - B)R_2$.
15. By equating the coefficients of different powers of x both sides, verify that $Q_2 - Q_1 = 0_{m \times m}$.
16. Verify that $R_1(xI_m - A) - (xI_m - B)R_2 = (xI_m - B)(Q_2 - Q_1)(xI_m - A) = (xI_m - B)0_{m \times m}(xI_m - A) = 0_{m \times m}$.

17. Therefore by adding $(xI_m - B)R_2$ to both sides, verify that $xR_1 - R_1A = R_1(xI_m - A) = (xI_m - B)R_2 = xR_2 - BR_2$.
18. By equating the coefficients of x on both sides, verify that $R_1 = R_2$.
19. Therefore verify that $xR_1 - R_1A = R_1(xI_m - A) = (xI_m - B)R_2 = (xI_m - B)R_1 = xR_1 - BR_1$.
20. Therefore by adding $-xR_1$ to both sides, verify that $-R_1A = -BR_1$.
21. Therefore by negating both sides, verify that $R_1A = BR_1$.
22. In a similar way to (8), construct a polynomial matrix Q_3 , and a rational matrix R_3 such that $M^{-1} = (xI - A)Q_3 + R_3$.
23. Verify that $I_m = MM^{-1} = ((xI_m - B)Q_1 + R_1)M^{-1} = (xI_m - B)Q_1M^{-1} + R_1M^{-1} = (xI_m - B)Q_1M^{-1} + R_1(xI - A)Q_3 + R_1R_3 = (xI_m - B)Q_1M^{-1} + (xI - B)R_1Q_3 + R_1R_3 = (xI_m - B)(Q_1M^{-1} + R_1Q_3) + R_1R_3$.
24. By equating the powers of x on both sides, verify that $Q_1M^{-1} + R_1Q_3 = 0$.
25. By substituting zero for $Q_1M^{-1} + R_1Q_3$, **verify that** $I_m = (xI_m - B)0_{m \times m} + R_1R_3 = R_1R_3$.
26. **Therefore, verify that** $B = BI_m = BR_1R_3 = R_1AR_3$.
27. **Yield the pair** (R_1, R_3) .

2.27 Algorithm 27

Choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, A . **Choose two integers** $1 \leq i, j \leq m$ **such that** $i \neq j$ **and do the following:**

1. Subtract row j from row i .
2. Add row i to row j .
3. Subtract row j from row i .
4. **Verify that the matrix obtained is the same as the original A with its i^{th} row negated and swapped with the j^{th} row.**

2.28 Algorithm 28

Choose a $\mathcal{M}_{m,m}(\mathbb{Q})$, A , **and do the following:**

1. Using **algorithm 8**, verify that $\det(xI - A)$ is a monic polynomial of degree m .
2. Execute **algorithm 3** on the polynomial matrix $xI - A$ and let $\langle B \rangle$ be the result.
3. If any of the diagonal entries of B equal zero, then do the following:
 - (a) Using **algorithm 8**, verify that $\det(B) = 0$.
 - (b) Therefore using **algorithm 19**, verify that $\det(xI - A) = 0$.
 - (c) **Abort algorithm.**
4. Otherwise do the following:
 - (a) Verify that none of the diagonal entries of B equal zero.
 - (b) If the last diagonal entry of B is not monic, then do the following:
 - i. Cognizant of the execution of **algorithm 3**, verify that the first $m - 1$ diagonal entries of B are monic.
 - ii. Using **algorithm 8**, verify that $\det(B)$ equals the product of the diagonal entries of B .
 - iii. Therefore verify that $\det(B)$ is not monic
 - iv. Therefore by **algorithm 19**, verify that $\det(xI - A)$ is not monic
 - v. **Abort algorithm.**
 - (c) Otherwise do the following:
 - i. Verify that the last diagonal entry of B is monic.
 - ii. **Verify that none of the diagonal entries of B equal zero.**
 - iii. **Verify that all the diagonal entries of B are monic.**

2.29 Algorithm 29 (Rational canonical form construction)

Choose a $\mathcal{M}_{m,m}(\mathbb{Q})$, A , **and do the following:**

1. Execute **algorithm 5** on the polynomial matrix $xI_m - A$ and let $\langle B, \cdot \rangle$ be the result.
2. Execute **algorithm 28** on A .

3. Let E and F be a 0×0 matrices.

4. **Now iterate through the diagonal entries**
 $p = x^k + p_1x^{k-1} + p_2x^{k-2} + \dots + p_kx^0$ **of B and:**

(a) **If $k > 0$:**

- i. Make a $k \times k$ matrix C .
- ii. Let C 's first $k-1$ columns be filled with the last $k-1$ columns of I_k .
- iii. Let C 's last column from top to bottom be $-p_k, -p_{k-1}, \dots, -p_1$.
- iv. Add k columns filled with zeros to the right end of E .
- v. Add k rows filled with zeros to the bottom end of E .
- vi. Set the bottom-right corner of E equal to C .
- vii. Let the matrix $D = xI_k - C$ be our working matrix.
- viii. For $i = k$ going down to $i = 2$, add x times row i to row $i-1$.
- ix. Verify that D 's first $k-1$ columns are now the last $k-1$ columns of $-I_k$.
- x. Verify that D 's last column is p followed by some other polynomials.
- xi. For $i = 2$ going up to $i = k$, subtract $D_{i,k}$ times column $i-1$ from column k .
- xii. Verify that D 's last column is now p followed by zeros.
- xiii. For $i = 2$ going up to $i = k$, negate row $i-1$ and exchange it with row i using [algorithm 27](#).
- xiv. Verify that D is now a diagonal matrix whose first $k-1$ diagonal entries are 1 and whose last diagonal entry is p .
- xv. Add k columns filled with zeros to the right end of F .
- xvi. Add k rows filled with zeros to the bottom end of F .
- xvii. Set the bottom-right corner of F equal to D .

(b) Otherwise if $k = 0$, then do the following:

- i. Verify that p is monic.

ii. Verify that $p = 1$.

(c) Otherwise do the following:

i. **Abort algorithm.**

5. Let the macro $[P]$ expand to "(if P , then yield 1, otherwise yield 0)".
6. Using [algorithm 8](#), verify that $\sum_{i=1}^{i=m} [\deg(B_{i,i}) > 0] \deg(B_{i,i}) = \sum_{i=1}^{i=m} [\deg(B_{i,i}) \geq 0] \deg(B_{i,i}) = \sum_{i=1}^{i=m} \deg(B_{i,i}) = \deg(\det(B)) = \deg(\det(xI_m - A)) = m$.
7. Therefore verify that E and F are $m \times m$ matrices.
8. **Based on operations (4aviii) to (4axiii), use row and column operations to transform $xI_m - E$ into F .**
9. **Yield the tuple $\langle E, F \rangle$.**

2.30 Algorithm 30

Choose a $\mathcal{M}_{m,m}(\mathbb{Q})$, A , and do the following:

1. Execute [algorithm 5](#) on the polynomial matrix $xI_m - A$ and let $\langle B, M_3^{-1}, N_3^{-1} \rangle$ be the result.
2. Verify that $M_3^{-1}(xI_m - A)N_3^{-1} = B$.
3. Execute [algorithm 6](#) on the polynomial matrix $xI_m - A$ and let $\langle M_3, B, N_3 \rangle$ be the result.
4. Verify that $xI_m - A = M_3BN_3$.
5. Using [algorithm 7](#), verify that $M_3M_3^{-1} = I_m$.
6. Using [algorithm 7](#), verify that $N_3^{-1}N_3 = I_m$.
7. Augment (9) in an analogous way to how [algorithm 5](#) augments [algorithm 3](#). Let $\langle F, M_1, N_1 \rangle$ receive the result once (9) has executed.
8. Augment (9) in an analogous way to how [algorithm 6](#) augments [algorithm 3](#). Let $\langle M_1^{-1}, F, N_1^{-1} \rangle$ receive the result once (9) has executed.
9. Execute [algorithm 29](#) on the matrix A and let $\langle E, F \rangle$ receive the result.
10. Verify that $M_1(xI_m - E)N_1 = F$.
11. Using [algorithm 7](#), verify that $M_1M_1^{-1} = I_m$.
12. Using [algorithm 7](#), verify that $N_1^{-1}N_1 = I_m$.

13. Augment (18) in an analogous way to how **algorithm 5** augments **algorithm 3**. Let $\langle B, M_2, N_2 \rangle$ receive the result once (18) has executed.
14. Augment (18) in an analogous way to how **algorithm 6** augments **algorithm 3**. Let $\langle M_2^{-1}, B, N_2^{-1} \rangle$ receive the result once (18) has executed.
15. Verify that F and B have the same positive degree polynomials on their diagonals.
16. Verify that the rest of the diagonals of F and B are 1s.
17. Verify that F is the same as B up to rearrangement of the diagonal entries.
18. Rearrange a copy of F to be B by using diagonal entry swaps. In general, swap the i^{th} and j^{th} diagonal entries as follows:
 - (a) Use **algorithm 27** to negate row i and swap it with row j .
 - (b) Use an algorithm analogous to **algorithm 27** to negate column i and swap it with column j .
19. Verify that $M_2 F N_2 = B$.
20. Using **algorithm 7**, verify that $M_2 M_2^{-1} = I_m$.
21. Using **algorithm 7**, verify that $N_2^{-1} N_2 = I_m$.
22. Let $M = M_3 M_2 M_1$.
23. Let $N = N_1 N_2 N_3$.
24. Verify that $xI_m - A = M_3 B N_3 = M_3 M_2 F N_2 N_3 = M_3 M_2 M_1 (xI_m - E) N_1 N_2 N_3 = M (xI_m - E) N$.
25. Let $M^{-1} = M_1^{-1} M_2^{-1} M_3^{-1}$.
26. Let $N^{-1} = N_3^{-1} N_2^{-1} N_1^{-1}$.
27. Verify that $MM^{-1} = M_3 M_2 M_1 M_1^{-1} M_2^{-1} M_3^{-1} = I_m$.
28. Verify that $N^{-1} N = N_3^{-1} N_2^{-1} N_1^{-1} N_1 N_2 N_3 = I_m$.
29. **Execute algorithm 26 on the matrices $\langle A, M, M^{-1}, E, N^{-1}, N \rangle$. Let the tuple $\langle R_1, R_3 \rangle$ be the result.**
30. Verify that $A = R_1 E R_3$.
31. Verify that $R_1 R_3 = I_m$.
32. **Yield the tuple $\langle R_1, E, R_3 \rangle$.**

