Certifying the rank of an integer matrix

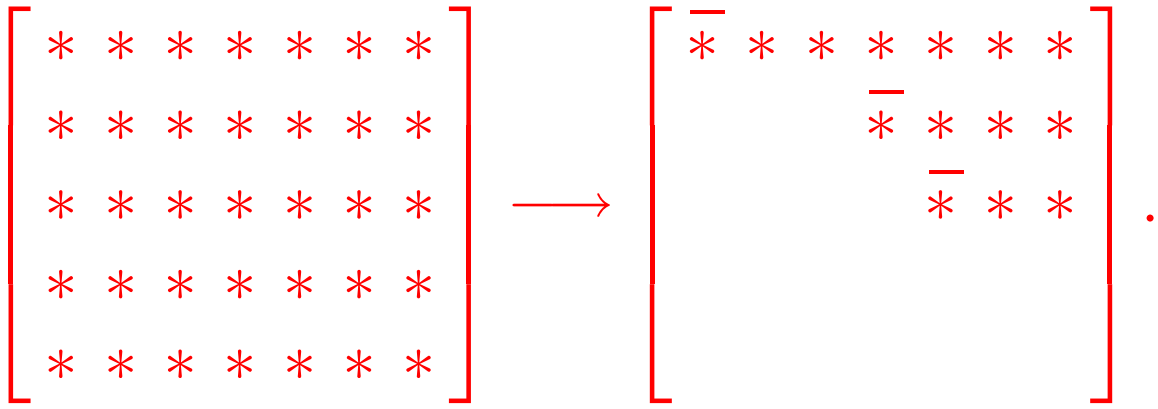
Arne Storjohann
David R. Cheriton School of Computer Science
University of Waterloo

Integer Matrix Rank

Input: an $n \times n$ integer matrix A

Output: the rank of A

Relationship with the row echeon form



$\longrightarrow$ the rank is equal to the number of nonzero rows

Cost of Integer Matrix Multiplication

Input: $n \times n$ matrices A and B filled with entries of size d digits

Output: $C := AB$

Cost: $\tilde{O}(n^3 d)$ bit operations

$$\underset{A}{\begin{bmatrix} 91 & 70 & 66 & 77 \\ 50 & 52 & 11 & 18 \\ 62 & 39 & 89 & 2 \\ 48 & 48 & 66 & 73 \end{bmatrix}} \underset{B}{\begin{bmatrix} 89 & 73 & 26 & 97 \\ 71 & 1 & 72 & 84 \\ 40 & 3 & 43 & 12 \\ 18 & 9 & 14 & 63 \end{bmatrix}} = \underset{C}{\begin{bmatrix} 17095 & 7604 & 11322 & 20350 \\ 8906 & 3897 & 5769 & 10484 \\ 11883 & 4850 & 8275 & 10484 \\ 11634 & 4407 & 8564 & 14079 \end{bmatrix}}$$

Cost of Integer Matrix Multiplication

Input: $n \times n$ matrices A and B filled with entries of size d digits

Output: $C := AB$

Cost: $\tilde{O}(n^3 d)$ bit operations

$$\underset{A}{\begin{bmatrix} 91 & 70 & 66 & 77 \\ 50 & 52 & 11 & 18 \\ 62 & 39 & 89 & 2 \\ 48 & 48 & 66 & 73 \end{bmatrix}} \underset{B}{\begin{bmatrix} 89 & 73 & 26 & 97 \\ 71 & 1 & 72 & 84 \\ 40 & 3 & 43 & 12 \\ 18 & 9 & 14 & 63 \end{bmatrix}} = \underset{C}{\begin{bmatrix} 17095 & 7604 & 11322 & 20350 \\ 8906 & 3897 & 5769 & 10484 \\ 11883 & 4850 & 8275 & 10484 \\ 11634 & 4407 & 8564 & 14079 \end{bmatrix}}$$

Major effort in past decade

Reduce cost of linear algebra over $\mathbb{Z}$ to matrix multiplication

Classical		Goal
$\tilde{O}(n^4 d)$	$\longrightarrow$	$\tilde{O}(n^3 d)$

Randomized Monte Carlo Rank Computation
$\longrightarrow$ aways fast, probably correct

Input: an $n \times n$ matrix A filled with integers of size d digits

Output: the rank of A

Classical approach using a signature function

1. Choose random prime p with $\log p \in O(\log n + \log d)$
2. Compute modular reduction: $B := A \bmod p \in \mathbb{Z}/(p)^{n \times n}$
3. Compute rank of B over $\mathbb{Z}/(p)$ using gaussian elimination

Cost assuming standard matrix multiplication is

$$\tilde{O}(n^3 + n^2 d)$$

bit operations.

