Lattice reduction of polynomial matrices

Arne Storjohann

David R. Cheriton School of Computer Science
University of Waterloo

Presented at the SIAM conference on Applied Algebraic Geometry at the Colorado State University, Fort Collins, Colorado, USA

August 4, 2013

Reduced basis

Input: Matrix $A \in \mathsf{K}[x]^{n\times m}$, K a field, e.g., $\mathsf{K} = \mathbb{Z}/(7)$.
Output: Reduced matrix $R \in K[x]^{n\times m}$ such that

- Set of all $\mathsf{K}[x]$-linear combinations of rows of R is same as A.
- Degrees of row of R are minimal among all bases.

Example: $n = 3$, $m = 1$

$$\overset{A}{\begin{bmatrix} 3x^4 + 2x^3 + 2x^2 + 3 \\ x^3 + 3x^2 + 3x + 2 \\ x^2 + 4x + 3 \end{bmatrix}} \longrightarrow \overset{R}{\begin{bmatrix} x + 3 \\ 0 \\ 0 \end{bmatrix}}$$

Reduced basis

Input: Matrix $A \in \mathsf{K}[x]^{n\times m}$, K a field, e.g., $\mathsf{K} = \mathbb{Z}/(7)$.
Output: Reduced matrix $R \in K[x]^{n\times m}$ such that

- Set of all $\mathsf{K}[x]$-linear combinations of rows of R is same as A.
- Degrees of row of R are minimal among all bases.

Example: $n = 3$, $m = 3$

$$\overset{A}{\begin{bmatrix} 4x^2+3x+5 & 4x^2+3x+4 & 6x^2+1 \\ 3x+6 & 3x+5 & 3+x \\ 6x^2+4x+2 & 6x^2 & 2x^2+x \end{bmatrix}} \longrightarrow \overset{R}{\begin{bmatrix} 3 & 4 & 1 \\ 6x+3 & 9x & 2x \\ 0 & 0 & 0 \end{bmatrix}}$$

- Obtained using unimodular row operations: $R = UA$.

Reduced basis

Canonical Popov form

The Popov form is a canonical normalization of a reduced basis.

- Let $[d]$ denote a polynomial of degree d
- Row pivot is the rightmost element of maximal degree.

$$\overset{R}{\begin{bmatrix} [1] & [1] & [1] & [1] \\ [2] & [2] & [2] & [2] \\ [2] & [2] & [2] & [2] \\ [4] & [4] & [4] & [4] \end{bmatrix}} \rightarrow \overset{W}{\begin{bmatrix} [1] & [1] & [1] & [1] \\ [2] & [1] & [1] & [1] \\ [1] & [2] & [2] & [1] \\ [3] & [4] & [3] & [3] \end{bmatrix}} \rightarrow \overset{P}{\begin{bmatrix} [1] & [1] & [1] & [1] \\ [2] & [1] & [1] & [0] \\ [1] & [2] & [2] & [0] \\ [1] & [4] & [1] & [0] \end{bmatrix}}$$

- R: minimal degrees and row degrees nonincreasing
- W: pivots have distinct indices
- P: degrees in columns strictly less than pivot

V. Popov. Some Properties of Control Systems with Irreducible Matrix Transfer Functions. Lecture Notes in Mathematics, Springer, 1969.

Iterative algorithm for basis reduction

Vector case: Euclidean algorithm

Input: $A \in \mathsf{K}[x]^{2\times 1}$

Output: Reduced basis for A

$$R_0 := A$$
$$\begin{bmatrix} 3x^4 + 2x^3 + 2x^2 + 3 \\ x^3 + 3x^2 + 3x + 2 \end{bmatrix}$$

Iterative algorithm for basis reduction

Vector case: Euclidean algorithm

Input: $A \in \mathsf{K}[x]^{2\times 1}$.

Output: Reduced basis for A.

$$\underbrace{\begin{bmatrix} & 1 \\ 1 & -3x \end{bmatrix}}_{Q_1} \underbrace{\begin{bmatrix} 3x^4+2x^3+2x^2+3 \\ x^3+3x^2+3x+2 \end{bmatrix}}_{R_0 := A} = \underbrace{\begin{bmatrix} x^3+3x^2+3x+2 \\ x+3 \end{bmatrix}}_{R_1}$$

Iterative algorithm for basis reduction

Vector case: Euclidean algorithm

Input: $A \in \mathsf{K}[x]^{2\times 1}$.