2.31 Algorithm 31 (Block matrix multiplication)

Choose a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, A , and a $\mathcal{M}_{n,k}(\mathbb{Q}[x])$, B . Choose integers $1 \leq a \leq m$, $1 \leq b \leq n$, and $1 \leq c \leq k$. Now do the following:

1. Let C be the submatrix of A that spans rows 1 to $a-1$ and columns 1 to $b-1$.
2. Let D be the submatrix of A that spans rows 1 to $a-1$ and columns b to n .
3. Let E be the submatrix of B that spans rows 1 to $b-1$ and columns 1 to $c-1$.
4. Let F be the submatrix of B that spans rows b to n and columns 1 to $c-1$.
5. Multiply matrix A by matrix B .
6. For each $1 \leq i \leq a-1$, do the following:
 - (a) For each $1 \leq j \leq c-1$, do the following:
 - i. Verify that $(AB)_{i,j} = \sum_{p=1}^n A_{i,p} B_{p,j} = \sum_{p=1}^{b-1} A_{i,p} B_{p,j} + \sum_{p=b}^n A_{i,p} B_{p,j} = \sum_{p=1}^{b-1} C_{i,p} E_{p,j} + \sum_{p=1}^{1+n-b} D_{i,p} F_{p,j} = (CE)_{i,j} + (DF)_{i,j}$.
7. **Therefore verify that the top left $(a-1) \times (c-1)$ block of AB equals $CE + DF$.**
8. **Do similar computations to verify that the other three blocks of AB are computed in an analogous way to multiplying two 2×2 matrices.**

2.32 Algorithm 32

Choose a $\mathcal{M}_{m,m}(\mathbb{Q})$, A , and do the following:

1. Execute **algorithm 3** on the polynomial matrix $xI_m - A$ and let the tuple $\langle B \rangle$ receive the result.
2. Execute **algorithm 28** on A .
3. Let $r = x^t + r_1 x^{t-1} + r_2 x^{t-2} + \dots + r_t x^0 = B_{m,m}$.
4. Execute **algorithm 30** on the matrix A and let the tuple $\langle R_1, E, R_3 \rangle$ receive the result.
5. Verify that $R_1 R_3 = I_m$.
6. Therefore using **algorithm 25**, verify that $R_3 R_1 = I_m$.

7. Using [algorithm 30](#), verify that $r(A) = A^t + r_1 A^{t-1} + r_2 A^{t-2} + \dots + r_t A^0 = (R_1 E R_3)^t + r_1 (R_1 E R_3)^{t-1} + r_2 (R_1 E R_3)^{t-2} + \dots + r_t (R_1 E R_3)^0 = R_1 (E^t + r_1 E^{t-1} + r_2 E^{t-2} + \dots + r_t E^0) R_3 = R_1 r(E) R_3$.
8. For $i = 0$ up to $i = t$, by repeated applications of [algorithm 31](#), verify that E^i evaluates to E with all its diagonal blocks exponentiated to i .
9. Therefore verify that $r(E)$ evaluates to $m \times m$ matrix whose diagonal blocks are the application of r on the corresponding diagonal blocks of E .
10. For $j = 1$ to $j = m$:
 - (a) If $\deg(B_{j,j}) > 0$, then do the following:
 - (b) Let $p = x^k + p_1 x^{k-1} + p_2 x^{k-2} + \dots + p_k x^0 = B_{j,j}$.
 - (c) Let G be the corresponding $k \times k$ block on the diagonal of E .
 - (d) Let e_i denote a $k \times 1$ matrix that is 0, except for its i^{th} entry which is 1.
 - (e) Then by G 's construction, for $i = 1$ up to $i = k$, verify that $G^{i-1} e_1 = G^{i-2} e_2 = \dots = G^0 e_i = e_i$.
 - (f) Let $0_{m \times n}$ denote an $m \times n$ matrix of zeros.
 - (g) Therefore, for $i = 1$ up to $i = k$: Cognizant of the construction of G 's last column, verify that $p(G) e_i = (G^k + p_1 G^{k-1} + p_2 G^{k-2} + \dots + p_k G^0) e_i = (G^k + p_1 G^{k-1} + p_2 G^{k-2} + \dots + p_k G^0) G^{i-1} e_1 = G^{i-1} (G G^{k-1} + p_1 G^{k-1} + p_2 G^{k-2} + \dots + p_k G^0) e_1 = G^{i-1} (G e_k + p_1 e_k + p_2 e_{k-1} + \dots + p_k e_1) = G^{i-1} 0_{k \times 1} = 0_{k \times 1}$.
 - (h) Therefore verify that $p(G) = 0_{k \times k}$.
 - (i) Cognizant of the execution of [algorithm 3](#) in (1), verify that $r = B_{m,m} = B_{j,j} u_{j+1} u_{j+2} \dots u_m = B_{j,j} q = pq$, where $q = u_{j+1} u_{j+2} \dots u_m$.
 - (j) Therefore verify that $r(G) = p(G) q(G) = 0_{k \times k} q(G) = 0_{k \times k}$.
11. Therefore verify that the diagonal blocks of $r(E)$ each equal $0_{i \times i}$, where i is the size of each diagonal block.
12. Therefore verify that $r(E) = 0_{m \times m}$.
13. Therefore verify that $r(A) = R_1 r(E) R_3 = R_1 0_{m \times m} R_3 = 0_{m \times m}$.

2.33 Algorithm 33

Choose a $\mathcal{M}_{m,m}(\mathbb{Q})$, A . Choose a $\mathbb{Q}[x]$ $p = p_0 x^t + p_1 x^{t-1} + p_2 x^{t-2} + \dots + p_t x^0$ where $p_0 \neq 0$, such that $p(A) = 0$.

1. Execute [algorithm 3](#) on the polynomial matrix $xI_m - A$ and let the tuple $\langle B \rangle$ receive the result.
2. Execute [algorithm 28](#) on A .
3. Let $r = x^u + r_1 x^{u-1} + r_2 x^{u-2} + \dots + r_u x^0 = B_{m,m}$.
4. Execute [algorithm 30](#) on the matrix A and let the tuple $\langle R_1, E, R_3 \rangle$ receive the result.
5. Let F be a 1×2 matrix consisting in-order of p and r .
6. Execute [algorithm 5](#) on F and let $\langle D, M, N \rangle$ receive the result.
7. Execute [algorithm 6](#) on F and let $\langle M^{-1}, D, N^{-1} \rangle$ receive the result.
8. Let $g = x^w + g_1 x^{w-1} + g_2 x^{w-2} + \dots + g_w x^0 = D_{1,1}$.
9. If $\deg(p) \neq \deg(r)$, do the following:
 - (a) Verify that the execution of the inner [algorithm 1](#) begun with repeated executions of (2c) to bring the degree of the higher degree polynomial down to that of the lower.
 - (b) Verify that afterwards, each iteration of (2) lowered the degree of either entry.
10. Therefore verify that $\deg(g) \leq \min(\deg(p), \deg(r))$.
11. Therefore verify that $w \leq u$.
12. Verify that $D = MFN$.
13. Therefore verify that $g = D_{1,1} = N_{1,1} p + N_{2,1} r$.
14. Therefore using [algorithm 32](#), verify that $g(A) = N_{1,1}(A) p(A) + N_{2,1}(A) r(A) = N_{1,1}(A) 0_{m \times m} + N_{2,1}(A) 0_{m \times m} = 0_{m \times m}$.
15. Using steps of [algorithm 32](#), [algorithm 25](#), and [algorithm 30](#), verify that $g(E) = I_m g(E) I_m = R_3 R_1 g(E) R_3 R_1 = R_3 g(A) R_1 = R_3 0_{m \times m} R_1 = 0_{m \times m}$.

16. Let G be the $u \times u$ block in E corresponding to the polynomial r in B .
17. Using steps of **algorithm 32**, verify that $g(G) = 0_{u \times u}$.
18. Therefore verify, using steps of **algorithm 32**, that $g(G)e_1 = (G^w + g_1G^{w-1} + g_2G^{w-2} + \dots + g_wG^0)e_1 = Ge_w + g_1e_w + g_2e_{w-1} + \dots + g_we_1$.
19. If $w < u$, then:
 - (a) Verify that $Ge_w + g_1e_w + g_2e_{w-1} + \dots + g_we_1 = e_{w+1} + g_1e_w + g_2e_{w-1} + \dots + g_we_1 = 0_{u \times 1}$.
 - (b) Therefore verify that $1 = 0$.
 - (c) **Abort algorithm.**
20. Otherwise, do the following:
 - (a) Verify that $w = u$.
 - (b) Verify that $Ge_w + g_1e_w + g_2e_{w-1} + \dots + g_we_1 = Ge_u + g_1e_u + g_2e_{u-1} + \dots + g_ue_1 = 0_{u \times 1}$.
 - (c) Therefore for $i = 1$ to $i = u$, do the following:
 - i. Verify that $-r_i + g_i = 0$.
 - ii. Therefore verify that $g_i = r_i$.
 - (d) **Therefore verify that $g = r$.**
 - (e) Verify that $F = M^{-1}DN^{-1}$.
 - (f) **Therefore verify that $p = F_{1,1} = D_{1,1}N^{-1}_{1,1} + D_{1,2}N^{-1}_{2,1} = N^{-1}_{1,1}g + N^{-1}_{2,1} * 0 = N^{-1}_{1,1}g = N^{-1}_{1,1}r$.**

2.34 Algorithm 34 (Difference of powers)

Choose an integer $n \geq 0$ and a $\mathbb{Q}[x]$ $p = p_0x^n + p_1x^{n-1} + \dots + p_n$.