Deterministic Rank Computation

Classical: $\tilde{O}(n^4 d)$ bit operations

$\longrightarrow$ gaussian elimination over $\mathbb{Q}$, or
$\longrightarrow$ fraction free gaussian elimination, or
$\longrightarrow$ signature function approach with $\tilde{O}(n)$ different primes

Randomized Las Vegas Rank Computation

$\longrightarrow$ aways correct, probably fast

Previous best: $\tilde{O}(n^{3.2} d)$ bit operations

$\longrightarrow$ trace certificate with fast characteristic polynomial algorithm

[2004, Saunders, Storjohann & Villard, *Matrix Rank Certification*]

[2005, Katofen & Villard, *Complexity of Computing Determinants*]

ISSAC 2009: $\tilde{O}(n^3 d)$ bit operations

Motivation: Problems at Least as Difficult as Rank

Hermite form

$$H = UA = \begin{bmatrix} h_1 & * & * & \bar{*} & \bar{*} & * & * \\ & & & h_2 & \bar{*} & * & * \\ & & & & h_3 & * & * \\ & & & & & & \\ & & & & & & \\ & & & & & & \\ & & & & & & \end{bmatrix}.$$

Smith form

$$S = VAW = \begin{bmatrix} s_1 & & & \\ & s_2 & & \\ & & \ddots & \\ & & & s_r \end{bmatrix}$$

Frobenius form

$$F = PAP^{-1} = \begin{bmatrix} C_{f_1} & & & \\ & C_{f_2} & & \\ & & \ddots & \\ & & & C_{f_l} \end{bmatrix}$$

Lattice reduction

$$B = TA = \begin{bmatrix} * & * & * & * & * & * & * \\ * & * & * & * & * & * & * \\ * & * & * & * & * & * & * \\ & & & & & & \\ & & & & & & \\ & & & & & & \\ & & & & & & \end{bmatrix}$$

The Rank Certification Problem

Input: $M := \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] \in \mathbb{Z}^{2n\times 2n}$ with $A \in \mathbb{Z}^{n\times n}$ nonsingular.

Equivalent questions:

- Is the rank of M equal to n?
- Does the nullspace of M have dimension n?
- Is $D - CA^{-1}B$ the zero matrix?

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

Output: (“True”, $CA^{-1}B = D$) or (“False”, $CA^{-1}B \neq D$)

A Concrete Example

$$\textbf{Input: } M := \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] = \left[\begin{array}{ccc|ccc} 6 & 40 & 23 & 12 & 7 & 18 \\ 24 & 45 & 30 & 30 & 18 & 12 \\ 37 & 51 & 38 & 44 & 27 & 8 \\ \hline 43 & 50 & 40 & 50 & 31 & 4 \\ 41 & 116 & 74 & 58 & 35 & 40 \\ 76 & 127 & 101 & 98 & 63 & 22 \end{array}\right]$$

$$\text{rank } M = 3$$

$\Longleftrightarrow$

$$\underset{C}{\begin{bmatrix} 43 & 50 & 40 \\ 41 & 116 & 74 \\ 76 & 127 & 101 \end{bmatrix}} \underset{A^{-1}}{\begin{bmatrix} -\frac{20}{127} & \frac{347}{1143} & -\frac{55}{381} \\ -\frac{22}{127} & \frac{623}{1143} & -\frac{124}{381} \\ \frac{49}{127} & -\frac{1174}{1143} & \frac{230}{381} \end{bmatrix}} \underset{B}{\begin{bmatrix} 12 & 7 & 18 \\ 30 & 18 & 12 \\ 44 & 27 & 8 \end{bmatrix}} = \underset{D}{\begin{bmatrix} 50 & 31 & 4 \\ 58 & 35 & 40 \\ 98 & 63 & 22 \end{bmatrix}}$$

