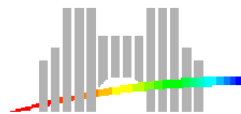


Algorithms for exact (dense) linear algebra

Gilles Villard

CNRS, Laboratoire LIP ENS Lyon

Montagnac-Montpezat, June 3, 2005



Introduction

Problem:

Study of **complexity estimates** for basic problems in exact **linear algebra** over $K[\mathbf{x}]$ and \mathbb{Z}

- ▷ Deterministic
 - Monte Carlo (non certified), Las Vegas (certified) randomized algorithms
- ▷ Time complexity
- ▷ Up to logarithmic factors, e.g. $O^{\sim}(n^c) = O(n^c \log^{\alpha} n)$
- ▷ (Space complexity)

Models

Algebraic complexity

K a commutative field, algebraic RAM: $+$, \times , $/$

Over $K[x]$, arithmetic operations in K

Bit complexity

Over \mathbb{Z} or \mathbb{Q} , bitwise computational cost

Motivations

- ↪ Complexity estimates with “concrete” entry domain
- ↪ Better understanding of linear algebra in bit complexity
- ↪ Improved algorithms for exact (or accurate) results

The talk

Introduction

I - Known reductions between problems

II - Divide-double and conquer

III - Matrix polynomials

IV - Integer matrices

Conclusion

The talk

Introduction

I - Known reductions between problems

II - Divide-double and conquer

III - Matrix polynomials

IV - Integer matrices

Conclusion

Algebraic complexity over K

[Survey and more in Bürgisser *et al.* 1997, Ch. 16]

Asymptotic **equivalence** to **matrix multiplication**

Matrix multiplication $n \times n$
 $A \times B$

$O(\mathbf{n}^\omega)$, $O(n^3)$ or $O(n^{2.376})$

**Determinant, inversion,
rank, characteristic polynomial**

...

Algorithms in $\tilde{O}(\mathbf{n}^\omega)$

Algebraic complexity over K

[Survey and more in Bürgisser *et al.* 1997, Ch. 16]

Asymptotic **equivalence** to **matrix multiplication**

Matrix multiplication $n \times n$
 $A \times B$

$O(\mathbf{n}^\omega)$, $O(n^3)$ or $O(n^{2.376})$

**Determinant, inversion,
rank, characteristic polynomial**

...

Algorithms in $O(\mathbf{n}^\omega)$

LinSys \preceq **MM** \approx **Det**

Example 1.

$\text{Det}_K \implies \text{Inversion}_K$

Example 1.

Det $\kappa \implies$ Inversion κ

Proof. **Derivative inequality** [Baur and Strassen, 1983]

$$\det A = a_{11} \det A_{2..n,2..n} + \dots, \text{ hence } \frac{\partial \det A}{\partial a_{11}} = \det A_{2..n,2..n}$$

$$A^{-1} = \frac{A^*}{\det A}, \quad a_{j,i}^* = \frac{\partial \det A}{\partial a_{i,j}}$$

↪ Does not carry over to the **polynomial** or **bit complexity case**

x, y two vectors with fixed size entries

c an n -bits integer

Compute $\phi = c \cdot x^T \cdot y$, $O(\mathbf{n})$ bit operations

↪ Does not carry over to the **polynomial** or **bit complexity case**

x, y two vectors with fixed size entries

c an n -bits integer

Compute $\phi = c \cdot x^T \cdot y$, $O(\mathbf{n})$ bit operations

Compute $[\partial\phi/\partial x_i]_{1 \leq i \leq n} = c \cdot y$, $O(\mathbf{n}^2)$ bit operations

Example 2.

$$\text{MM}_K \implies \text{CharPoly}_K$$

Example 2.

$$\text{MM}_K \implies \text{CharPoly}_K$$

Proof. **Minimum polynomial** [Keller-Gehrig, 1985]

$$A \in K^{n \times n}, u \in K^n$$

Example 2.

$$\text{MM}_K \implies \text{CharPoly}_K$$

Proof. **Minimum polynomial** [Keller-Gehrig, 1985]

$$A \in K^{n \times n}, u \in K^n$$

$$A \cdot u \rightarrow [u, Au]$$

Example 2.