1. Let the $\mathbb{Q}[y, z]$ $G(y, z) = \sum_{r=1}^n p_{n-r}(z^{r-1} + z^{r-2}y + \dots + zy^{r-2} + y^{r-1})$.
2. **Verify that the $\mathbb{Q}[y, z]$ $p(z) - p(y) = (p_0z^n + p_1z^{n-1} + \dots + p_n) - (p_0y^n + p_1y^{n-1} + \dots + p_n) = (\sum_{r=0}^n p_{n-r}z^r) - (\sum_{r=0}^n p_{n-r}y^r) = \sum_{r=1}^n p_{n-r}(z^r - y^r) = \sum_{r=1}^n p_{n-r}(z - y)(z^{r-1} + z^{r-2}y + \dots + zy^{r-2} + y^{r-1}) = (z - y) \sum_{r=1}^n p_{n-r}(z^{r-1} + z^{r-2}y + \dots + zy^{r-2} + y^{r-1}) = (z - y)G(y, z)$.**

3. **Yield the tuple $\langle G(y, z) \rangle$.**

2.35 Algorithm 35

Choose a $\mathbb{Q}[x]$ $p = x^n + p_1x^{n-1} + \dots + p_n$ and \mathbb{Q} s $a_1 < a_2 < \dots < a_n < a_{n+1}$ in such a way that for $i = 1$ to $i = n + 1$, $p(a_i) = 0$. Now do the following:

1. Write p as $1 * p$, so that it has two factors.
2. For $i = 1$ up to $i = n$, do the following:
 - (a) Let g be the rightmost factor of p .
 - (b) If $g(a_i) \neq 0$, do the following:
 - i. For $k = 1$ to $k = i - 1$, verify that $(a_i - a_k) \neq 0$.
 - ii. Verify that $p(a_i) \neq 0$.
 - iii. **Abort algorithm.**
 - (c) Otherwise $g(a_i) = 0$. Now do the following:
 - i. Execute **algorithm 34** on g and let the tuple $\langle G(x, y) \rangle$ receive the result.
 - ii. Let the $\mathbb{Q}[x]$ $q = q(x) = G(a_i, x)$.
 - iii. Verify that the $\mathbb{Q}[x]$ $g = g(x) = g(x) - g(a_i) = (x - a_i)G(a_i, x) = (x - a_i)q(x) = (x - a_i)q$.
 - iv. Verify that $p = (x - a_1)(x - a_2) \dots (x - a_i)q$.
3. Now verify that $p = (x - a_1)(x - a_2) \dots (x - a_n)1$.
4. Using (3), verify that $p(a_{n+1}) \neq 0$.
5. **Abort algorithm.**

2.36 Algorithm 36 (Bisection)

Choose a $\mathbb{Q}[x]$ f . Choose \mathbb{Q} s $a < b$ such that $\text{sgn}(f(a)) = -\text{sgn}(f(b))$. Choose a rational number target $B > 0$. Now do the following:

1. Execute **algorithm 34** on f and let the tuple $\langle G(x, y) \rangle$ receive the result.
2. Verify that the $\mathbb{Q}[x, y]$ $f(y) - f(x) = (y - x)G(x, y)$.
3. Let G' be G but with all negative signs replaced with positive signs.
4. Let $U = G'(|a|, |b|)$.

5. Until $|b - a|U < B$
 - (a) Let $c = \frac{a+b}{2}$.
 - (b) If $\text{sgn}(f(a)) = -\text{sgn}(f(c))$, then:
 - i. Let $b = c$.
 - (c) Otherwise if $\text{sgn}(f(c)) = -\text{sgn}(f(b))$, then:
 - i. Let $a = c$.
 - (d) Otherwise if $f(c) = 0$, then do the following:
 - i. Record the rational number c .
 - ii. If less than or equal to i rational numbers have been recorded, then:
 - A. Let $a = c$.
 - B. Go to (1bi).
 - iii. Otherwise, do the following:
 - A. Let $c_1 < c_2 < \dots < c_i < c_{i+1}$ be the $i + 1$ numbers that were recorded.
 - B. Execute **algorithm 35** on the polynomial f_i and the rationals $c_1 < c_2 < \dots < c_i < c_{i+1}$.
- C. **Abort algorithm.**
- (e) Otherwise, do the following:
 - i. Verify that $f(a) \not\leq 0$.
 - ii. Verify that $f(a) \neq 0$.
 - iii. Verify that $f(a) \not\geq 0$.
 - iv. **Abort algorithm.**
6. **Verify that** $|f(a)|, |f(b)| < |f(b) - f(a)| = |(b - a)G(a, b)| < |(b - a)G'(|a|, |b|)| = |b - a|U < B$.
7. **Yield the tuple** $\langle a, b \rangle$.

2.37 Algorithm 37

Choose a $\mathbb{Q}[x]$ $f_n = x^n + p_1x^{n-1} + \dots + p_n$ **and pairs of** \mathbb{Q} s $(a_n, b_n), (a_{n-1}, b_{n-1}), \dots, (a_0, b_0)$ **in such a way that:**

1. $a_n < b_n \leq a_{n-1} < b_{n-1} \leq \dots \leq a_1 < b_1 \leq a_0 < b_0$.
2. **For** $i = 0$ **to** $i = n$, $\text{sgn}(f_n(a_i)) = -\text{sgn}(f_n(b_i))$.

Now do the following:

1. **For** $i = n$ **to** $i = 1$:
 - (a) Let $B = \min_{k=0}^{i-1} \min(|f_i(a_k)|, |f_i(b_k)|)$.
 - (b) **For** $k = 0$ **to** $k = i - 1$, verify that $|f_i(a_k)| \geq B$.
 - (c) Execute **algorithm 36** on the formal polynomial f_i , interval (a_i, b_i) , and target of B . Let the tuple $\langle a_i, b_i \rangle$ receive the result.
 - (d) Verify that $|f_i(b_i)| < B$.
 - (e) Execute **algorithm 34** on the formal polynomial f_i and let the tuple $\langle G_{i-1}(x, y) \rangle$ receive the result.
 - (f) Let the formal polynomial $f_{i-1} = f_{i-1}(x) = G_{i-1}(b_i, x)$.
 - (g) Verify that f_{i-1} is a monic $(i - 1)^{\text{th}}$ degree formal polynomial.
 - (h) Verify that the formal polynomial $f_i = f_i(x) = f_i(x) - f_i(b_i) + f_i(b_i) = (x - b_i)G_{i-1}(b_i, x) + f_i(b_i) = (x - b_i)f_{i-1}(x) + f_i(b_i) = (x - b_i)f_{i-1} + f_i(b_i)$.
 - (i) **For** $k = 0$ **to** $k = i - 1$, do the following:
 - i. If $f_i(a_k) \geq B$, in-order verify that:
 - A. $f_i(a_k) \geq B > |f_i(b_i)| \geq f_i(b_i)$.
 - B. $f_i(a_k) - f_i(b_i) > 0$.
 - C. $(a_k - b_i)f_{i-1}(a_k) > 0$.
 - D. $f_{i-1}(a_k) > 0$.
 - E. $f_i(b_k) \leq -B < -|f_i(b_i)| \leq f_i(b_i)$.
 - F. $f_i(b_k) - f_i(b_i) < 0$.
 - G. $(b_k - b_i)f_{i-1}(b_k) < 0$.
 - H. $f_{i-1}(b_k) < 0$.
 - ii. Otherwise, if $f_i(a_k) \leq -B$, do the following:
 - A. Using steps similar to (1ii), verify that $f_{i-1}(a_k) < 0$.
 - B. Using steps similar to (1ii), verify that $f_{i-1}(b_k) > 0$.
2. Using (1g), verify that $f_0 = 1$.
3. Using (1iiD) and (1iiH) or (1iiiA) and (1iiiB), verify that $\text{sgn}(f_0(a_0)) = -\text{sgn}(f_0(b_0))$.
4. Therefore verify that $\text{sgn}(1) = -\text{sgn}(1)$.

5. Therefore verify that $1 = -1$.
6. **Abort algorithm.**

2.38 Algorithm 38 (Sturm's algorithm initialization)

Choose a sequence of $\mathbb{Q}[x]$ s $s_0 = s_{00}, s_1 = s_{10}x^1 + s_{11}, \dots, s_m = s_{m0}x^m + s_{m1}x^{m-1} + \dots + s_{mm}$ and another sequence of $\mathbb{Q}[x]$ s q_1, q_2, \dots, q_{m-1} in such a way that

1. For $i = 0$ to $i = m$, $s_{i0} > 0$
2. For $i = 1$ to $i = m - 1$, $s_{i-1} + s_{i+1} = q_i s_i$.

Now do the following:

1. Let $J_i(x)$ be a shorthand for the number of sign changes in the sequence $s_0(x), s_1(x), \dots, s_i(x)$.
2. For $i = 0$ to $i = m$, do the following:
 - (a) Execute **algorithm 34** on s_i and let $\langle G_i(x, y) \rangle$ receive the result.
 - (b) **Verify that the** $\mathbb{Q}[x, y]$ $s_i(y) - s_i(x) = (y - x)G_i(x, y)$.
3. For $i = 1$ to $i = m - 1$, do the following:
 - (a) Verify that $q_i s_i - s_{i+1} = s_{i-1}$.
 - (b) Let H_i be the equation $q_i s_i - s_{i+1} = s_{i-1}$.
 - (c) If $i > 1$, do the following:
 - i. Let Q_i be the result of:
 - A. Substituting the equation H_i into the equation H_{i-1} through s_{i-1} .
 - B. Distributing out the cofactor of H_i over H_i within Q_i .
 - C. Factoring the term s_i out of the two terms now containing it within Q_i .
 - ii. Let H_i be Q_i .
 - (d) Verify that H_i is of the form $ps_i + qs_{i+1} = s_0$ where p and q are some polynomials.
 - (e) Let $g_i = \frac{p}{s_0}$.
 - (f) Let $h_i = \frac{q}{s_0}$.
 - (g) **Verify that** $g_i s_{i+1} + h_i s_i = 1$.