$\Longleftrightarrow$

$$\underset{C}{\begin{bmatrix} 43 & 50 & 40 \\ 41 & 116 & 74 \\ 76 & 127 & 101 \end{bmatrix}} \underset{A^{-1} \bmod 10^{11}}{\begin{bmatrix} 39370078740 & 7436570429 & 86089238845 \\ 43307086614 & 47069116361 & 81364829396 \\ 53543307087 & 90113735782 & 49081364830 \end{bmatrix}} \underset{B}{\begin{bmatrix} 12 & 7 & 18 \\ 30 & 18 & 12 \\ 44 & 27 & 8 \end{bmatrix}} \equiv \underset{D}{\begin{bmatrix} 50 & 31 & 4 \\ 58 & 35 & 40 \\ 98 & 63 & 22 \end{bmatrix}} \bmod 10^{11}$$

A Smaller Concrete Example

Input: $M := \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right] = \left[\begin{array}{c|c} 21 & 14 \\ \hline 6 & 4 \end{array}\right]$

$$\begin{aligned} \operatorname{rank} M = 1 &\iff CA^{-1}B = D \\ &\iff 6 \cdot \frac{1}{21} \cdot 14 = 4 \\ &\iff 6 \cdot \operatorname{rem}(21^{-1}, 10^{32}) \cdot 14 \equiv 4 \bmod 10^{32} \end{aligned}$$

$$\begin{aligned} 6 \cdot \operatorname{rem}(21^{-1}, 10^{32}) \cdot 14 &= 6 \cdot 80952380952380952380952380952381 \cdot 14 \\ &= 68000000000000000000000000000004 \\ &= 4 + 68 \cdot 10^{32}. \end{aligned}$$

Reduction of Problem Order

$$6 \cdot \mathrm{rem}(21^{-1}, 10^{32}) \cdot 14 = 6 \cdot \overbrace{80952380952380}^{H}\overbrace{95}^{L}\overbrace{2380952380952381}^{L} \cdot 14$$

$$= (6 \cdot L \cdot 14) + (6 \cdot H \cdot 10^{16} \cdot 14)$$
$$= (4 + 20 \cdot 10^{16}) + (-20 \cdot 10^{16} + 68 \cdot 10^{32})$$

Reduction of Problem Order

$$6 \cdot \mathrm{rem}(21^{-1}, 10^{32}) \cdot 14 = 6 \cdot \overbrace{80952380952380}^{H}\overbrace{952380952381}^{L} \cdot 14$$

$$= (6 \cdot L \cdot 14) + (6 \cdot H \cdot 10^{16} \cdot 14)$$

$$= (4 + 20 \cdot 10^{16}) + (-20 \cdot 10^{16} + 68 \cdot 10^{32})$$

1. Use high-order lifting to compute only E.
2. Use E to compute modulo 10^{16} adjustment.

$$6 \cdot E \cdot 14 = 6 \cdot 2380 \cdot 14 = -80 + 20 \cdot 10^4$$

3. Use E to compute $B' = -70$ such that

$$6 \cdot \mathrm{rem}(21^{-1}, 10^{32}) \cdot 14 \equiv 4 \bmod 10^{32}$$

$$\Longleftrightarrow$$

$$6 \cdot \mathrm{rem}(21^{-1}, 10^{16}) \cdot \left[\, 14 \,\middle|\, -70 \,\right] \equiv \left[\, 4 \,\middle|\, 20 \,\right] \bmod 10^{16}$$

Repeated Reduction of Problem Order

$$C \cdot A^{-1} \cdot B \equiv D \bmod 10^k$$

$$\Longleftrightarrow$$

$$C \cdot A^{-1} \left[B_1 \middle| B_2 \right] \equiv \left[D_1 \middle| D_2 \right] \bmod 10^{k/2}$$

$$\Longleftrightarrow$$

$$C \cdot A^{-1} \left[B_1 \middle| B_2 \middle| B_3 \middle| B_4 \right] \equiv \left[D_1 \middle| D_2 \middle| D_3 \middle| D_4 \right] \bmod 10^{k/4}$$

$$\vdots \qquad\qquad\qquad\qquad \vdots$$

$$\Longleftrightarrow$$

$$C \cdot A^{-1} \left[B_1 \middle| B_2 \middle| B_3 \middle| B_4 \middle| B_5 \middle| \cdots \middle| B_n \right] \equiv \left[D_1 \middle| D_2 \middle| D_3 \middle| D_4 \middle| D_5 \middle| \cdots \middle| D_n \right] \bmod 10^{k/n}$$