$$\text{MM}_K \implies \text{CharPoly}_K$$

Proof. **Minimum polynomial** [Keller-Gehrig, 1985]

$$A \in K^{n \times n}, u \in K^n$$

$$A \cdot u \rightarrow [u, Au]$$

$$A^2 \cdot [u, Au] \rightarrow [u, Au, A^2u, A^3u] \rightarrow A^4 \cdot [u, Au, A^2u, A^3u]$$

Example 2.

$$\text{MM}_K \implies \text{CharPoly}_K$$

Proof. **Minimum polynomial** [Keller-Gehrig, 1985]

$$A \in K^{n \times n}, u \in K^n$$

$$A \cdot u \rightarrow [u, Au]$$

$$A^2 \cdot [u, Au] \rightarrow [u, Au, A^2u, A^3u] \rightarrow A^4 \cdot [u, Au, A^2u, A^3u]$$

$$\dots \text{repeated squaring} \dots \rightarrow [u, Au, A^2u, A^3u, \dots, A^d u]$$

Example 2.

$$\text{MM}_K \implies \text{CharPoly}_K$$

Proof. **Minimum polynomial** [Keller-Gehrig, 1985]

$$A \in K^{n \times n}, u \in K^n$$

$$A \cdot u \rightarrow [u, Au]$$

$$A^2 \cdot [u, Au] \rightarrow [u, Au, A^2u, A^3u] \rightarrow A^4 \cdot [u, Au, A^2u, A^3u]$$

$$\dots \text{repeated squaring} \dots \rightarrow [u, Au, A^2u, A^3u, \dots, A^d u]$$

$$A^d u + c_{d-1} A^{d-1} u + \dots + c_0 u = 0 \implies \pi(\mathbf{x}) = x^d + c_{d-1} x^{d-1} + \dots + c_0$$

↪ Does not carry over to the **polynomial** or **bit complexity case**

A of size $\log \|A\|$

$A^{n/2}$ has entries of size $O(n \log \|A\|)$

The multiplication by $A^{n/2}$ costs $O(n^\omega \times n \log \|A\|) = O(n^{\omega+1} \log \|A\|)$

Impact of data size ?

Ex. Determinant computation/Output size : $\mathbf{n}d$ or $O(\mathbf{n} \log \|A\|)$,

Evaluation/interpolation or homomorphic scheme

or $O(\mathbf{n} \log \|A\|)$ bits *a priori* :

↑
 \mathbf{n}^ω
↓



Impact of data size ?

Ex. Determinant computation/Output size : $\mathbf{n}d$ or $O(\mathbf{n} \log \|A\|)$,

Evaluation/interpolation or homomorphic scheme

or $O(\mathbf{n} \log \|A\|)$ bits *a priori* :

← $\mathbf{n}d$ points or $O(\mathbf{n} \log \|A\|)$ bits →

↑
 \mathbf{n}^ω
↓



Impact of data size ?

Ex. Determinant computation/Output size : nd or $O(\mathbf{n} \log \|A\|)$,

Evaluation/interpolation or homomorphic scheme

or $O(n \log \|A\|)$ bits *a priori* :

← nd points or $O(\mathbf{n} \log \|A\|)$ bits →

Complexity estimates:

↑
 \mathbf{n}^ω
↓

$$O(n^\omega \times nd) = O(\mathbf{n}^{\omega+1} d)$$
$$O(\mathbf{n}^{\omega+1} \log \|A\|)$$

- ▷ **MM**(\mathbf{n}, \mathbf{d}) = $O^{\sim}(n^{\omega} d)$: cost for multiplying $n \times n$ matrices of degree d
- ▷ **MM**($\mathbf{n}, \log \|\mathbf{A}\|\|$) = $O^{\sim}(n^{\omega} \log \|A\|\|)$: cost for multiplying $n \times n$ integer matrices
(general case: consider generalized functions $\overline{\text{MM}}$)

Previous analysis shows that the **determinant** may be computed in $O(n \cdot \text{MM}(n, d))$ or $O(n \cdot \text{MM}(n, \log \|A\|\|))$ operations, *i.e.* in **n corresponding matrix products**