Output: Reduced basis for A.

$$\overset{Q_1}{\begin{bmatrix} & 1 \\ 1 & -3x \end{bmatrix}} \overset{R_0 := A}{\begin{bmatrix} 3x^4 + 2x^3 + 2x^2 + 3 \\ x^3 + 3x^2 + 3x + 2 \end{bmatrix}} = \overset{R_1}{\begin{bmatrix} x^3 + 3x^2 + 3x + 2 \\ x + 3 \end{bmatrix}}$$

$$\overset{Q_2}{\begin{bmatrix} & 1 \\ 1 & -x^2 \end{bmatrix}} \overset{R_1}{\begin{bmatrix} x^3 + 3x^2 + 3x + 2 \\ x + 3 \end{bmatrix}} = \overset{R_2}{\begin{bmatrix} x + 3 \\ 3x + 2 \end{bmatrix}}$$

Iterative algorithm for basis reduction

Matrix case: Extension of the Euclidean algorithm

Goal Reduce an input matrix $A \in \mathsf{K}[x]^{n \times m}$.

Algorithm: Add monomial multiples of one row to another to either move a pivot to the left or decrease the degree of the row. Stop when no more transformations are possible.

$$\begin{bmatrix} [3] & [3] & [2] \\ [1] & [1] & [0] \\ [3] & [2] & [2] \end{bmatrix} \xrightarrow{(1)} \begin{bmatrix} [3] & [2] & [2] \\ [1] & [1] & [0] \\ [3] & [2] & [2] \end{bmatrix} \xrightarrow{(2)} \begin{bmatrix} [2] & [2] & [2] \\ [1] & [1] & [0] \\ [3] & [2] & [2] \end{bmatrix}$$

- (1) add $*x^2$ times second row to first row (appropriate $* \in \mathsf{K}$)
- (2) add $*$ times last row to first row
- final matrix is in weak Popov form (distinct pivot locations)

Iterative algorithm for basis reduction

Cost analysis

Input: $A \in \mathsf{K}[x]^{n \times m}$ of degree d and rank r.

- number of rows is n
- number of times a pivot can move left is $O(r)$
- number of times a pivot can decrease in degree is $O(d)$
- cost of each simple transformation is $O(md)$ ops from K

Overall cost: $O(nmr \times d^2)$ field operations from K.

$$\begin{bmatrix} [3] & [3] & [2] \\ [1] & [1] & [0] \\ [3] & [2] & [2] \end{bmatrix} \xrightarrow{(1)} \begin{bmatrix} [3] & [2] & [2] \\ [1] & [1] & [0] \\ [3] & [2] & [2] \end{bmatrix} \xrightarrow{(2)} \begin{bmatrix} [2] & [2] & [2] \\ [1] & [1] & [0] \\ [3] & [2] & [2] \end{bmatrix}$$

Mulders and S. On Lattice Reduction for Polynomial Matrices. Journal of Symbolic Computation, 2003.

Questions regarding the cost of lattice reduction

Asymptotically faster algorithms

- Square nonsingular input $A \in \mathsf{K}[x]^{n \times n}$ of degree d.
- Iterative algorithm has cost $O(n^3 d^2)$ operations from K.

Questions:

- How to incorporate fast matrix multiplication?
  I.e, Reduce cost in n from $O(n^3)$ to $O(n^\omega)$.
  Here, $2 < \omega \leq 3$ is the exponent of matrix multiplication.
- How to incorporate fast polynomial multiplication?
  I.e., Reduce cost in d from $O(d^2)$ to $O(d^{1+\epsilon})$.
  Here, $0 < \epsilon \leq 1$ depending on algorithms used.

Goal:

- Reduce lattice reduction to polynomial matrix multiplication.
- Thus, target cost is $O(n^\omega d^{1+\epsilon})$, at least up to log factors.

Iterative algorithm for basis reduction

Recursive approach to incorporate polynomial multiplication?