2.39 Algorithm 39 (Change in number of sign changes verification)

1. Execute **algorithm 38**.
2. Choose \mathbb{Q} s c and d in such a way that:
 - (a) $J_m(c)$ and $J_m(d)$ are well defined.
 - (b) Letting $B = \max_{i=1}^m |G_i(c, d)|$.
 - (c) Letting $C = \max_{i=1}^{m-1} \max(|g_i(c)|, |h_i(c)|, |g_i(d)|, |h_i(d)|)$.
 - (d) Letting $D = \max_{i=1}^{m-1} \max(|q_i(c)|, |q_i(d)|, 2)$.
 - (e) $|d - c| < \frac{1}{BCD}$.
3. Let $i = 0$.
4. Do the following:
 - (a) Verify that $\text{sgn}(s_i(c)) = \text{sgn}(s_i(d))$.
 - (b) Verify that $J_i(c) = J_i(d)$.
 - (c) If $\text{sgn}(s_{i+1}(c)) = \text{sgn}(s_{i+1}(d))$, do the following:
 - i. Verify that $J_{i+1}(c) = J_{i+1}(d)$.
 - ii. Set i to $i + 1$ and go to (4) if the new $i < m$.
 - (d) Otherwise, if $\text{sgn}(s_{i+1}(c)) \neq \text{sgn}(s_{i+1}(d))$ and $i + 2 \leq m$, verify the following:
 - i. $|s_{i+1}(c)| < |s_{i+1}(c) - s_{i+1}(d)| = |c - d||G_{i+1}(c, d)| < |c - d|B < lB = \frac{1}{CD}$
 - ii. $|s_{i+1}(d)| < \frac{1}{CD}$
 - iii. $1 = g_{i+1}(c)s_{i+2}(c) + h_{i+1}(c)s_{i+1}(c) = |g_{i+1}(c)s_{i+2}(c) + h_{i+1}(c)s_{i+1}(c)| \leq |g_{i+1}(c)||s_{i+2}(c)| + |h_{i+1}(c)||s_{i+1}(c)| < C(|s_{i+2}(c)| + \frac{1}{CD})$
 - iv. $\frac{1}{C}(1 - \frac{1}{D}) < |s_{i+2}(c)|$
 - v. $\frac{1}{C}(1 - \frac{1}{D}) < |s_{i+2}(d)|$
 - vi. If $\text{sgn}(s_{i+2}(c)) \neq \text{sgn}(s_{i+2}(d))$, do the following:
 - A. Verify that $|s_{i+2}(c)| < \frac{1}{CD} = \frac{1}{C} \cdot \frac{1}{D} < \frac{1}{C}(1 - \frac{1}{D})$.
 - B. Verify that $\frac{1}{C}(1 - \frac{1}{D}) < \frac{1}{C}(1 - \frac{1}{D})$.
- Abort algorithm.**

vii. Otherwise if $\text{sgn}(s_i(c)) = \text{sgn}(s_{i+2}(c))$, do the following:

A. Verify that $2\frac{1}{C}(1 - \frac{1}{D}) \leq |s_i(c)| + |s_{i+2}(c)| = |s_i(c) + s_{i+2}(c)| = |q_{i+1}(c)s_{i+1}(c)| < D\frac{1}{CD}$.

B. Verify that $2(1 - \frac{1}{D}) < 1$.

C. Verify that $D < 2$.

D. Verify that $2 < 3$.

E. **Abort algorithm.**

viii. Otherwise, do the following:

A. Verify that $\text{sgn}(s_{i+2}(c)) = \text{sgn}(s_{i+2}(d))$.

B. Verify that $\text{sgn}(s_i(c)) \neq \text{sgn}(s_{i+2}(c))$.

C. Verify that $J_{i+2}(c) = J_{i+2}(d)$.

D. Set i to $i + 2$ and go to (4).

(e) Otherwise, verify the following:

i. $\text{sgn}(s_{i+1}(c)) \neq \text{sgn}(s_{i+1}(d))$.

ii. $i + 1 = m$

iii. $|s_{i+1}(c)| < \frac{1}{CD}$.

iv. $|s_{i+1}(d)| < \frac{1}{CD}$.

v. $|J_{i+1}(c) - J_{i+1}(d)| = 1$.

5. If $\text{sgn}(s_m(c)) = \text{sgn}(s_m(d))$, then do the following:

(a) Verify that $J_m(c) = J_m(d)$.

6. Otherwise do the following:

(a) Verify that $|J_m(d) - J_m(c)| = 1$.

2.40 Algorithm 40 (Cauchy's positive verification)

Choose a $\mathbb{Q}[x]$ $p = p_0x^t + p_1x^{t-1} + p_2x^{t-2} + \dots + p_tx^0$, where $p_0 > 0$. Choose a \mathbb{Q} $k > 1 + \max_{i=1}^t |\frac{p_i}{p_0}|$. In reverse order verify the following:

1. $p(k) > 0$
2. $p_0k^n + p_1k^{n-1} + \dots + p_nk^0 > 0$
3. $k^n + \frac{p_1}{p_0}k^{n-1} + \dots + \frac{p_n}{p_0}k^0 > 0$
4. $k^n > -(\frac{p_1}{p_0}k^{n-1} + \dots + \frac{p_n}{p_0}k^0)$

$$5. k^n > |\frac{p_1}{p_0}k^{n-1} + \dots + \frac{p_n}{p_0}k^0|$$

$$6. k^n > |\max_{i=1}^t |\frac{p_i}{p_0}| (k^{n-1} + \dots + k^0)|$$

$$7. k^n > \max_{i=1}^t |\frac{p_i}{p_0}| \frac{k^n - 1}{k - 1}$$

$$8. k^{n+1} - k^n > \max_{i=1}^t |\frac{p_i}{p_0}| (k^n - 1)$$

$$9. k^{n+1} - (1 + \max_{i=1}^t |\frac{p_i}{p_0}|)k^n + \max_{i=1}^t |\frac{p_i}{p_0}| > 0$$

$$10. k > 1 + \max_{i=1}^t |\frac{p_i}{p_0}|$$

2.41 Algorithm 41 (Cauchy's alternation verification)

Choose a $\mathbb{Q}[x]$ $p = p_0x^t + p_1x^{t-1} + p_2x^{t-2} + \dots + p_tx^0$, where $p_0 > 0$. Choose a \mathbb{Q} $k < -(1 + \max_{i=1}^t |\frac{p_i}{p_0}|)$. Now do the following:

1. Let $q = q_0x^t + q_1x^{t-1} + q_2x^{t-2} + \dots + q_tx^0$, where $q_i = (-1)^i p_i$.
2. Verify that $k < -(1 + \max_{i=1}^t |\frac{q_i}{q_0}|)$.
3. Therefore verify that $-k > 1 + \max_{i=1}^t |\frac{q_i}{q_0}|$.
4. Execute [algorithm 40](#) on q and $-k$.
5. **Therefore, verify that** $(-1)^t p(k) = (-1)^t \sum_{i=0}^t p_i k^{t-i} = \sum_{i=0}^t (-1)^i (-1)^{t-i} p_i k^{t-i} = \sum_{i=0}^t q_i (-k)^{t-i} = q(-k) > 0$.

2.42 Algorithm 42 (Sturm's sign change)

1. Execute [algorithm 38](#).

2. Let $U = 1 + \max_{i=0}^m \left(1 + \max_{j=1}^i |\frac{s_{i,j}}{s_{i,0}}|\right)$

3. Using [algorithm 40](#), verify that $J(U) = 0$.

4. Using [algorithm 41](#), verify that $J(-U) = m$.

5. For $i = 1$ to $i = m$, do the following:

(a) Let $G'_i(x, y)$ be $G_i(x, y)$ with all negative signs replaced with positive signs.

6. Let the rational $B = \max_{i=1}^m G'_i(U, U)$.

7. For $i = 1$ to $i = m - 1$, do the following:

(a) Let the polynomial g'_i be g_i with all negative signs replaced with positive signs.

(b) Let the polynomial h'_i be h_i with all negative signs replaced with positive signs.

- (c) Let the polynomial q'_i be q_i with all negative signs replaced with positive signs.
- 8. Let $C = \max_{i=1}^m \max(g'_i(U), h'_i(U))$.
- 9. Let $D = \max(3, \max_{i=1}^m q'_i(U))$
- 10. Let $l = \frac{1}{BCD}$.
- 11. Let $c = -U$.
- 12. Do the following:
 - (a) If $c + l \leq U$, then do the following:
 - i. Choose a number d in a way such that $c < d < c + l$ and $J(d)$ is well-defined.
 - (b) Otherwise do the following:
 - i. Let $d = U$.
 - (c) Execute **algorithm 39**.
 - (d) **If $J_m(c) \neq J_m(d)$, then record the pair of rational numbers (c, d) .**
 - (e) If the $d \neq U$, then do the following:
 - i. Let $c = d$.
 - ii. Go to (12).
- 13. If less than m pairs of rational numbers were recorded, then do the following:
 - (a) Verify that each change of $J_m(x)$ over the course of (12) was by 1.
 - (b) Verify that $J_m(x)$ changed less than m times over the course of (12).
 - (c) Therefore verify that $|J_m(U) - J_m(-U)| < m$.
 - (d) Therefore verify that $m < m$.
 - (e) **Abort algorithm.**
- 14. If more than m pairs of rational numbers were recorded, then verify the following:
 - (a) Execute **algorithm 37** on the formal polynomial $s_m(x)$ along with the first $m + 1$ recorded pairs.
 - (b) **Abort algorithm.**
- 15. **Otherwise, do the following:**
 - (a) **Verify that exactly m pairs of rational numbers $(c_1, d_1), (c_2, d_2), \dots, (c_m, d_m)$ were recorded.**

- (b) **Verify that $c_1 < d_1 \leq c_2 < d_2 \leq \dots \leq c_m < d_m$.**
- (c) **For $i = 1$ to $i = m$, do the following:**
 - i. **Verify that $\text{sgn}(s_m(c_i)) = -\text{sgn}(s_m(d_i))$.**
- (d) **Yield the tuple $\langle c_1, d_1, c_2, d_2, \dots, c_m, d_m \rangle$.**

2.43 Algorithm 43

Choose a $\mathcal{M}_{m,m}(\mathbb{Q})$, A . Execute **algorithm 3 on the polynomial matrix $xI_m - A$ and let the tuple $\langle B \rangle$ receive the result. Choose a $\mathbb{Q}[x]$ p such that $p(A) = 0$ and $\deg(p) < \deg(B_{m,m})$. Now do the following:**

1. Execute **algorithm 33** on matrix A and polynomial p .
2. Cognizant of steps (8) to (10) of **algorithm 33**, verify for **algorithm 33**'s g that $\deg(g) \leq \deg(B_{m,m}) - 1$.
3. Cognizant of step (20d) of **algorithm 33**, verify that $B_{m,m} = g$.
4. Therefore verify that $\deg(B_{m,m}) = \deg(g) \leq \deg(B_{m,m}) - 1$.
5. Therefore verify that $0 \leq -1$.
6. **Abort algorithm.**

2.44 Algorithm 44

Choose a $\mathcal{M}_{m,m}(\mathbb{Q})$, A , and do the following:

1. Execute **algorithm 3** on the polynomial matrix $xI_m - A$ and let the tuple $\langle B \rangle$ receive the result.
2. Execute **algorithm 28** on A .
3. Let $r = x^t + r_1x^{t-1} + r_2x^{t-2} + \dots + r_tx^0 = B_{m,m}$.
4. Make an $m^2 \times t$ matrix, F , whose i^{th} column is the sequential concatenation of the columns of A^{t-i} .
5. Execute **algorithm 5** on F and let the tuple $\langle D, M, N \rangle$ receive the result.
6. Verify that $MFN = D$.
7. Execute **algorithm 6** on F and let the tuple $\langle M^{-1}, D, N^{-1} \rangle$ receive the result.