Fundamentals of dense linear algebra over $K[x]$ or \mathbb{Z} (1967 \rightarrow 2000) :

Monte Carlo rank

$$O(n^\omega + n^2 \log \|A\|)$$

System solution (Hensel lifting)

$$O^\sim(n^3 \log \|A\|)$$

[Moenck & Carter 79, Dixon 82]

Determinant, inversion, nullspace, rank, . . .

$$O^\sim(\mathbf{n} \cdot \text{MM}(n, \log \|A\|))$$

[Edmonds 67, Bareiss 69, Moenck & Carter 79]

Deterministic

Frobenius form (minimum, **characteristic polynomial**)

$$O^\sim(\mathbf{n} \cdot \text{MM}(n, \log \|A\|))$$

[Giesbrecht 93, Giesbrecht & Storjohann 02]

Las Vegas

Hermite and Smith forms (diophantine systems)

$$O^\sim(\mathbf{n} \cdot \text{MM}(n, \log \|A\|))$$

[Kannan & Bachem 79, Domich 85, Giesbrecht 95, Storjohann 96-00]

Deterministic

Bit complexity \preceq algebraic complexity \times output size

Bit complexity \preceq algebraic complexity \times output size

Is this bound pessimistic?

$$\text{Bit complexity} \preceq \text{algebraic complexity} \times \text{output size}$$

Is this bound pessimistic?

Clue. The output length may not be necessary *a priori*, i.e. at the beginning of the computation, but only at its very end.

Reduction to matrix multiplication

Question: Which dense linear algebra problems over $K[x]$ or \mathbb{Z} can be solved by algorithms using “about” the same number of operations as for multiplying two corresponding matrices plus the input/output size?

The talk

Introduction

I - Known reductions between problems

II - Divide-double and conquer

III - Matrix polynomials

IV - Integer matrices

Conclusion

Triangularization in $\log_2(n)$ steps

$$A = \begin{bmatrix} * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \end{bmatrix}$$

Triangularization in $\log_2(n)$ steps

$$LA = \begin{bmatrix} * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ & & & & * & * & * & * \\ & & & & * & * & * & * \\ & & & & * & * & * & * \\ & & & & * & * & * & * \end{bmatrix}$$

Triangularization in $\log_2(n)$ steps

$$L'LA = \begin{bmatrix} * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * \\ & & * & * & * & * & * & * \\ & & * & * & * & * & * & * \\ & & & * & * & * & * & * \\ & & & & * & * & * & * \\ & & & & * & * & * & * \\ & & & & & * & * & * \\ & & & & & & * & * \\ & & & & & & * & * \end{bmatrix}$$

Triangularization in $\log_2(n)$ steps

$$L''L'LA = \begin{bmatrix} * & * & * & * & * & * & * & * \\ & * & * & * & * & * & * & * \\ & & * & * & * & * & * & * \\ & & & * & * & * & * & * \\ & & & & * & * & * & * \\ & & & & & * & * & * \\ & & & & & & * & * \\ & & & & & & & * \\ & & & & & & & & * \end{bmatrix} = T$$

Divide and conquer

[Strassen 1969, Schönhage 1973, Bunch & Hopcroft 1974]

$$\begin{bmatrix} I & 0 \\ -BA^{-1} & I \end{bmatrix} \cdot \begin{bmatrix} A & C \\ B & D \end{bmatrix} = \begin{bmatrix} A & C \\ 0 & D - BA^{-1}C \end{bmatrix}$$

At next step :

↪ Dimension: divided by two

Divide and conquer

[Strassen 1969, Schönhage 1973, Bunch & Hopcroft 1974]

$$\begin{bmatrix} I & 0 \\ -BA^{-1} & I \end{bmatrix} \cdot \begin{bmatrix} A & C \\ B & D \end{bmatrix} = \begin{bmatrix} A & C \\ 0 & D - BA^{-1}C \end{bmatrix}$$

At next step :

↪ Dimension: divided by two

↪ **Entry size : multiplied by $n/2$**

Divide-double and conquer

[Jeannerod & Villard 2002, Storjohann 2002]

The **dimension is divided by two** while the **entry size is at most doubled**

$$\Rightarrow \text{Cost: } \sum_{i=1}^{\log n} \left(\frac{n}{2^i}\right)^\omega 2^i d = O(\mathbf{n}^\omega \mathbf{d})$$

$$A = \begin{bmatrix} -85 & -55 & -37 & -35 \\ 49 & 63 & 57 & -59 \\ 43 & -62 & 77 & 66 \\ -50 & -12 & -18 & 31 \\ -91 & -47 & -61 & 41 \\ 94 & 83 & -86 & 23 \\ -53 & 85 & 49 & 78 \\ -86 & 30 & 80 & 72 \end{bmatrix}$$

(Left) nullspace? $N \cdot A = 0$?

