

Workshop on Complexity — FoCM
Minneapolis, Aug. 12, 2002

EXACT COMPUTATION OF THE DETERMINANT AND OF THE INVERSE OF A MATRIX

Gilles Villard
CNRS - LIP ENS Lyon / INRIA
<http://www.ens-lyon.fr/~gvillard/>

Parts of this work have been done with Claude-Pierre Jeannerod (INRIA, LIP ENS Lyon)
and with Erich Kaltofen (North Carolina State University).

Problems.

A , $n \times n$ matrix.

Determinant and inverse computation.

- .. Algebraic complexity over $K[x]$, $K(x)$
- .. Bit complexity over \mathbb{Z} , \mathbb{Q}
- .. Algebraic complexity without divisions over \mathbb{R}

- ▷ Deterministic or
Monte Carlo or Las Vegas randomized algorithms.
- ▷ Time complexity (& practical algorithms).
- ▷ (Space complexity).

→ A new algorithm and a survey of recent results.

The talk

1. Classical facts in linear algebra
2. Matrix inversion over $K(x)$
3. Determinant without divisions over R
4. Bit complexity

Remaining problems

1. CLASSICAL FACTS IN LINEAR ALGEBRA

Classical facts |/ Algebraic complexity

- ▷ Mm : matrix multiplication (or n^ω) .
- ▷ Det : determinant.
- ▷ Inv : inversion.
- ▷ SysLin : linear system solution.

- [Strassen 69, Bunch and Hopcroft 74] :

$$\text{Det} \preceq \text{Mm}, \quad \text{SysLin} \preceq \text{Mm}$$

(Recursive factorization).

$$\text{Mm} \preceq \text{Inv}$$

- [Strassen 73, Baur & Strassen 83] :

$$\text{Inv} \preceq \text{Det}$$

(Automatic differentiation).

$$\rightarrow \text{SysLin} \preceq \text{Mm} \approx \text{Det} \approx \text{Inv}$$

$A \in \mathbb{K}[x]^{n \times n}$ of degree d ,

one must take into account the degrees of the polynomials involved in the computations.

The determinant has degree nd at worst.

- [Mc Clellan 73] :

The **determinant** can be computed in $\tilde{O}(n^\omega \times nd)$ arithmetic operations.

Proof : evaluation / interpolation scheme.

Linear system solution

$$Ay = b$$

- [Moenck & carter 79, Dixon 82, Storjohann 2002] :

If the polynomial matrix A is invertible then $Ay = b$ can be solved in $\tilde{O}(n^\omega d)$ arithmetic operations.

“ x -adic lifting”

For i from 1 to $2nd$

Computation of $\bar{y} = \bar{y}_0 + \bar{y}_1x + \bar{y}_2x^2 + \dots + \bar{y}_ix^i$:

$$\bar{y}_i = A^{-1}b_i \pmod{x} \quad // \text{ Correction}$$

$$b_{i+1} = (b_i - A\bar{y}_i)/x \quad // \text{ New residue}$$

Reconstruction (e.g. Padé approximation) of the rational solution y .

- For generic matrices [Pan 87] :

When the Smith normal form is trivial.

The polynomial matrix **determinant** can be computed in $\tilde{O}(n^\omega d)$ arithmetic operations.

Classical facts III/ Bit complexity, \mathbb{Z} , \mathbb{Q}

$A \in \mathbb{Z}^{n \times n}$, with entries of bit-lengths bounded by $O(\log \|A\|)$

one must take into account the lengths of the integers involved in the computations.

The determinant has length $\tilde{O}(n \times \log \|A\|)$ at worst.

- [Mc Clellan 73] :

The **determinant** can be computed in $\tilde{O}(n^\omega \times n \log \|A\|)$ bit operations.

Proof : Chinese remaindering.

Classical facts IV/ Algebraic complexity without divisions

- [Strassen 73] :

Removing divisions from programs that compute polynomials.

The **determinant** can be computed in $\tilde{O}(n^\omega \times n)$ ring operations.

Proof.