Cost analysis

$T_n(k) = 2T_n(k/2) + \tilde{O}(n^3 d)$ with $k = n$ gives $\tilde{O}(n^4 d)$

Using Compression to Reduce the Column Dimension

Input: A long skinny matrix $A = \begin{bmatrix} * & * & * & * & * & * & * & * \end{bmatrix} \in \mathbb{Z}^{n \times *}$.

For example $A = \begin{bmatrix} -15 & 99 & -44 & -62 & 88 & 10 & -20 & 5 & -38 & -1 & -63 & 10 & 45 & -35 & 80 \\ 2 & -59 & 26 & -83 & 95 & -61 & -78 & -91 & -38 & 63 & -26 & 22 & -14 & 21 & 19 \\ -88 & 10 & -3 & 9 & 63 & -26 & -4 & -44 & 91 & -23 & 30 & 12 & 60 & 90 & 88 \end{bmatrix}$

Output: The rank of A.

Approach using compression

1. Let $B := AA^T = \begin{bmatrix} 39239 & 10380 & 8413 \\ 10380 & 45732 & 7595 \\ 8413 & 7595 & 43829 \end{bmatrix}$
2. Return $\text{rank}(B)$.

Using Compression to Reduce the Column Dimension

Input: A long skinny matrix $A = \begin{bmatrix} * & * & * & * & * & * & * & * \end{bmatrix} \in \mathbb{Z}^{n \times *}$.

For example $A = \begin{bmatrix} -15 & 99 & -44 & -62 & 88 & 10 & -20 & 5 & -38 & -1 & -63 & 10 & 45 & -35 & 80 \\ 2 & -59 & 26 & -83 & 95 & -61 & -78 & -91 & -38 & 63 & -26 & 22 & -14 & 21 & 19 \\ -88 & 10 & -3 & 9 & 63 & -26 & -4 & -44 & 91 & -23 & 30 & 12 & 60 & 90 & 88 \end{bmatrix}$

Output: The rank of A.

Approach using compression

1. Let $B := AA^T = \begin{bmatrix} 39239 & 10380 & 8413 \\ 10380 & 45732 & 7595 \\ 8413 & 7595 & 43829 \end{bmatrix}$
2. Return $\text{rank}(B)$.

Note: Not valid over a finite field! Consider $A = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$ over $\text{GF}(2)$.

Using Compression to Reduce the Column Dimension

$$\mathrm{rem}(C \cdot A^{-1} \cdot \overset{B}{\left[B_1\ B_2\ B_3\ B_4\ B_5\ B_6\ B_7\ B_8 \right]} - \overset{D}{\left[D_1\ D_2\ D_3\ D_4\ D_5\ D_6\ D_7\ D_8 \right]}, 10^k) = 0$$

$$\Longleftrightarrow$$

$$\mathrm{rem}\left(C \cdot A^{-1} \cdot \overset{B}{\left[* * * * * * * * \right]} - \overset{D}{\left[* * * * * * * * \right]}, 10^k \right) \times \mathrm{rem}\left(\begin{bmatrix} * \\ * \\ * \\ * \\ * \\ * \\ * \\ * \end{bmatrix}^{B^T} \cdot (A^{-1})^T \cdot C^T - \begin{bmatrix} * \\ * \\ * \\ * \\ * \\ * \\ * \\ * \end{bmatrix}^{D^T}, 10^k \right) = 0$$

$$\Longleftrightarrow$$

$$\mathrm{rem}(C \cdot A^{-1} \left[B'_1\ B'_2\ B'_3 \right] - \left[D'_1\ D'_2\ D'_3 \right], 10^k) = 0$$

Cost Analysis

Order reduction without compression

$$T_n(k) = 2T_n(k/2) + \tilde{O}(n^3 d) \text{ with } k = n \text{ gives } \tilde{O}(n^4 d)$$

Order reduction with compression

$$T_n(k) = T_n(k/2) + \tilde{O}(n^3 d) \text{ with } k = n \text{ gives } \tilde{O}(n^3 d)$$

Certifying the Rank in the General Case

Example Input: $M := \left[\begin{array}{c|c|c|c|c} A & B_1 & B_2 & B_3 & B_4 \\ \hline C_1 & D_{11} & D_{12} & D_{13} & D_{14} \\ C_2 & D_{21} & D_{22} & D_{23} & D_{24} \\ C_3 & D_{31} & D_{32} & D_{33} & D_{34} \end{array}\right] \in \mathbb{Z}^{n \times m} = \mathbb{Z}^{4r \times 5r}$.