Gaussian elimination (Schur complement):

$$N_g = \begin{bmatrix} 7646610 & -17525750 & -3967680 & 29755220 & \dots\dots \\ -15181842 & 13894262 & 0 & -40184660 & \dots\dots \\ -2804568 & 4081928 & 0 & 18871120 & \dots\dots \\ 4368828 & -4023028 & 0 & 35835160 & \dots\dots \end{bmatrix}$$

Gaussian elimination (Schur complement):

$$N_g = \begin{bmatrix} 7646610 & -17525750 & -3967680 & 29755220 & \dots\dots \\ -15181842 & 13894262 & 0 & -40184660 & \dots\dots \\ -2804568 & 4081928 & 0 & 18871120 & \dots\dots \\ 4368828 & -4023028 & 0 & 35835160 & \dots\dots \end{bmatrix}$$

However, one can choose instead (and compute over $K[x]$):

$$N = \begin{bmatrix} -25 & -32 & -16 & -38 & 1 & -30 & 32 & -33 \\ -27 & -68 & -43 & 23 & -71 & -1 & -55 & 61 \\ 106 & -43 & 28 & -95 & -50 & 30 & 53 & -7 \\ -23 & -25 & -12 & 182 & -90 & -40 & 36 & -74 \end{bmatrix}$$

Example: for **inversion** and **nullspace**

$$\begin{bmatrix} A(x) \end{bmatrix} \in \mathbb{K}[x]^{2n \times n} \text{ of degree } d$$

Divide and conquer

Gaussian elimination

$$N(x) \cdot A(x) = 0$$

$$N(x) \in \mathbb{K}[x]^{2n \times n} \text{ of degree } O(nd)$$

$$\text{Total size: } O(n^3d)$$

Example: for **inversion** and **nullspace**

$$\begin{bmatrix} A(x) \end{bmatrix} \in \mathbb{K}[x]^{2n \times n} \text{ of degree } d$$

Divide and conquer

Gaussian elimination

$$N(x) \cdot A(x) = 0$$

$$N(x) \in \mathbb{K}[x]^{2n \times n} \text{ of degree } O(nd)$$

$$\text{Total size: } O(n^3d)$$

Divide-double and conquer

Minimal module bases

$$M(x) \cdot A(x) = 0$$

$$M(x) \in \mathbb{K}[x]^{2n \times n} \text{ with degree sum } O(nd) \\ \text{e.g. generically degree } d \text{ (Kronecker indices)}$$

$$\text{Total size: } O(\mathbf{n^2d})$$

Theorem:

The **rank** r of $M \in \mathbb{K}[x]^{n \times n}$ (degree d) and $n - r$ independent **nullspace** vectors can be computed in $O^\sim(\mathbf{MM}(\mathbf{n}, \mathbf{d})) = O^\sim(n^\omega d)$ operations in \mathbb{K} by a randomized **Las Vegas** (certified) algorithm.

[Storjohann & Villard, 2005]

The talk

Introduction

I - Known reductions between problems

II - Divide-double and conquer

III - Matrix polynomials

IV - Integer matrices

Conclusion

Matrix polynomial inversion, degree d over $K[x]$

Over K :

Input/output size: \mathbf{n}^2 / Cost: \mathbf{n}^3 , n^ω
 $A^{-1} = B$.

Over $K(x)$, output degree nd ,

Output size: \mathbf{n}^3d / Cost (e.g. Newton): \mathbf{n}^4d , $n^{\omega+1}d$

$$A^{-1}(x) = A^*(x) / \det A(x) = (B_0 + xB_1 + \dots + x^{nd-1}B_{nd-1}) / \det A(x)$$

Using minimal bases

Theorem:

The generic **matrix inverse** of a polynomial matrix (degree d) can be computed in essentially optimal time $O^{\sim}(\mathbf{n}^3\mathbf{d})$.