8. Verify that $F = M^{-1}DN^{-1}$.
9. Using **algorithm 7**, verify that $M^{-1}MFN = I_{m^2}FN = FN = M^{-1}D$.
10. If any column i of N , Ne_i , is equal to zero, then:
 - (a) Verify that $0_{t \times 1} = N^{-1}0_{t \times 1} = N^{-1}(Ne_i) = (N^{-1}N)e_i = I_te_i = e_i$.
 - (b) Therefore verify that $0=1$.
 - (c) **Abort algorithm.**
11. Otherwise if $C_t(D)_{1,1} = 0$, then:
 - (a) Verify that for some $1 \leq i \leq t$, $D_{i,i} = 0$.
 - (b) Therefore verify that $De_i = 0_{m^2}$.
 - (c) Therefore verify that $F(Ne_i) = (FN)e_i = (M^{-1}D)e_i = M^{-1}(De_i) = 0_{m^2}$.
 - (d) Therefore verify that $N_{1,i}A^{t-1} + N_{2,i}A^{t-2} + \dots + N_{t,i}A^0 = 0_{m \times m}$.
 - (e) Execute **algorithm 43** on matrix A and polynomial $p = N_{1,i}x^{t-1} + N_{2,i}x^{t-2} + \dots + N_{t,i}x^0$.
 - (f) **Abort algorithm.**
12. Otherwise, if any column i of $C_t(M^{-1})$, $C_t(M^{-1})e_i$, is equal to zero, then:
 - (a) Using **algorithm 18**, **algorithm 7**, and **algorithm 14**, verify that $0_{m^2 \times 1} = C_t(M)0_{m^2 \times 1} = C_t(M)(C_t(M^{-1})e_i) = (C_t(M)C_t(M^{-1}))e_i = C_t(MM^{-1})e_i = C_t(I_{m^2})e_i = I_{\binom{m^2}{t}}e_i = e_i$.
 - (b) Therefore verify that $0=1$.
 - (c) **Abort algorithm.**
13. Otherwise, if $C_t(N^{-1}) = 0$, then:
 - (a) Verify that $1 = C_t(I_t) = C_t(N^{-1}N) = C_t(N^{-1})C_t(N) = 0 * C_t(N) = 0$.
 - (b) **Abort algorithm.**
14. Otherwise, do the following:
 - (a) Verify that all columns of $C_t(M^{-1})$ are non-zero.
 - (b) Verify that $C_t(D)_{1,1} \neq 0$.
 - (c) Verify that $C_t(N^{-1}) \neq 0$.

$$\begin{aligned}
 \text{(d) Verify that } C_t(F) &= C_t(M^{-1}DN^{-1}) = \\
 &= C_t(M^{-1})C_t(D)C_t(N^{-1}) = \\
 &= C_t(M^{-1})C_t(D)_{1,1}e_1C_t(N^{-1}) = \\
 &= C_t(D)_{1,1}C_t(N^{-1})C_t(M^{-1})e_1 \neq 0_{\binom{m^2}{t} \times 1}.
 \end{aligned}$$

(e) **Yield** $\langle F \rangle$.

2.45 Algorithm 45

Choose a symmetric $\mathcal{M}_{m,m}(\mathbb{Q})$, A . Now do the following:

1. **Execute algorithm 44 on the matrix A and let the tuple $\langle F \rangle$ receive the result.**
2. Using **algorithm 23**, verify that $C_t(F^TF) = C_t(F^T)C_t(F) = C_t(F)^TC_t(F) = \|C_t(F)\|^2 > 0$.
3. Execute **algorithm 6** on F^TF and let the tuple $\langle M^{-1}, B, N^{-1} \rangle$ receive the result.
4. Verify that $F^TF = M^{-1}BN^{-1}$
5. If B has a zero on its diagonal, then:
 - (a) Verify that $C_t(F^TF) = C_t(M^{-1}BN^{-1}) = C_t(B) = 0$.
 - (b) Therefore verify that $0 > 0$.
 - (c) **Abort algorithm.**
6. Otherwise, do the following:
 - (a) Verify that B does not have a zero on its diagonal.
 - (b) Let $t = \deg(B_{m,m})$.
 - (c) Let $s_t = B_{m,m}$.
 - (d) Let $\text{tr}(X)$ be a shorthand for the sum of the diagonal entries of the square matrix X .
 - (e) Let $\text{mat}(p_1x^{t-1} + p_1x^{t-2} + \dots + p_t)$ be a shorthand for $p_1e_1 + p_2e_2 + \dots + p_te_t$.
 - (f) Let $\text{pol}(p_1e_1 + p_2e_2 + \dots + p_te_t)$ be a shorthand for $p_1x^{t-1} + p_1x^{t-2} + \dots + p_t$.
 - (g) Let $H = (F^TF) \setminus e_1$.
 - (h) Let $h = \text{pol}(H)$.
 - (i) Execute **algorithm 5** on a 1×2 matrix comprising s_t followed by h . Let the tuple $\langle D, M, N \rangle$ receive the result.

- (j) Execute **algorithm 6** on a 1×2 matrix comprising s_t followed by h . Let the tuple $\langle M^{-1}, D, N^{-1} \rangle$ receive the result.
- (k) Let $d = D_{1,1}$.
- (l) Verify that d is monic.
- (m) If $\deg(d) > 0$, then do the following:
 - i. Let $b = N^{-1}_{1,1}$.
 - ii. Let $c = N^{-1}_{1,2}$.
 - iii. Verify that $s_t = bd$.
 - iv. Verify that b is a monic polynomial with degree $z < t$.
 - v. Verify that $h = cd$.
 - vi. Let $u = x^{t-z-1}b$.
 - vii. Verify that $\text{tr}(u(A)h(A)) = \text{mat}(u)^T F^T F H = \text{mat}(u)^T F^T F ((F^T F) \setminus e_1) = \text{mat}(u)^T e_1 = \text{mat}(u)_{1,1} = 1$.
 - viii. Verify that $\text{tr}(u(A)h(A)) = \text{tr}(A^{z-1}b(A)c(A)d(A)) = \text{tr}(A^{z-1}c(A)b(A)d(A)) = \text{tr}(A^{z-1}c(A)s_t(A)) = \text{tr}(A^{z-1}c(A)0_{m \times m}) = \text{tr}(0_{m \times m}) = 0$.
 - ix. Therefore verify that $0=1$.
 - x. **Abort algorithm.**
- (n) Otherwise, do the following:
 - i. Verify that $d = 1$.
 - ii. Let $u = N_{1,1}$.
 - iii. Let $s_{t+1} = N_{2,1}$.
 - iv. **Verify that** $us_t + s_{t+1}h = 1$.
 - v. **Yield the tuple** $\langle u, s_t, s_{t+1}, h \rangle$.
- (d) Execute **algorithm 46** on the tuple $\langle e, b \rangle$. Let the tuple $\langle c, d \rangle$ receive the result.
- (e) Verify that $cb + d = e$.
- (f) Verify that $\deg(d) < \deg(b)$.
- (g) Therefore verify that $cb + d = a - yb$.
- (h) **Therefore verify that** $(y + c)b + d = a$.
- (i) **Also verify that** $\deg(d) < \deg(b)$.
- (j) **Now yield the tuple** $\langle y + c, d \rangle$.
- 2. Otherwise:
 - (a) **Verify that** $0 * b + a = a$.
 - (b) **Verify that** $\deg(a) < \deg(b)$.
 - (c) **Yield the tuple** $\langle 0, a \rangle$.

2.47 Algorithm 47 (Edwards' Sturm chain construction)

Choose a symmetric $\mathcal{M}_{m,m}(\mathbb{Q})$, A . Now do the following:

1. **Execute algorithm 45 on the matrix** A . **Let the tuple** $\langle u, s_t, s_{t+1}, h \rangle$ **receive the result.**
2. Execute **algorithm 46** on the tuple $\langle s_{t+1}, s_t \rangle$. Let the tuple $\langle q_t, s_{t-1} \rangle$ receive the result.
3. Verify that $s_{t+1} = q_t s_t + s_{t-1}$, where $\deg(s_{t-1}) < t$.
4. Therefore verify that $us_t + (q_t s_t + s_{t-1})h = 1$.
5. Therefore verify that $u(A)s_t(A) + (q_t(A)s_t(A) + s_{t-1}(A))h(A) = I_{m,m}$.
6. Therefore verify that $s_{t-1}(A)h(A) = I_{m,m}$.
7. Therefore verify that $s_{t-1,0} = \text{tr}(s_{t-1}(A)h(A)) = \text{tr}(I_{m,m}) = m > 0$.
8. For $i = t - 1$ down to $i = 1$, do the following:
 - (a) If $i < t - 1$, then do the following:
 - i. Verify that $s_i = p_1 s_{t-1} + j_1 s_t$ where $\deg(s_i) = i$, $s_{i0} > 0$, $\deg(p_1) = t - 1 - i$, and $\deg(j_1) = t - 2 - i$.
 - ii. Verify that $s_{i+1} = p_2 s_{t-1} + j_2 s_t$ where $\deg(s_{i+1}) = i$, $\deg(p_2) = t - 2 - i$, and $\deg(j_2) = t - 3 - i$.