Certify that $C_i \cdot A^{-1} \cdot B_j - D_{ij} = 0$ for $1 \leq i \leq 3$ and $1 \leq j \leq 4$.

Cost: $O\tilde{}(nmrd)$ bit operations.

Current and Future Work

- Obtain $O\tilde{}(n^3 d)$ Las Vegas algorithms for various canonical forms

- Compute inverse of a nonsingular $A \in \mathbb{Z}^{n \times n}$ in $(n^3 d)$ bit operations.

$$\begin{bmatrix} 25 & -16 & -38 & 57 & -32 & 99 \\ 94 & -9 & -18 & 27 & -74 & 29 \\ 12 & -50 & 87 & -93 & -4 & 44 \\ -2 & -22 & 33 & -76 & 27 & 92 \\ 50 & 45 & -98 & -72 & 8 & -31 \\ 10 & -81 & -77 & -2 & 69 & 67 \end{bmatrix}^{-1} = \begin{bmatrix} -\frac{2043699293}{72674318372} & \frac{1921892393}{72674318372} & -\frac{5197032317}{218022955116} & \frac{11614232501}{436045910232} & -\frac{4273458011}{436045910232} & \frac{2028363569}{436045910232} \\ -\frac{838573559}{72674318372} & \frac{620810971}{72674318372} & -\frac{1522814569}{72674318372} & \frac{3362614441}{145348636744} & -\frac{453009351}{145348636744} & -\frac{886053851}{145348636744} \\ -\frac{300458509}{18168579593} & \frac{218826900}{18168579593} & -\frac{674660030}{54505738779} & \frac{1856662385}{109011477558} & -\frac{1148992613}{109011477558} & -\frac{99479911}{109011477558} \\ -\frac{347815739}{36337159186} & \frac{340592137}{36337159186} & -\frac{1594931579}{109011477558} & \frac{2114306231}{218022955116} & -\frac{2037856205}{218022955116} & \frac{447817619}{218022955116} \\ -\frac{584700471}{18168579593} & \frac{356811254}{18168579593} & -\frac{1721772194}{54505738779} & \frac{3697142975}{109011477558} & -\frac{1450539425}{109011477558} & \frac{770731325}{109011477558} \\ \frac{297871357}{72674318372} & \frac{20118095}{72674318372} & -\frac{851335927}{218022955116} & \frac{3893593471}{436045910232} & -\frac{433417321}{436045910232} & -\frac{613719389}{436045910232} \end{bmatrix}$$

- Compute a nullspace basis of $A \in \mathbb{Z}^{n \times 2n}$ in $O\tilde{}(n^3 d)$ bit operations.

$$\begin{bmatrix} 25 & -16 & -38 & 57 & -32 & 99 \\ 94 & -9 & -18 & 27 & -74 & 29 \\ 12 & -50 & 87 & -93 & -4 & 44 \end{bmatrix} \begin{bmatrix} \frac{11614232501}{436045910232} & -\frac{4273458011}{436045910232} & \frac{2028363569}{436045910232} \\ \frac{3362614441}{145348636744} & -\frac{453009351}{145348636744} & -\frac{886053851}{145348636744} \\ \frac{1856662385}{109011477558} & -\frac{1148992613}{109011477558} & -\frac{99479911}{109011477558} \\ \frac{2114306231}{218022955116} & -\frac{2037856205}{218022955116} & \frac{447817619}{218022955116} \\ \frac{3697142975}{109011477558} & -\frac{1450539425}{109011477558} & \frac{770731325}{109011477558} \\ \frac{3893593471}{436045910232} & -\frac{433417321}{436045910232} & -\frac{613719389}{436045910232} \end{bmatrix} = 0$$