[Jeannerod & Villard, 2002-2005]

Using minimal bases

Theorem:

The generic **matrix inverse** of a polynomial matrix (degree d) can be computed in essentially optimal time $O^{\sim}(\mathbf{n}^3\mathbf{d})$.

[Jeannerod & Villard, 2002-2005]

Corollary:

For a generic $A \in K^{n \times n}$, the **matrix powers** A, A^2, \dots, A^n , can be computed in essentially optimal time $O^{\sim}(\mathbf{n}^3\mathbf{d})$.

Hint: $(I - xA)^{-1} = \sum_{i=0}^{\infty} x^i A^i$.

Using high order lifting

$$A(x) \longrightarrow \text{unimodular transforms} \longrightarrow \begin{bmatrix} s_1(x) & & & \\ & s_2(x) & & \\ & & \dots & \\ & & & s_n(x) \end{bmatrix}$$

Theorem:

The **Smith normal form**, hence the **determinant** of $M \in \mathbb{K}[x]^{n \times n}$ (degree d) can be computed in $O^\sim(\text{MM}(\mathbf{n}, \mathbf{d})) = O^\sim(n^\omega d)$ operations in \mathbb{K} by a randomized **Las Vegas** (certified) algorithm.

[Storjohann, 2002-2003]

Using high order lifting and minimal bases

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

Theorem:

A **basis** ($n \times n$, degree d) of a $K[x]$ -module can be **reduced** in $O^{\sim}(\mathbf{MM}(\mathbf{n}, \mathbf{d})) = O^{\sim}(n^{\omega}d)$ operations in K by a randomized **Las Vegas** (certified) algorithm (cf also the matrix Gcd, and matrix Padé approximants).

[Giorgi, Jeannerod & Villard, 2003]

The talk

Introduction

I - Known reductions between problems

II - Divide-double and conquer

III - Matrix polynomials

IV - Integer matrices

Conclusion

Fact: The known improvements in **bit complexity** “come from” corresponding improvements over the polynomials (or truncated power series).

Example 1. “**Correspondence**” between $K[x]$ and \mathbb{Z}

Multiplication

$M(d) = O(d \log d \log \log d) = \tilde{O}(d)$: product in $K[x]$

$M(\log |a|) = M(s) = O(s \log s \log \log s) = \tilde{O}(s)$: product in \mathbb{Z}

Example 1. “Correspondence” between $K[x]$ and \mathbb{Z}

Multiplication

$M(d) = O(d \log d \log \log d) = O^\sim(d)$: product in $K[x]$

$M(\log |a|) = M(s) = O(s \log s \log \log s) = O^\sim(s)$: product in \mathbb{Z}



Gcd

[Knuth/Schönhage 1970-1971]

Gcd in $K[x]$: $O(M(d) \log d)$

Gcd in \mathbb{Z} : $O(M(s) \log s)$

Example 2. Characteristic polynomial, “correspondence” between \mathbb{R} and $\mathbb{Z}^{n \times n}$

Best known estimations for the **determinant without divisions** carry over to the integer case, and lead to the characteristic polynomial

Example 2. Characteristic polynomial, “correspondence” between R and $\mathbb{Z}^{n \times n}$

Best known estimations for the **determinant without divisions** carry over to the integer case, and lead to the characteristic polynomial

↔ Algebraic without divisions, R

One tries to limit the **degree increase**

↔ Bit complexity, \mathbb{Z}

One tries to limit the **size increase**

Strassen's transformation for eliminating divisions works over $K[[x]]$

$$A \rightarrow I + x(A - I)$$

Reducing the cost over $K[[x]] \implies$ reducing the bit complexity

\rightsquigarrow **Determinant without division** over R

$$\text{Det}_K \preceq \text{Det}_R$$

[Strassen 1973, *Vermeidung von Divisionen*] $O^\sim(n^{\omega+1})$

[(Le Verrier) Samuelson/Berkowitz, 1984] [Chistov, 1985]