2.46 Algorithm 46 (Euclidean division)

Choose two $\mathbb{Q}[x]$ s, $\langle a, b \rangle$, and do the following:

1. If $\deg(a) \geq \deg(b)$:
 - (a) Let $y = \frac{a's \text{ leading coefficient}}{b's \text{ leading coefficient}} x^{\deg(a) - \deg(b)}$
 - (b) Let $e = a - yb$.
 - (c) Verify that $\deg(e) < \deg(a)$.

- (b) Execute **algorithm 46** on the tuple $\langle -s_{i+1}, -s_i \rangle$. Let the tuple $\langle q_i, s_{i-1} \rangle$ receive the result.
- (c) Verify that $\deg(q_i) = 1$.
- (d) Verify that $q_{i0} = \frac{s_{i+10}}{s_{i0}}$.
- (e) Also verify that $-s_{i+1} = -q_i s_i + s_{i-1}$.
- (f) Therefore verify that $q_i s_i = s_{i+1} + s_{i-1}$.
- (g) Therefore verify that $q_i s_i - s_{i+1} = s_{i-1}$.
- (h) If $i < t - 1$, then do the following:
- i. Let $p_3 = q_i p_1 - p_2$.
 - ii. Verify that $\deg(p_3) = t - i$.
 - iii. Let $j_3 = q_i j_1 - j_2$.
 - iv. Verify that $\deg(j_3) = t - 1 - i$.
 - v. **Verify that** $s_{i-1} = q_i(p_1 s_{t-1} + j_1 s_t) - (p_2 s_{t-1} + j_2 s_t) = p_3 s_{t-1} + j_3 s_t$.
- (i) Otherwise do the following:
- i. Let $p_3 = q_{t-1}$.
 - ii. Verify that $\deg(p_3) = 1 = t - 1$.
 - iii. Let $j_3 = -1$.
 - iv. Verify that $\deg(j_3) = 0 = t - 1 - i$.
 - v. **Verify that** $s_{i-1} = s_{t-2} = q_{t-1} s_{t-1} - s_t = p_3 s_{t-1} + j_3 s_t$.
- (j) Therefore verify that $s_{i-1}(A) = p_3(A)s_{t-1}(A) + j_3(A)s_t(A) = p_3(A)s_{t-1}(A) + j_3(A)0_{m \times m} = p_3(A)s_{t-1}(A)$.
- (k) If $p_3(A) = 0$, then do the following:
- i. Execute **algorithm 43** on the matrix A and polynomial p_3 .
 - ii. **Abort algorithm.**
- (l) Otherwise, if $s_{i-1}(A) = 0_{m \times m}$, then do the following:
- i. Verify that $p_3(A)s_{t-1}(A)h(A) = s_{i-1}(A)h(A) = 0_{m \times m}h(A) = 0_{m \times m}$.
 - ii. Verify that $p_3(A)s_{t-1}(A)h(A) = p_3(A)I_{m,m} = p_3(A) \neq 0_{m \times m}$.
 - iii. **Abort algorithm.**
- (m) Otherwise if $s_{i-1}(A)h(A) = 0_{m \times m}$, then do the following:
- i. Verify that $s_{i-1}(A)h(A)s_{t-1}(A) = 0_{m \times m}s_{t-1}(A) = 0_{m \times m}$.
 - ii. Verify that $s_{i-1}(A)h(A)s_{t-1}(A) = s_{i-1}(A)I_{m,m} = s_{i-1}(A) \neq 0$.
 - iii. **Abort algorithm.**
- (n) Otherwise, do the following:
- i. Verify that $\deg(s_{i-1}) < i$.
 - ii. Execute the **auxilliary algorithm** on the tuple $(i - 1, s_{i-1})$.
 - iii. Now verify that $\text{tr}(s_{i-1}(A)^2 h(A)^2) = \frac{s_{i-10}}{s_{i0}}$.
 - iv. Verify that $s_{i-1}(A)h(A) \neq 0_{m \times m}$.
 - v. Therefore verify that $\text{tr}(s_{i-1}(A)^2 h(A)^2) = \text{tr}((s_{i-1}(A)h(A))^2) = \|s_{i-1}(A)h(A)\|^2 > 0$.
 - vi. Therefore verify that $\frac{s_{i-10}}{s_{i0}} > 0$.
 - vii. **Therefore verify that** $s_{i-10} > 0$.
9. Yield the tuple $\langle \langle s_0, s_1, \dots, s_t \rangle, \langle q_1, q_2, \dots, q_{t-1} \rangle \rangle$.

2.47.1 Auxilliary algorithm

Choose an integer $0 \leq k \leq t$ **such that polynomial** s_k **is defined.** **Choose a** $\mathbb{Q}[x]$ $g = g_0 x^k + g_1 x^{k-1} + \dots + g_k$.

1. If $k = t$, then verify that $\text{tr}(g(A)s_k(A)h(A)^2)$
 - (a) $= \text{tr}(g(A)s_t(A)h(A)^2)$.
 - (b) $= \text{tr}(g(A)0_{m \times m}h(A)^2)$.
 - (c) $= \text{tr}(0_{m \times m})$.
 - (d) $= 0$.
2. Otherwise if $k = t - 1$, then verify that $\text{tr}(g(A)s_k(A)h(A)^2)$
 - (a) $= \text{tr}(g(A)s_{t-1}(A)h(A)^2)$.
 - (b) $= \text{tr}(g(A)I_{m,m}h(A))$.
 - (c) $= \text{tr}(g(A)h(A))$.
 - (d) $= g_0$.

$$(e) = \frac{g_0}{s_{k+1_0}}.$$

3. Otherwise if $k < t - 1$, then do the following:

$$(a) \text{ Verify that } \text{tr}(g(A)s_k(A)h(A)^2) = \text{tr}(g(A)(q_{k+1}(A)s_{k+1}(A) + s_{k+2}(A))h(A)^2).$$

$$(b) \text{ Verify that } \text{tr}(g(A)s_k(A)h(A)^2) = \text{tr}(g(A)q_{k+1}(A)s_{k+1}(A)h(A)^2) + \text{tr}(g(A)s_{k+2}(A)h(A)^2).$$

(c) Verify that $\deg(gq) = k + 1$.

(d) Verify that $k + 1 < t$.

(e) Execute the **auxilliary algorithm** on the tuple $\langle k + 1, gq \rangle$.

(f) Cognizant of the execution of the **auxilliary algorithm**, verify that $\text{tr}((g(A)q_{k+1}(A))s_{k+1}(A)h(A)^2) = \frac{(s_{k+2_0}/s_{k+1_0})g_0}{s_{k+2_0}} = \frac{g_0}{s_{k+1_0}}.$

(g) Verify that $\deg(g) = k$.

(h) Execute the **auxilliary algorithm** on the tuple $\langle k + 2, g \rangle$.

(i) If $k + 2 < t$, then do the following:

i. Cognizant of the execution of the **auxilliary algorithm**, verify that $\text{tr}(g(A)s_{k+2}(A)h(A)^2) = \frac{0}{s_{k+2_0}} = 0.$

(j) Otherwise, do the following:

i. Verify that $k + 2 = t$.

ii. Cognizant of the execution of the **auxilliary algorithm**, verify that $\text{tr}(g(A)s_{k+2}(A)h(A)^2) = \text{tr}(g(A)s_t(A)h(A)^2) = 0.$

(k) **Therefore** **verify** **that** $\text{tr}(g(A)s_k(A)h(A)^2) = \frac{g_0}{s_{k+1_0}} + 0 = \frac{g_0}{s_{k+1_0}}.$

2.48 Algorithm 48

Choose a symmetric $\mathcal{M}_{m,m}(\mathbb{Q})$, A . Now do the following:

1. Execute **algorithm 3** on the polynomial matrix $xI_m - A$ and let the tuple $\langle D \rangle$ receive the result.
2. Verify that $D_{m,m} = u_1 u_2 \cdots u_m$.
3. Execute **algorithm 47** on the matrix A and let the tuple $\langle \langle s_0, s_1, \dots, s_t \rangle, \langle q_1, q_2, \dots, q_{t-1} \rangle \rangle$ receive the result.

4. Execute **algorithm 42** supplying the tuple $\langle \langle s_0, s_1, \dots, s_t \rangle, \langle q_1, q_2, \dots, q_{t-1} \rangle \rangle$. Let the tuple $\langle c_1, d_1, c_2, d_2, \dots, c_m, d_m \rangle$ receive the result.

5. For $i = 1$ to $i = t$ do the following:

(a) If $\text{sgn}(u_1(c_i)) = \text{sgn}(u_1(d_i)), \text{sgn}(u_2(c_i)) = \text{sgn}(u_2(d_i)), \dots, \text{sgn}(u_m(c_i)) = \text{sgn}(u_m(d_i))$, then do the following:

i. Verify that $\text{sgn}(u_1(c_i)) \text{sgn}(u_2(c_i)) \cdots \text{sgn}(u_m(c_i)) = \text{sgn}(u_1(d_i)) \text{sgn}(u_2(d_i)) \cdots \text{sgn}(u_m(d_i)).$

ii. Verify that $\text{sgn}(u_1(c_i)u_2(c_i) \cdots u_m(c_i)) = \text{sgn}(u_1(d_i)u_2(d_i) \cdots u_m(d_i)).$

iii. Verify that $\text{sgn}(s_t(c_i)) = \text{sgn}(s_t(d_i)).$

iv. **Abort algorithm.**

(b) Otherwise do the following:

i. Assign (c_i, d_i) to one of the u_j s for which $\text{sgn}(u_j(c_i)) = -\text{sgn}(u_j(d_i)).$

6. Let n_i be the number of pairs assigned to the polynomial u_i .

7. Verify that $\sum_{i=1}^m n_j = t$.

8. If for any $i = 1$ to $i = m$, $n_i > \deg(u_i)$, then do the following:

(a) Execute **algorithm 37** on the polynomial u_i along with $\deg(u_i) + 1$ of the rational number pairs assigned to it.

(b) **Abort algorithm.**

9. Otherwise if for any $i = 1$ to $i = m$, $n_i < \deg(u_i)$, then do the following:

(a) Verify that $\sum_{i=1}^m n_j < t$.