Scalar case: Example of $A \in \mathsf{K}[x]^{2\times 1}$ with degree 3.

$$\overset{U}{\begin{bmatrix} 4x+5 & 2x \\ 3x^2+2x+1 & 5x^2+4 \end{bmatrix}} \overset{A}{\begin{bmatrix} 2x^3+6x^2+3x+2 \\ 3x^3+4x^2+3 \end{bmatrix}} = \overset{R}{\begin{bmatrix} x+3 \\ 0 \end{bmatrix}}$$

- Fact: $\deg U \leq \deg A$
- The celebrated recursive "half-gcd" approach can introduce polynomial multiplication.

General case: Example of an $A \in \mathsf{K}[x]^{30\times 30}$ with degree 12.

$$\overset{U}{\begin{bmatrix} [299] & \cdots & [300] \\ \vdots & \ddots & \vdots \\ [303] & \cdots & [304] \end{bmatrix}} \overset{A}{\begin{bmatrix} [12] & \cdots & [11] \\ \vdots & \ddots & \vdots \\ [12] & \cdots & [10] \end{bmatrix}} = \overset{R}{\begin{bmatrix} [0] & \cdots & [0] \\ \vdots & \ddots & \vdots \\ [1] & \cdots & [4] \end{bmatrix}}$$

- Degrees in U too large: lower order coefficients involved.

Technique 1: Fast minimal approximant basis

Input: • $G \in \mathsf{K}[x]^{2n \times m}$ and approximation order Δ.

• Degree contraints $[\delta_1, \delta_2, \ldots, \delta_{2n}]$ for columns of M.

Output: Reduced basis $M \in \mathsf{K}[x]^{n \times n}$ such that $MG \equiv 0 \bmod x^{\Delta}$.

$$\overset{M}{\left[\begin{array}{c|c} * & * \\ \hline * & * \end{array}\right]} \overset{G}{\left[\begin{array}{c} * \\ \hline * \end{array}\right]} \equiv 0_{2n \times n} \bmod x^{\Delta}$$

Cost: $O(n^{\omega} \Delta^{1+\epsilon})$ operations from K.

- Beckermann and Labahn. A uniform approach for the fast computation of matrix-type Padé approximants. SIAM Journal on Matrix Analysis and Applications, 1994
- Giorgi, Jeannerod and Villard. On the complexity of polynomial matrix computations, ISSAC 2003.

Technique 1: Fast minimimal approximant basis

Input: • $G = \begin{bmatrix} A & -I \end{bmatrix}^T \in \mathsf{K}[x]^{2n \times m}$ and $\Delta = nd + d + 1$.
• Degree contraints $[nd, \ldots, nd, 0, \ldots, 0]$ for columns of M.

Output: Reduced basis $M \in \mathsf{K}[x]^{n \times n}$ such that $MG \equiv 0 \bmod x^{\Delta}$.

$$\overset{M}{\left[\begin{array}{c|c} U & R \\ \hline * & * \end{array}\right]} \overset{G}{\left[\begin{array}{c} A \\ \hline -I \end{array}\right]} \equiv 0_{2n \times n} \bmod x^{\Delta}$$

Fact: For $\Delta \geq nd + d + 1$ a reduced basis R will appear in M.

Cost: $O(n^{\omega}(nd)^{1+\epsilon})$ operations from K

- Beckermann and Labahn. A uniform approach for the fast computation of matrix-type Padé approximants. SIAM Journal on Matrix Analysis and Applications, 1994
- Giorgi, Jeannerod and Villard. On the complexity of polynomial matrix computations. ISSAC 2003.

Dual space approach for lattice reduction

Example: $A = \begin{bmatrix} 1 & 1 \\ x & 1 \end{bmatrix}$

$$\begin{aligned} A^{-1} &= \begin{bmatrix} \frac{1}{1-x} & \frac{1}{x-1} \\ \frac{x}{x-1} & \frac{1}{1-x} \end{bmatrix} \\ &= \left[\begin{array}{c|c} 1+x+x^2+x^3+\cdots & -1-x-x^2-x^3+\cdots \\ \hline -x-x^2-x^3+\cdots & 1+x+x^2+x^3+\cdots \end{array}\right] \\ &= \overset{B_0}{\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}} + \overset{B_1}{\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}} x + \overset{B_2}{\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}} x^2 + \cdots . \end{aligned}$$

Fact: $R \in \mathsf{K}[x]^{2\times 2}$ is a reduced basis for A precisely when

- R is nonsingular,
- R has minimal degrees, and
- $R(B_0 + B_1 x + B_2 x^2 + \cdots)$ is finite.