[Kaltofen, 1992] $O^\sim(n^{3+1/2})$, $O(n^{3.03})$

[Kaltofen & Villard, 2002-2005] $O^\sim(n^{3+1/5})$, **$O(n^{2.7})$**

Baby steps/Giant steps and elimination of the divisions, over \mathbb{Z}

[Shanks, Kaltofen 1992, Kaltofen & Villard 2002-2005]

$$u^T A^k v, \quad k = 0, \dots, n-1, \quad A \in \mathbb{Z}^{n \times n}, u, v \in \mathbb{Z}^n?$$

Baby steps/Giant steps and elimination of the divisions, over \mathbb{Z}

[Shanks, Kaltofen 1992, Kaltofen & Villard 2002-2005]

$$u^T A^k v, \quad k = 0, \dots, n-1, \quad A \in \mathbb{Z}^{n \times n}, u, v \in \mathbb{Z}^n?$$

$$v, Av, \dots, A^{\sqrt{n}-1}v \quad \mathbf{n^2 \sqrt{n} \times \sqrt{n}}$$

Baby steps/Giant steps and elimination of the divisions, over \mathbb{Z}

[Shanks, Kaltofen 1992, Kaltofen & Villard 2002-2005]

$$u^T A^k v, \quad k = 0, \dots, n-1, \quad A \in \mathbb{Z}^{n \times n}, u, v \in \mathbb{Z}^n?$$

$$v, Av, \dots, A^{\sqrt{n}-1}v \quad \mathbf{n^2 \sqrt{n} \times \sqrt{n}}$$

$$B = A^{\sqrt{n}} \quad \mathbf{n^3 \times \sqrt{n}}$$

Baby steps/Giant steps and elimination of the divisions, over \mathbb{Z}

[Shanks, Kaltofen 1992, Kaltofen & Villard 2002-2005]

$$u^T A^k v, \quad k = 0, \dots, n-1, \quad A \in \mathbb{Z}^{n \times n}, u, v \in \mathbb{Z}^n?$$

$$v, Av, \dots, A^{\sqrt{n}-1}v \quad \mathbf{n^2 \sqrt{n} \times \sqrt{n}}$$

$$B = A^{\sqrt{n}} \quad \mathbf{n^3 \times \sqrt{n}}$$

$$u^T, u^T B, \dots, u^T B^{\sqrt{n}-1} \quad \mathbf{n^2 \sqrt{n} \times n}$$

Baby steps/Giant steps and elimination of the divisions, over \mathbb{Z}

[Shanks, Kaltofen 1992, Kaltofen & Villard 2002-2005]

$$u^T A^k v, \quad k = 0, \dots, n-1, \quad A \in \mathbb{Z}^{n \times n}, u, v \in \mathbb{Z}^n?$$

$$v, Av, \dots, A^{\sqrt{n}-1}v \quad \mathbf{n^2 \sqrt{n} \times \sqrt{n}}$$

$$B = A^{\sqrt{n}} \quad \mathbf{n^3 \times \sqrt{n}}$$

$$u^T, u^T B, \dots, u^T B^{\sqrt{n}-1} \quad \mathbf{n^2 \sqrt{n} \times n}$$

$$u^T B^i A^j v = u^T A^k v, \quad i = 0, \dots, \sqrt{n}-1, \quad j = 0, \dots, \sqrt{n}-1 \quad \mathbf{n^2 \times n}$$

Baby steps/Giant steps and elimination of the divisions, over \mathbb{Z}

[Shanks, Kaltofen 1992, Kaltofen & Villard 2002-2005]

$$u^T A^k v, \quad k = 0, \dots, n-1, \quad A \in \mathbb{Z}^{n \times n}, u, v \in \mathbb{Z}^n?$$

$$v, Av, \dots, A^{\sqrt{n}-1}v \quad \mathbf{n^2 \sqrt{n} \times \sqrt{n}}$$

$$B = A^{\sqrt{n}} \quad \mathbf{n^3 \times \sqrt{n}}$$

$$u^T, u^T B, \dots, u^T B^{\sqrt{n}-1} \quad \mathbf{n^2 \sqrt{n} \times n}$$

$$u^T B^i A^j v = u^T A^k v, \quad i = 0, \dots, \sqrt{n}-1, \quad j = 0, \dots, \sqrt{n}-1 \quad \mathbf{n^2 \times n}$$