(b) Verify that $\sum_{i=1}^m n_j < \sum_{i=1}^m \deg(u_i).$

(c) **Abort algorithm.**

10. Otherwise if for any $i = 1$ to $i = m$, $n_i \neq \deg(u_i)$, then do the following:

(a) Verify that $n_i \neq \deg(u_i).$

(b) Verify that $n_i \not\leq \deg(u_i).$

(c) Verify that $n_i \not\geq \deg(u_i).$

(d) **Abort algorithm.**

11. **For all** $i = 1$ **to** $i = m$, **verify that** $n_i = \deg(u_i).$

2.49 Algorithm 49 (Upper triangular matrix multiplication)

Choose two upper triangular $\mathcal{M}_{m,m}(\mathbb{Q}[x])$ s, A and B . Now do the following:

1. Multiply A by B and let C be the result.
2. For $i = 1$ to $i = m$, do the following:
 - (a) **Verify that** $C_{i,i} = \sum_{k=1}^m (A_{i,k} B_{k,i}) = \sum_{k=1}^{i-1} (A_{i,k} B_{k,i}) + A_{i,i} B_{i,i} + \sum_{k=i+1}^m (A_{i,k} B_{k,i}) = \sum_{k=1}^{i-1} (0 * B_{k,i}) + A_{i,i} B_{i,i} + \sum_{k=i+1}^m (A_{i,k} * 0) = A_{i,i} B_{i,i}$.
3. For $i = 2$ to $i = m$, do the following:
 - (a) For $j = 1$ to $j = i - 1$, do the following:
 - i. Verify that $C_{i,j} = \sum_{k=1}^m A_{i,k} B_{k,j} = \sum_{k=1}^{i-1} A_{i,k} B_{k,j} + \sum_{k=i}^m A_{i,k} B_{k,j} = \sum_{k=1}^{i-1} 0 * B_{k,j} + \sum_{k=i}^m A_{i,k} * 0 = 0$.
4. **Therefore verify that C is upper triangular.**

2.50 Algorithm 50 (Orthogonalization)

Choose integers $m \geq n \geq 0$. Choose a $\mathcal{M}_{n,m}(\mathbb{Q}[x])$, M , and a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, A_0 , such that $MA_0 = I_n$. Now do the following:

1. Using [algorithm 8](#), verify that $C_n(M_0 A_0) = C_n(I_n) = 1$.
2. If $C_n(A_0) = 0_{\binom{m}{n} \times 1}$, then do the following:
 - (a) Verify that $C_n(M_0 A_0) = C_n(M_0) C_n(A_0) = C_n(M_0) 0_{\binom{m}{n} \times 1} = 0$.
 - (b) **Abort algorithm.**
3. Otherwise, do the following:
4. Verify that $C_n(A_0) \neq 0_{\binom{m}{n} \times 1}$.
5. For $i = 1$ to $i = n$, do the following:
 - (a) If $A_{i-1} e_i = 0_{m \times 1}$, then do the following:
 - i. Verify that $C_n(A_{i-1}) = 0$.
 - ii. **Abort algorithm.**
 - (b) Otherwise, do the following:
 - (c) Verify that $\|A_{i-1} e_i\|^2 \neq 0$.

- (d) Let D_i be a $n \times n$ diagonal matrix comprising i 1s followed by $n - i$ $\|A_{i-1} e_i\|^2$ s.
- (e) **Verify that D_i is upper triangular.**
- (f) Verify that $C_n(D_i) = (\|A_{i-1} e_i\|^2)^{n-i} \neq 0$.
- (g) Let $N_i = I_n$ except that its i^{th} row is $i - 1$ 0s followed by a 1 followed by $-(A_{i-1}^T A_{i-1})_{i,i+1}$, then $-(A_{i-1}^T A_{i-1})_{i,i+2}$, all the way up to $-(A_{i-1}^T A_{i-1})_{i,n}$.
- (h) **Verify that N_i is upper triangular.**
- (i) Using [algorithm 8](#), verify that $C_n(N_i) = 1 \neq 0$.
- (j) Let $A_i = A_{i-1} D_i N_i$.
- (k) **Verify that** $C_n(A_i) = C_n(A_{i-1} D_i N_i) = C_n(A_{i-1}) C_n(D_i) C_n(N_i) = C_n(A_{i-1}) C_n(D_i) \neq 0$.
- (l) Verify that $A_{i-1}^T A_i = (A_{i-1}^T A_{i-1}) D_i N_i$ is a matrix with 0s from position $(i, i + 1)$ to (i, n) .
- (m) **Verify that** $A_i^T A_i = (A_{i-1} D_i N_i)^T (A_{i-1} D_i N_i) = N_i^T D_i^T (A_{i-1}^T A_{i-1}) D_i N_i$ **is a matrix with 0s from position $(i, i + 1)$ to (i, n) and from position $(i + 1, i)$ to (n, i) .**
- (n) Verify that $A_i = A_0 (D_1 N_1) \cdots (D_i N_i)$.
- (o) Verify that $MA_i = (D_1 N_1) \cdots (D_i N_i)$.
- (p) **Therefore verify that $A_0 M A_i = A_i$.**
- (q) For $j = 1$ to $j = n$, do the following:
 - i. Using [algorithm 49](#), verify that $(e_j^T M)(A_i e_j) = e_j^T (M A_i) e_j = e_j^T ((D_1 N_1) \cdots (D_i N_i)) e_j = (D_{1,j,j} N_{1,j,j}) \cdots (D_{i,j,j} N_{i,j,j})$.
 - ii. **Therefore using (5d) verify that** $(e_j^T M)(A_i e_j) = D_{1,j,j} \cdots D_{i,j,j} = D_{1,j,j} \cdots D_{\min(i,j-1),j,j} \|A_0 e_1\|^2 \cdots \|A_{\min(i,j-1)-1, \min(i,j-1)}\|^2$.
6. **Verify that** $A_n^T A_n = (A_0 (D_1 N_1) \cdots (D_n N_n))^T (A_0 (D_1 N_1) \cdots (D_n N_n)) = ((D_1 N_1) \cdots (D_n N_n))^T (A_0^T A_0) ((D_1 N_1) \cdots (D_n N_n))$ **is a diagonal matrix.**
7. **Yield the tuple $\langle A_0, A_1, \dots, A_n \rangle$.**

2.51 Algorithm 51 (Cauchy-Schwarz inequality)

Choose a $\mathcal{M}_{1,m}(\mathbb{Q})$, A , and a $\mathcal{M}_{m,1}(\mathbb{Q})$, B . Now do the following:

1. Verify that 0
 - (a) $\leq \frac{1}{2} \sum_{i=1}^m \sum_{j=1}^m (A_i B_j - A_j B_i)^2$
 - (b) $= \frac{1}{2} \sum_{i=1}^m \sum_{j=1}^m (A_i^2 B_j^2 - 2A_i B_j A_j B_i + A_j^2 B_i^2)$
 - (c) $= \frac{1}{2} \sum_{i=1}^m A_i^2 \sum_{j=1}^m B_j^2 + \frac{1}{2} \sum_{i=1}^m B_i^2 \cdot \sum_{j=1}^m A_j^2 - \sum_{i=1}^m A_i B_i \sum_{j=1}^m A_j B_j$
 - (d) $= \frac{1}{2} (AA^T)(B^T B) + \frac{1}{2} (AA^T)(B^T B) - (AB)^2$
 - (e) $= (AA^T)(B^T B) - (AB)^2$.
2. Therefore verify that $(AB)^2 \leq (AA^T)(B^T B)$.

2.52 Algorithm 52

Choose integers $m \geq n > 0$. Choose a $\mathcal{M}_{n,m}(\mathbb{Q}[x])$, M , and a $\mathcal{M}_{m,n}(\mathbb{Q}[x])$, A_0 , such that $MA_0 = I_n$. Choose a \mathbb{Q} , x . Now do the following:

1. Execute algorithm 50 on M and A_0 . Let the tuple $\langle A_0, A_1, \dots, A_n \rangle$ receive the result.
2. Let $a = \max(\|M(x)\|^2, 1)$.
3. Choose a column index $1 \leq j \leq n$ such that $\|A_n(x)e_j\|^2 < \frac{1}{a^{(2n+2)!!}}$.
4. Let $i = n$.
5. Verify that $\|A_i(x)e_j\|^2 < \frac{1}{a^{(2i+2)!!}}$.
6. Using algorithm 51, verify that $(e_j^T M(x) A_i(x) e_j)^2 \leq \|e_j^T M(x)\|^2 \|A_i(x)e_j\|^2 < \|M(x)\|^2 \frac{1}{a^{(2i+2)!!}} \leq a \frac{1}{a^{(2i+2)!!}} \leq \frac{1}{a^{(2i)!! * 2i}} \leq 1$.
7. If $i = 0$, then do the following:
 - (a) Verify that $(e_j^T M(x) A_i(x) e_j)^2 = (e_j^T M(x) A_0(x) e_j)^2 = (e_j^T I_n e_j)^2 = 1$.
 - (b) Abort algorithm.
8. Otherwise, do the following:
9. Using algorithm 50, verify that $(1\|A_0 e_1\|^2 \cdots \|A_{\min(i,j-1)-1} e_{\min(i,j-1)}\|^2)^2 = (e_j^T M(x) A_i(x) e_j)^2 < \frac{1}{a^{(2i)!! * 2i}} \leq 1$.
10. If $\min(i, j-1) = 0$, then do the following:

- (a) Verify that $(1\|A_0(x)e_1\|^2 \cdots \|A_{\min(i,j-1)-1}(x)e_{\min(i,j-1)}\|^2)^2 = 1^2 = 1$.

- (b) Abort algorithm.

11. Otherwise do the following:

- (a) Verify that $\min(i, j-1) > 0$.
- (b) If for all $k = 0$ to $k = \min(i, j-1) - 1$, $\|A_k(x)e_{k+1}\|^2 \geq \frac{1}{a^{(2i)!!}}$, then do the following:
 - i. Verify that $(e_j^T M(x) A_i(x) e_j)^2 = (\|A_0(x)e_1\|^2 \cdots \|A_{\min(i,j-1)-1}(x)e_{\min(i,j-1)}\|^2)^2 \geq (\frac{1}{a^{(2i)!!}})^{2 \min(i,j-1)} \geq (\frac{1}{a^{(2i)!!}})^{2i} = \frac{1}{a^{(2i)!! * 2i}}$.
 - ii. Abort algorithm.
- (c) Otherwise, do the following:

- i. Let k , where $0 \leq k < i$, be one of the integers for which $\|A_k(x)e_{k+1}\|^2 < \frac{1}{a^{(2i)!!}}$.
- ii. Verify that $\|A_k(x)e_{k+1}\|^2 < \frac{1}{a^{(2i)!!}} \leq \frac{1}{a^{(2k+2)!!}}$.
- iii. Simultaneously set i to k and j to $k+1$.
- iv. Go to (5).