Dual space approach for lattice reduction

In conjunction with minimal approximant basis

Original formulation

- Apply minimal approximant basis algorithm directly

$$\overset{M}{\left[\begin{array}{c|c} U & R \\ \hline * & * \end{array}\right]} \overset{G}{\left[\begin{array}{c} A \\ \hline -I \end{array}\right]} \equiv 0_{2n \times n} \bmod x^{\Delta}$$

- Need $\Delta \geq nd + d + 1$

Dual space formulation

- Compute x-adic expansion: $A^{-1} = B_0 + B_1 x + B_2 x^2 + \cdots$
- Apply minimal approximant basis algorithm

$$\overset{M}{\left[\begin{array}{c|c} R & U \\ \hline * & * \end{array}\right]} \overset{G}{\left[\begin{array}{c} B_0 + B_1 x + B_2 x^2 + \cdots \\ \hline -I \end{array}\right]} \equiv 0_{2n \times n} \bmod x^{\Delta}$$

- Need $\Delta \geq nd + d + 1$

Using a high-order component of the inverse

Scalar example

$$A^{-1} = \frac{U}{R} = \frac{x^4 + 6x^3 + 4x^2 + 3x + 1}{x + 1}$$

$$= 1 + 2x + 2x^2 + 4x^3 + 4x^4 + 3x^5 + 4x^6 + 3x^7 + 4x^8 + \cdots$$

<u>Original (dual) minimal approximant basis problem</u>

$$\overset{M}{\left[\begin{array}{c|c} R & U \\ \hline * & * \end{array}\right]} \overset{G}{\left[\begin{array}{c} 1 + 2x + 2x^2 + 4x^3 + 4x^4 + 3x^5 + 4x^6 \\ \hline -I \end{array}\right]} \equiv 0 \bmod x^7$$

Using a high-order component of the inverse

Scalar example

$$A^{-1} = \frac{U}{R} = \frac{x^4 + 6x^3 + 4x^2 + 3x + 1}{x + 1}$$

$$= 1 + 2x + 2x^2 + 4x^3 + 4x^4 + 3x^5 + 4x^6 + 3x^7 + 4x^8 + \cdots$$

Original (dual) minimal approximant basis problem

$$\overset{M}{\left[\begin{array}{c|c} R & U \\ \hline * & * \end{array}\right]} \overset{G}{\left[\begin{array}{c} 1 + 2x + 2x^2 + 4x^3 + 4x^4 + 3x^5 + 4x^6 \\ \hline -I \end{array}\right]} \equiv 0 \bmod x^7$$

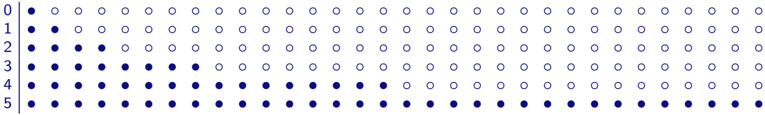
New (dual) problem using high-order component

$$\overset{M}{\left[\begin{array}{c|c} R & 3 \\ \hline * & * \end{array}\right]} \overset{G}{\left[\begin{array}{c} 3 + 4x + 3x^2 \\ \hline -I \end{array}\right]} \equiv 0 \bmod x^3$$

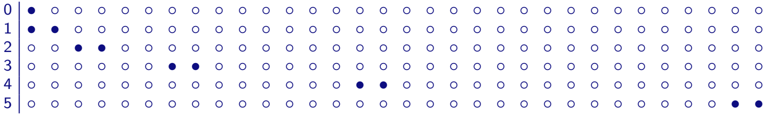
Technique 2: High-Order component lifting

$$A^{-1} = \bullet + \bullet x + \bullet x^2 + \bullet x^3 + \bullet x^4 + \bullet x^5 + \bullet x^6 + \bullet x^7 + \cdots$$

Standard quadratic lifting (a la Newton iteration)



High-order component lifting



- Input A has degree d
- Need a high-order component at order $\Omega(nd)$ of degree d
- Cost reduced from $O(n^\omega (nd)^{1+\epsilon})$ to $O(n^\omega d^{1+\epsilon}(\log n))$