\Rightarrow Characteristic polynomial in time $O(\mathbf{n^{3+\sqrt{n}} \log \|\mathbf{A}\|})$ or $\dots O(\mathbf{n^{2.7} \log \|\mathbf{A}\|})$

Example 3. “**Correspondence**” between $K[x]$ and \mathbb{Z}

Linear system solution

$$A(x)Y(x) = b(x), K[x]$$

$$AY = b, \mathbb{Z}$$

Example 3. “Correspondence” between $K[x]$ and \mathbb{Z}

Linear system solution

$$A(x)Y(x) = b(x), K[x]$$

$$AY = b, \mathbb{Z}$$

$$B = A_0^{-1}(\text{mod } x)$$

$$B = A^{-1} \text{ mod } p$$

Example 3. “**Correspondence**” between $K[x]$ and \mathbb{Z}

Linear system solution

$$A(x)Y(x) = b(x), K[x]$$

$$AY = b, \mathbb{Z}$$

$$B = A_0^{-1}(\text{mod } x)$$

$$B = A^{-1} \text{ mod } p$$

$$By_{i+1} = r_i(\text{mod } x)$$

$$By_{i+1} = r_i \text{ mod } p$$

Example 3. “Correspondence” between $K[x]$ and \mathbb{Z}

Linear system solution

$$A(x)Y(x) = b(x), K[x]$$

$$AY = b, \mathbb{Z}$$

$$B = A_0^{-1}(\text{mod } x)$$

$$B = A^{-1} \text{ mod } p$$

$$\begin{aligned} By_{i+1} &= r_i(\text{mod } x) \\ r_{i+1} &= (A(x)y_{i+1} - b(x))/x \end{aligned}$$

$$\begin{aligned} By_{i+1} &= r_i \text{ mod } p \\ r_{i+1} &= (Ay_{i+1} - b)/p \end{aligned}$$

Example 3. “Correspondence” between $K[x]$ and \mathbb{Z}

Linear system solution

$$A(x)Y(x) = b(x), K[x]$$

$$AY = b, \mathbb{Z}$$

$$B = A_0^{-1}(\text{mod } x)$$

$$B = A^{-1} \text{ mod } p$$

$$\begin{aligned} By_{i+1} &= r_i(\text{mod } x) \\ r_{i+1} &= (A(x)y_{i+1} - b(x))/x \end{aligned}$$

$$\begin{aligned} By_{i+1} &= r_i \text{ mod } p \\ r_{i+1} &= (Ay_{i+1} - b)/p \end{aligned}$$

$$\text{LinSys}_{K[x]}(n, d) = O^{\sim}(\mathbf{MM}(\mathbf{n}, \mathbf{d}))$$

$$\text{LinSys}_{\mathbb{Z}}(n, \log \|A\|) = O^{\sim}(\mathbf{MM}(\mathbf{n}, \log \|\mathbf{A}\|)) \text{ [Storjohann 2002-2005]}$$

Theorem:

The **Smith normal form** of $A \in \mathbb{Z}^{n \times n}$, hence the **determinant**, can be computed in $O^{\sim}(\text{MM}(\mathbf{n}, \log \|A\|)) = O^{\sim}(n^{\omega} \log \|A\|)$ operations in K by a randomized **Las Vegas** (certified) algorithm.

[Storjohann, 2004-2005]

Proof.

Fast system solution (correction of the residue / p -adic lifting)

Divide-double and conquer (based on the sizes of the invariant factors)

The talk

Introduction

I - Known reductions between problems

II - Divide-double and conquer

III - Matrix polynomials

IV - Integer matrices

Conclusion

▷ Classical open problems, algebraic complexity

Determinant without divisions in $O^\sim(n^\omega)$?

Reduction of matrix multiplication to **system solution**?

▷ Open problems, $K[x]$ or bit complexity

Small nullspace bases in $O^\sim(n^\omega \log \|A\|)$? (\mathbb{Z})

Essentially optimal **inversion**?

New **reductions** to matrix multiplication?