- Gaussian elimination without division for the identity matrix.
- Homotopy :

$$B(z) = I + z(A - I),$$

avec : $B|_{z=0} = I, \quad B|_{z=1} = A$

- Multiplications instead divisions :

$$\frac{1}{1-z} = 1 + z + z^2 + z^3 + \dots = (1+z)(1+z^2)(1+z^4)\dots$$

- Computations on truncated power series.

Worst case classical complexities
 (Constant input size d or $\log \|A\|$), up to log factors)

	K	Ring	$K[x]$	\mathbb{Z}
$Ax = b$	n^ω	—	n^ω	n^ω
Det	n^ω	$n^{\omega+1}$	$n^{\omega+1}$	$n^{\omega+1}$
Inv (Adj)	n^ω	$n^{\omega+1}$	$n^{\omega+1}$	$n^{\omega+1}$

Avoid the product algebraic complexity \times size ?

2. MATRIX INVERSION OVER $\mathbf{K}(x)$

$A \in \mathbf{K}[x]^{n \times n}$ of degree d ,

A^{-1} has size $n^3 d$

Theorem. The inverse of a generic matrix polynomial can be computed in $\tilde{O}(n^3 d)$ arithmetic operations.

Recursive block algorithm ?

$$\left[\begin{array}{c|c} \hline & \\ \times & \times \\ \hline \end{array} \right] \cdot \left[\begin{array}{c|c} \times & \times \\ \times & \times \\ \hline \end{array} \right] = \left[\begin{array}{c|c} \times & \times \\ \hline 0 & \times \\ \hline \end{array} \right] \quad ?$$

The usual approach based on Schur complement leads to high degrees,

$$\left[\begin{array}{c|c} I & 0 \\ \hline -CA^{-1} & I \\ \hline \end{array} \right] \cdot \left[\begin{array}{c|c} A & B \\ \hline C & D \\ \hline \end{array} \right] = \left[\begin{array}{c|c} A & B \\ \hline 0 & D - CA^{-1}B \\ \hline \end{array} \right]$$

$$\left[\begin{array}{c|c} & \\ \hline \times & \times \end{array} \right] \cdot \left[\begin{array}{c|c} \times & \times \\ \hline \times & \times \end{array} \right] = \left[\begin{array}{c|c} \times & \times \\ \hline 0 & \times \end{array} \right] \quad ?$$

Sub-problem : $B \in \mathbb{K}[x]^{n \times (n/2)}$

Compute a basis of the kernel of B as a $\mathbb{K}[x]$ -module.

$$\left[\begin{array}{c|c} \times & \times \end{array} \right] \cdot \left[\begin{array}{c} \times \\ \times \end{array} \right] = \left[\begin{array}{c} 0 \end{array} \right] \quad ?$$

Definition. A basis is minimal with row degrees d_i if any other basis has degrees $d'_i \geq d_i$.

Sub-problem : $B \in \mathbb{K}[x]^{n \times (n/2)}$, compute a **minimal basis of the kernel of B as a $\mathbb{K}[x]$ -module.**

Example,

6×3 matrix polynomial of degree 2 over $\text{GF}(7)[x]$

Schur complement \rightarrow degrees 6.

Minimal polynomial basis of degree 2 :

$$B = \begin{bmatrix} 4x^2 + 5x + 6 & 4x^2 + 3x & 4x^2 + x + 6 \\ 5x^2 + 5x & 3x^2 + 2x + 1 & 4x \\ 5x^2 + 6 & 5x^2 + 5x + 3 & x^2 + 2x + 6 \\ 6x + 3 & 4x^2 + 3x + 2 & 2x^2 + 5x \\ 5x^2 + 3x + 1 & 6x^2 + 4x & 4x^2 + 2x + 1 \\ 3x^2 + 4 & 2x^2 + 6 & 5x^2 + 1 \end{bmatrix}$$

$$\begin{bmatrix} 4x & x + 6 + 5x^2 & 4x + 2x^2 & 6x^2 + 5 & 5 + x & 2 + 4x \\ 2x + 4 + x^2 & 6x + 3 + 3x^2 & 4x + 1 & 5 + x & 6x^2 + 6x + 3 & 2 \\ 1 & 4x^2 + 5x + 6 & 6x + 3 + 5x^2 & 6x + 2 & 5x + 6 & 6x^2 + 4x + 5 \end{bmatrix} \cdot B = 0.$$

Lemma. A minimal polynomial basis for the kernel of a generic matrix $B \in \mathbb{K}[x]^{n \times (n/2)}$ of degree d has all its row degrees equal to d and can be computed in $\tilde{O}(n^\omega d)$.