S. High-order lifting and integrality certification, Journal of Symbolic Computation, 2003.

Normalization of row reduced forms

$$\overset{R}{\begin{bmatrix} [1] & [1] & [1] & [1] \\ [2] & [2] & [2] & [2] \\ [2] & [2] & [2] & [2] \\ [4] & [4] & [4] & [4] \end{bmatrix}} \overset{(1)}{\rightarrow} \overset{W}{\begin{bmatrix} [1] & [1] & [1] & [1] \\ [2] & [1] & [1] & [1] \\ [1] & [2] & [2] & [1] \\ [3] & [4] & [3] & [3] \end{bmatrix}} \overset{(2)}{\rightarrow} \overset{P}{\begin{bmatrix} [1] & [1] & [1] & [1] \\ [2] & [1] & [1] & [0] \\ [1] & [2] & [2] & [0] \\ [1] & [4] & [1] & [0] \end{bmatrix}}$$

- (1) Suffices to work only with $\mathrm{LC}(R)$.
- (2) Based on following observation

$$\overset{P}{\begin{bmatrix} [1] & [1] & [1] & [1] \\ [2] & [1] & [1] & [0] \\ [1] & [2] & [2] & [0] \\ [1] & [4] & [1] & [0] \end{bmatrix}} \overset{X}{\begin{bmatrix} x^2 & & & \\ & 1 & & \\ & & x^2 & \\ & & & x^3 \end{bmatrix}} = \overset{PX}{\begin{bmatrix} [3] & [1] & [3] & [4] \\ [4] & [1] & [3] & [3] \\ [3] & [2] & [4] & [3] \\ [3] & [4] & [3] & [3] \end{bmatrix}}.$$

- Row reduce WX, apply step (1), postmultiply by X^{-1}.

Sarkar and S. Normalization of row reduced matrices. ISSAC 2011.

Technique 3: x-basis decomposition

Used for derandomization of fast lattice reduction algorithm

Problem: What if A is singular modulo x?

$$A^{-1} = \bullet + \bullet x + \bullet x^2 + \bullet x^3 + \bullet x^4 + \quad ?$$

Solution: Compute an x-basis decomposition.

- $$\overset{A}{\begin{bmatrix} x^2 & x+1 & x+4 \\ x & x^2+5x & 6x+1 \\ 0 & 3x+5 & x^2+6x+6 \end{bmatrix}} = \overset{U}{\begin{bmatrix} x & x+1 & 1 \\ 1 & x^2+5x & 3x+5 \\ 0 & 3x+5 & 2 \end{bmatrix}} \overset{H}{\begin{bmatrix} x & 0 & 2x^2+1 \\ & 1 & 4x^2+3x+4 \\ & & x^3 \end{bmatrix}}$$
- $\det A = (\det U) \times (\det H) = (x^2 + 4x + 3) \times x^4$

Gupta, Sarkar, S. and Valeriote. Triangular x-basis decompositions and derandomization of linear algebra algorithms over $\mathsf{K}[x]$. Journal of Symbolic Computation, 2012.

Conclusions

Deterministic algorithm for computing the Popov form of a nonsingular matrix.

$$\overset{A}{\begin{bmatrix} [20] & [52] & [13] & [32] \\ [32] & [13] & [45] & [12] \\ [18] & [25] & [24] & [17] \\ [36] & [43] & [33] & [32] \end{bmatrix}} \rightarrow \overset{P}{\begin{bmatrix} [1] & [1] & [1] & [1] \\ [2] & [1] & [1] & [0] \\ [1] & [2] & [2] & [0] \\ [1] & [4] & [1] & [0] \end{bmatrix}}$$

- Input: Nonsingular $A \in \mathsf{K}[x]^{n \times n}$
- Output: Canonical Popov form P (a reduced lattice) of A
- Cost: $O(n^{\omega} d^{1+\epsilon} (\log n)^2)$ operations from K

Extension to matrices of arbitrary shape and rank?

- Sarkar and S. Normalization of row reduced matrices. ISSAC 2011.
- PhD thesis of Wei Zhou, University of Waterloo, 2012.
- Zhou and Labahn. Computing column bases of polynomial matrices. ISSAC 2013.