12. Abort algorithm.

2.53 Algorithm 53

Choose a symmetric $\mathcal{M}_{m,m}(\mathbb{Q})$, A . Now do the following:

1. Execute algorithm 48 on the matrix A .
2. For $i = 1$ to $i = t$, let k_i be the index of the polynomial to which (c_i, d_i) was associated.
3. Verify that $\sum_{i=1}^t (m+1-k_i)$
 - (a) $= \sum_{i=1}^t \sum_{j=1}^m [k_i \leq j]$
 - (b) $= \sum_{j=1}^m \sum_{i=1}^t [k_i \leq j]$
 - (c) $= \sum_{j=1}^m \sum_{i=1}^t [k_i \leq j] \sum_{l=1}^m [k_i = l]$
 - (d) $= \sum_{j=1}^m \sum_{l=1}^m \sum_{i=1}^t [k_i \leq j][k_i = l]$
 - (e) $= \sum_{j=1}^m \sum_{l=1}^m \sum_{i=1}^t [l \leq j][k_i = l]$

- (f) $= \sum_{j=1}^m \sum_{l=1}^m [l \leq j] \sum_{i=1}^t [k_i = l]$
- (g) $= \sum_{j=1}^m \sum_{l=1}^m [l \leq j] n_l$
- (h) $= \sum_{j=1}^m \sum_{l=1}^m [l \leq j] \deg u_l$
- (i) $= \sum_{j=1}^m \sum_{l=1}^j \deg u_l$
- (j) $= \sum_{j=1}^m \deg D_{j,j}$
- (k) $= m$

4. **Verify that** $\sum_{i=1}^t (m+1-k_i) = m$.

2.54 Algorithm 54 (Symmetric matrix spectral algorithm initialization)

Choose a symmetric $\mathcal{M}_{m,m}(\mathbb{Q})$, A . **Choose a** \mathbb{Q} $\epsilon > 0$. Now do the following:

1. Execute **algorithm 48** on the matrix A .
2. Execute **algorithm 6** with $xI_m - A$ as the choice matrix. Let the tuple $\langle M^{-1}, D, N^{-1} \rangle$ receive the result.
3. Let M' be the matrix obtained by replacing all the negative signs in M^{-1} with positive signs.
4. Let $M'' = \max_{i=1}^m \max_{j=1}^m M'(\max(|c_1|, |d_t|))_{i,j}$.
5. Let N' be the matrix obtained by replacing all the negative signs in N with positive signs.
6. Let $N'' = \max_{i=1}^m \max_{j=1}^m N'(\max(|c_1|, |d_t|))_{i,j} + 1$.
7. Let L be the formal polynomial obtained by replacing all the negative signs in $(\|N^{-1}\|^2)^{(2m+2)!!}$ with positive signs.
8. Let $L' = \frac{1}{\max(1, L(|c_1|), L(|d_t|))}$.
9. Let $\delta = \min(1, \min_{i=1}^{t-1} (c_{i+1} - c_i))$.
10. For $i = 1$ to $i = t$, do the following:
 - (a) Let k_i be the index of the polynomial to which (c_i, d_i) was associated.
 - (b) Verify that $\text{sgn}(u_{k_i}(c_i)) \neq \text{sgn}(u_{k_i}(d_i))$.
 - (c) Let Q be the last $m+1-k_i$ columns of I_m .
 - (d) Verify that $(Q^T N^{-1})(NQ) = Q^T (N^{-1}N)Q = Q^T I_m Q = Q^T Q = I_{m+1-k_i}$.

(e) Execute **algorithm 50** on the matrices $Q^T N^{-1}$ and NQ . Let the tuple $\langle \cdot, \dots, K_i \rangle$ receive the result.

(f) **Verify that** $K_i^T K_i$ is a diagonal matrix.

(g) Let $E = Q^T N^{-1} K_i$ be a $(m+1-k_i) \times (m+1-k_i)$ matrix.

(h) Cognizant of the execution of **algorithm 50**, verify that $K_i = NQE$.

(i) Let E' be the matrix obtained by replacing all the negative signs in E with positive signs.

(j) Let $E'' = \max_{j=1}^m \max_{l=1}^m E'(\max(|c_1|, |d_t|))_{j,l}$.

11. Let $E'' = 1 + \max_{i=1}^t E''_i$.

12. For $i = 1$ to $i = t$, do the following with the symbols Q , E , and F retaining their values from the corresponding iteration of the loop at (7).

(a) Let $b = \frac{\epsilon \delta}{M'' N'' E''^2 m^2 (m+1-k_i)}$.

(b) For $j = k$ to $j = m$, do the following:

i. Execute **algorithm 36** on the formal polynomial $D_{j,j}$, interval (c_i, d_i) , and target of b . Let c_i and d_i receive their updates.

(c) If a diagonal entry of $K_i(c_i)^T K_i(c_i)$ is less than L' , then do the following:

i. Let z be the index of the column of the entry.

ii. Verify that $L' \leq \frac{1}{\max(\|Q^T N^{-1}\|(c_i)\|^2, 1)^{(2(m+1-k_i)+2)!!}}$.

iii. Execute **algorithm 52** with matrices $Q^T N^{-1}$ and NQ , rational number c_i , and column index z .

iv. **Abort algorithm.**

(d) Otherwise, do the following:

i. **For** $j = 1$ **to** $j = m+1-k_i$, **verify that** $(K_i(c_i)^T K_i(c_i))_{j,j} \geq L'$.

ii. Verify that $xK_i - AK_i = (xI_m - A)K_i = M^{-1}DN^{-1}K_i = M^{-1}DN^{-1}NQE = M^{-1}DQE$.

iii. Verify that $\|c_i K_i(c_i) - AK_i(c_i)\|^2 = \|M^{-1}(c_i)D(c_i)QE(c_i)\|^2 \leq$

$$\begin{aligned}
& \|M'' J_m \frac{\epsilon \delta}{M'' N'' E'' m^2 (m+1-k_i)} Q E'' J_{m+1-k} \|^2 = & \text{v. } & \leq |(K e_i)^T A (K e_j) - (K e_i)^T A^T (K e_j)| + \\
& \|J_m \frac{\epsilon \delta}{N'' E'' m^2 (m+1-k_i)} Q J_{m+1-k} \|^2 = & & |m N'' E'' J_{1 \times m} \frac{\epsilon \delta}{N'' E'' m^2} J_{m \times 1}| + \\
& \|\frac{\epsilon \delta}{N'' E'' m^2} J_{m \times (m+1-k_i)} \|^2 = & & |\frac{\epsilon \delta}{N'' E'' m^2} J_{1 \times m} m N'' E'' J_{m \times 1}| \\
& \frac{m+1-k_i}{m^3} \cdot \frac{\epsilon^2 \delta^2}{(N'' E'')^2} \cdot & \text{vi. } & = 2\epsilon \delta.
\end{aligned}$$

iv. **Therefore verify that** $\|c_i K_i(c_i) - AK_i(c_i)\|^2 \leq \frac{m+1-k_i}{m^3} \cdot \frac{\epsilon^2 \delta^2}{(N'' E'')^2} \leq \frac{m+1-k_i}{m} \epsilon^2$.
(c) **Therefore verify that** $|e_i^T (K^T K) e_j| = |(K e_i)^T (K e_j)| \leq \frac{2\epsilon \delta}{c_b - c_a} \leq 2\epsilon$.

13. Yield the tuple $\langle \langle K_1, c_1 \rangle, \dots, \langle K_t, c_t \rangle \rangle$.

2.55 Algorithm 55 (Symmetric matrix spectral)

Choose a symmetric $\mathcal{M}_{m,m}(\mathbb{Q})$, A . Choose a \mathbb{Q} $\epsilon > 0$. Now do the following:

1. Execute **algorithm 54** on matrix A and rational ϵ . Let the tuple $\langle \langle K_1, c_1 \rangle, \dots, \langle K_t, c_t \rangle \rangle$ receive the result.
2. Let C be a diagonal matrix whose i^{th} , where $1 \leq i \leq t$, group of entries are $m+1-k_i$ c_i s.
3. Using **algorithm 53**, verify that C is $m \times m$.
4. Let K be a matrix whose columns are the in-order concatenation of those of $K_1(c_1), K_2(c_2), \dots, K_t(c_t)$.
5. Using **algorithm 53** and (9e), verify that K is $m \times m$.
6. **Using algorithm 53 and algorithm 54, verify that** $\|KC - AK\|^2 \leq \sum_{i=1}^t \frac{m+1-k_i}{m} \epsilon^2 = \frac{\sum_{i=1}^t (m+1-k_i)}{m} \epsilon^2 = \frac{m}{m} \epsilon^2 = \epsilon^2$.
7. For $i = 1$ to $i = m$, do the following: For $j = 1$ to $j = m$, do the following:
 - (a) If $K e_i$ was constructed during iteration $i = a$ and $K e_j$ during iteration $i = b$ of (11), and if $a \neq b$, then do the following:
 - (b) Verify that $|(c_b - c_a)(K e_i)^T (K e_j)|$
 - i. $= |c_b (K e_i)^T (K e_j) - c_a (K e_i)^T (K e_j)|$
 - ii. $= |(K e_i)^T (c_b K e_j) - (c_a K e_i)^T (K e_j)|$
 - iii. $= |(K e_i)^T (AK e_j + c_b K e_j - AK e_j) - (AK e_i + c_a K e_i - AK e_i)^T (K e_j)|$
 - iv. $\leq |(K e_i)^T (AK e_j) - (AK e_i)^T (K e_j)| + |(K e_i)^T (c_b K e_j - AK e_j)| + |(c_a K e_i - AK e_i)^T (K e_j)|$

8. Using (7c) and **algorithm 54**, verify that the absolute values of all the non-diagonal entries $K^T K$ are less than or equal to 2ϵ .

9. Using **algorithm 54**, verify that all the diagonal entries of $K^T K$ are more than or equal to L' .

10. Yield the tuple $\langle K, C \rangle$.