Proof.

1. Existence.

By linearization (matrix resultants), the coefficients of such a minimal basis may be computed from linear systems involving the block Toeplitz matrix

$$T = \begin{bmatrix} B_d & B_{d-1} & \dots & B_0 & 0 & \dots & 0 \\ 0 & B_d & B_{d-1} & \dots & B_0 & \dots & 0 \\ & & \ddots & \ddots & \ddots & \ddots & \\ 0 & \dots & 0 & B_d & B_{d-1} & \dots & B_0 \end{bmatrix} \in \mathbb{K}^{(nd) \times (nd)}.$$

T is generically invertible.

2. Computation. Block Toeplitz system solution or matrix Padé approximation (minimal basis computation) or Knuth-Schönage's half-gcd (matrix generalization) ...

K[x] — Recursive block inversion

$$\left[\begin{array}{c} \text{Min. basis 2} \\ \hline \text{Min. basis 1} \end{array} \right] \cdot \left[\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array} \right] = \left[\begin{array}{c|c} \times & 0 \\ \hline 0 & \times \end{array} \right] \quad ?$$

Degrees : d d **2d**

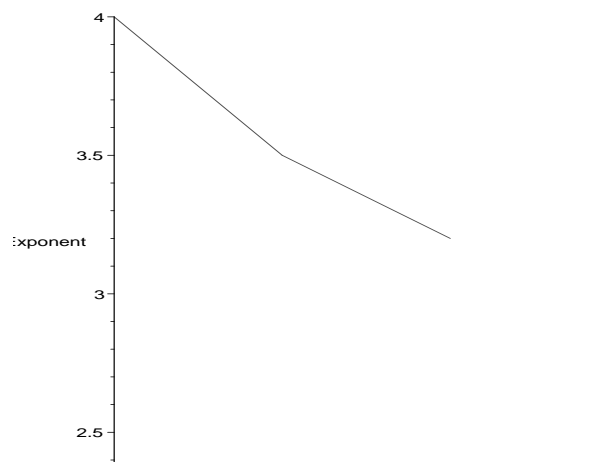
- One step :

Compute 2^{k+1} minimal bases, each in $\tilde{O}\left(\left(\frac{n}{2^k}\right)^\omega 2^k d\right)$.

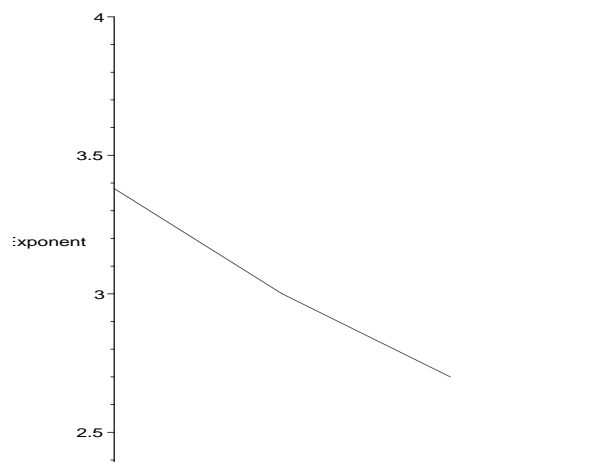
Update of the transformation, $\left(\frac{n}{2^k} \times \frac{n}{2^k}\right)$ -block diagonal matrix times a matrix of degree $2^k d$ in $\tilde{O}\left(\left(\frac{n}{2^k}\right)^\omega 2^{3k} d\right)$.

- $O(\log n)$ steps, $\tilde{O}(n^3 d + (n/2)^3(2d) + \dots + nd) = \tilde{O}(n^3 d)$.

3. DETERMINANT WITHOUT DIVISIONS



Matrix multiplication in n^3 ,



in n^ω

$A \in K^{n \times n}$.

[Strassen 73], $\tilde{O}(n^4)$, $\tilde{O}(n^{\omega+1})$

Removal of the divisions.

[Kaltofen 92], $\tilde{O}(n^{3+1/2})$, $O(n^{3.03})$

- Lanczos-Wiedemann approach, - removal of the divisions,
- baby step / giant step strategy.

[Kaltofen and Villard 2001-2002], $\tilde{O}(n^{3+1/5})$, $O(n^{2.7})$

- block Wiedemann strategy in above approach,
- Knuth-Schönage's half gcd computation.

Theorem. The **determinant**, the **characteristic polynomial** and the **adjoint** of an $n \times n$ matrix over \mathbb{R} can be computed in $O(n^{2.698})$ (or $\tilde{O}(n^{3+1/5})$ or $\tilde{O}(n^{3+1/3})$) **ring operations**. The algorithm is deterministic.

Corollary. The determinant, the characteristic polynomial and the Smith normal form of an $n \times n$ matrix over \mathbb{Z} can be computed in $O(n^{2.698})$ bit operations. The algorithm is Las Vegas randomized.

Lanczos-Wiedemann approach

$u^t v, u^t A v, u^t A^2 v, \dots, u^t A^{2n} v$ Berlekamp-Massey

Minimal polynomial of A ,

$$\pi(x) = x^d + p_{d-1}x^{d-1} + \dots + p_1x + p_0$$

↓

$B = DA$ has distinct eigenvalues, then,

Characteristic polynomial of $B =$ Minimal polynomial of B

$$\chi(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0$$

$$\det B = c_0 \quad \rightarrow \quad \det A$$

Block generalization.

$$U, V \in \mathbb{K}^{n \times m}, \quad U^t V, U^t A V, U^t A^2 V, \dots, U^t A^{2n/m} V$$

Matrix minimal polynomial :

$$x^d I + x^{d-1} C_{d-1} + \dots + C_0 \in \mathbb{K}[x]^{m \times m}, \quad \det A = \det C_0.$$

→ Less iterates thus smaller order truncated power series in Strassen's removing of divisions + block normal point.

Step 1. `/* Pre-conditioning */`

The minimal polynomial is different from the characteristic polynomial, its Frobenius form is :

$$F = \begin{bmatrix} 0 & 1 & & & & \\ 1 & 2 & & & & \\ & & 0 & 1 & & \\ & & 1 & 2 & & \\ & & & & 0 & 1 \\ & & & & 1 & 2 \end{bmatrix}$$



Random diagonal matrix
diag(1, 2, 3, 4, 5, 6)



The new matrix B and its Frobenius form :

$$B = \begin{bmatrix} 2 & -1 & -5 & -3 & -4 & 2 \\ -20 & -14 & 14 & 14 & 4 & -18 \\ -12 & -9 & 33 & 21 & 15 & -15 \\ -12 & -16 & -24 & -8 & -20 & -8 \\ 60 & 55 & -55 & -50 & -10 & 60 \\ 30 & 30 & 0 & -12 & 12 & 24 \end{bmatrix}, \quad F_B = \begin{bmatrix} & & & & & 720 \\ 1 & & & & & 2136 \\ & 1 & & & & -3480 \\ & & 1 & & & -1588 \\ & & & 1 & & 43 \\ & & & & 1 & 27 \end{bmatrix}.$$

Step 2.

/ Computation of the minimal matrix polynomial */*

/ Computation of the matrix sequence */*

$$C(x) = \begin{bmatrix} 13 & 8 \\ 8 & 14 \end{bmatrix}, \begin{bmatrix} 217 & 185 \\ 107 & 97 \end{bmatrix}, \begin{bmatrix} 11280 & 9937 \\ -109 & -137 \end{bmatrix}, \begin{bmatrix} 376483 & 329832 \\ 44410 & 39843 \end{bmatrix}$$

/ Matrix half-gcd */*

$$\begin{bmatrix} -\frac{174528786}{3457457} - \frac{8507719079}{17287285}x - \frac{3160837177}{17287285}x^2 + x^3 & -\frac{175402998}{3457457} - \frac{7511942372}{17287285}x - \frac{2766671371}{17287285}x^2 \\ -\frac{209510760}{3457457} + \frac{2483844884}{17287285}x + \frac{3074596254}{17287285}x^2 & -\frac{161245200}{3457457} + \frac{2070367712}{17287285}x + \frac{2694080482}{17287285}x^2 + x^3 \end{bmatrix}$$

Étape 3.

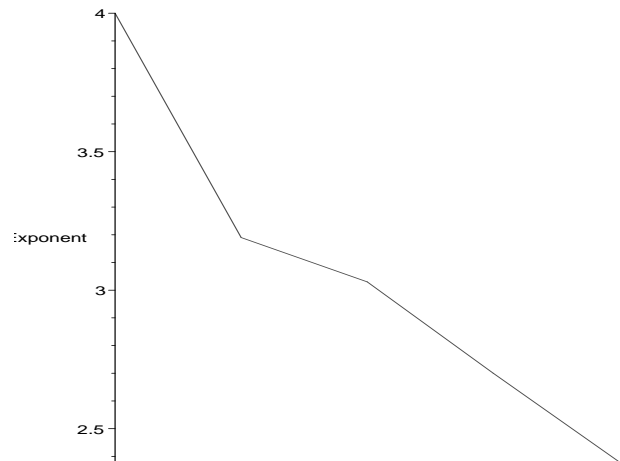
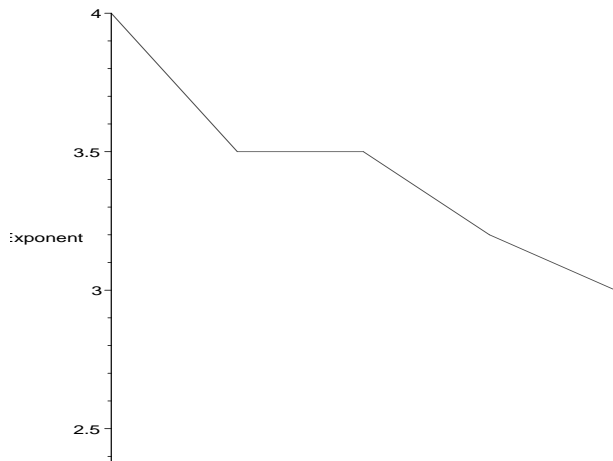
/ Recursive call, determinant of smaller dimension */*

$$\det C(0) = -720$$

Back to A i.e. “undo” the pre-conditioning :

$$\rightarrow \det A = -720/720 = -1.$$

4. BIT COMPLEXITY



Matrix multiplication in n^3 ,

in n^ω

$A \in \mathbb{Z}^{n \times n}$, up to $\tilde{O}(\log \|A\|)$

[Eberly, Giesbrecht and Villard, 2000], $\tilde{O}(n^{3.5})$, $\tilde{O}(n^{3.19})$.

Additive (rank k) matrix perturbations.

[Kaltofen 92-2000], $\tilde{O}(n^{3.5})$, $O(n^{3.03})$.

Baby step / giant step strategy.

[Kaltofen and Villard 2001-2002], $\tilde{O}(n^{3+1/5})$, $O(n^{2.7})$

Block strategy in above approach.

[Kaltofen 2002, Emiris and Pan 2002].

Output sensitive approach.

[Storjohann 2002], $\tilde{O}(n^3)$, $O(n^\omega)$

High order lifting.

EXTENSIONS
AND REMAINING PROBLEMS

Extensions

- Black box (structured, sparse . . .) matrix characteristic polynomial.
- Smith normal form computation.
- Parallel algorithms.

Remaining problems

	K	Ring	$K[x]$	\mathbb{Z}
$Ax = b$	n^ω	—	n^ω	n^ω
Det	n^ω	<u>$n^{2.7}$</u>	n^ω	n^ω
Inv (Adj)	n^ω	<u>$n^{2.7}$</u>	<u>$n^{\omega+1}$</u>	<u>$n^{\omega+1}$</u>