Fast linear solving over $\mathbb{Z} \subset \mathbb{Q}$

George Labahn and Arne Storjohann

Cheriton School of Computer Science
University of Waterloo

Recent Trends in Computer Algebra, Institut Henri Poincaré,

September 2023

Nonsingular linear system solving

Nonsingular linear system solving

Problem:

- Given:
  - $A \in \mathbb{Z}^{n \times n}$
  - $b \in \mathbb{Z}^{n \times 1}$

Nonsingular linear system solving

Problem:

- Given:
  - $A \in \mathbb{Z}^{n \times n}$
  - $b \in \mathbb{Z}^{n \times 1}$

    Note: we assume $\log b \in O(n(\log n + \log ||A||))$

Nonsingular linear system solving

Problem:

- Given:
  - $A \in \mathbb{Z}^{n \times n}$
  - $b \in \mathbb{Z}^{n \times 1}$

    Note: we assume $\log b \in O(n(\log n + \log ||A||))$
- Compute:
  - $A^{-1}b \in \mathbb{Q}^{n \times 1}$

Nonsingular linear system solving

Problem:

- Given:
  - $A \in \mathbb{Z}^{n \times n}$
  - $b \in \mathbb{Z}^{n \times 1}$

  Note: we assume $\log b \in O(n(\log n + \log ||A||))$
- Compute:
  - $A^{-1}b \in \mathbb{Q}^{n \times 1}$

Example:

- $$A = \begin{bmatrix} 594 & 24 & 601 & 604 & 827 \\ 476 & 397 & 49 & 378 & 174 \\ 7 & 361 & 173 & 939 & 392 \\ 844 & 186 & 655 & 896 & 453 \\ 76 & 621 & 38 & 603 & 582 \end{bmatrix} \quad b = \begin{bmatrix} 450 \\ 717 \\ 508 \\ 238 \\ 366 \end{bmatrix}$$
- $$A^{-1}b = \begin{bmatrix} -58686180258858 \\ 70644871354626 \\ 143314986631278 \\ -49969380574326 \\ -42023211987798 \end{bmatrix} \frac{1}{-26592243059232}$$

Dixon's linear lifting: X-adic lifting

Dixon's linear lifting: X-adic lifting

- Choose a lifting modulos $X \in \mathbb{Z}_{>0}$ with

Dixon's linear lifting: X-adic lifting

- Choose a lifting modulos $X \in \mathbb{Z}_{>0}$ with
  - $X \perp \det A$
  - $\log X \in \Theta(\log n + \log ||A||)$

Dixon's linear lifting: X-adic lifting

- Choose a lifting modulos $X \in \mathbb{Z}_{>0}$ with
  - $X \perp \det A$
  - $\log X \in \Theta(\log n + \log ||A||)$
- Compute the (unique) X-adic expansion

$$A^{-1}b \equiv c_0 + c_1 X + c_2 X^2 + \cdots + c_{d-1} X^{d-1} \bmod X^d$$

up to precision $d \in O(n)$

$\rightarrow$ Each $c_* \in \mathbb{Z}^{n \times 1}$ has entries reduced modulo X

$\rightarrow$ Example: $(\frac{1}{7})3 \equiv 9 + 2(10) + 4(10)^2 + 1(10)^3 + 7(10)^4 + 5(10)^5 \bmod 10^6$

Dixon's linear lifting: X-adic lifting

- Choose a lifting modulos $X \in \mathbb{Z}_{>0}$ with
  - $X \perp \det A$
  - $\log X \in \Theta(\log n + \log ||A||)$
- Compute the (unique) X-adic expansion

$$A^{-1}b \equiv c_0 + c_1 X + c_2 X^2 + \cdots + c_{d-1} X^{d-1} \bmod X^d$$

  up to precision $d \in O(n)$

  $\rightarrow$ Each $c_* \in \mathbb{Z}^{n \times 1}$ has entries reduced modulo X

  $\rightarrow$ Example: $(\frac{1}{7})3 \equiv 9 + 2(10) + 4(10)^2 + 1(10)^3 + 7(10)^4 + 5(10)^5 \bmod 10^6$
- Reconstruct $A^{-1}b$ from the expansion using radix conversion and rational number reconstruction

Dixon's linear lifting: X-adic lifting

- Choose a lifting modulos $X \in \mathbb{Z}_{>0}$ with
  - $X \perp \det A$
  - $\log X \in \Theta(\log n + \log ||A||)$
- Compute the (unique) X-adic expansion

$$A^{-1}b \equiv c_0 + c_1 X + c_2 X^2 + \cdots + c_{d-1} X^{d-1} \bmod X^d$$

  up to precision $d \in O(n)$

  $\rightarrow$ Each $c_* \in \mathbb{Z}^{n \times 1}$ has entries reduced modulo X

  $\rightarrow$ Example: $(\frac{1}{7})3 \equiv 9 + 2(10) + 4(10)^2 + 1(10)^3 + 7(10)^4 + 5(10)^5 \bmod 10^6$
- Reconstruct $A^{-1}b$ from the expansion using radix conversion and rational number reconstruction

Cost:

Dixon's linear lifting: X-adic lifting

- Choose a lifting modulos $X \in \mathbb{Z}_{>0}$ with
  - $X \perp \det A$
  - $\log X \in \Theta(\log n + \log ||A||)$
- Compute the (unique) X-adic expansion

$$A^{-1}b \equiv c_0 + c_1 X + c_2 X^2 + \cdots + c_{d-1} X^{d-1} \bmod X^d$$

  up to precision $d \in O(n)$

  $\rightarrow$ Each $c_* \in \mathbb{Z}^{n \times 1}$ has entries reduced modulo X

  $\rightarrow$ Example: $(\frac{1}{7})3 \equiv 9 + 2(10) + 4(10)^2 + 1(10)^3 + 7(10)^4 + 5(10)^5 \bmod 10^6$
- Reconstruct $A^{-1}b$ from the expansion using radix conversion and rational number reconstruction

Cost:

- $O(n^3(\log n + \log ||A||)^2)$ in naive model

Dixon's linear lifting: X-adic lifting

- Choose a lifting modulos $X \in \mathbb{Z}_{>0}$ with
  - $X \perp \det A$
  - $\log X \in \Theta(\log n + \log ||A||)$
- Compute the (unique) X-adic expansion

$$A^{-1}b \equiv c_0 + c_1 X + c_2 X^2 + \cdots + c_{d-1} X^{d-1} \bmod X^d$$

  up to precision $d \in O(n)$

  $\rightarrow$ Each $c_* \in \mathbb{Z}^{n \times 1}$ has entries reduced modulo X

  $\rightarrow$ Example: $(\frac{1}{7})3 \equiv 9 + 2(10) + 4(10)^2 + 1(10)^3 + 7(10)^4 + 5(10)^5 \bmod 10^6$
- Reconstruct $A^{-1}b$ from the expansion using radix conversion and rational number reconstruction

Cost:

- $O(n^3(\log n + \log ||A||)^2)$ in naive model
- $(n^3 \log ||A||)^{1+o(1)}$ using fast arithmetic

Linear and quadratic lifting: the classic algorithms

Linear and quadratic lifting: the classic algorithms

Key identity in lifting to compute the inverse, that is, solve $AC = I$

$$A^{-1} = \overbrace{C_0 + C_1 X + C_2 X^2 + \cdots + C_{i-1} X^{i-1}}^{\mathrm{Rem}(A^{-1}, X^i)} + A^{-1} R X^i$$

Linear and quadratic lifting: the classic algorithms

Key identity in lifting to compute the inverse, that is, solve $AC = I$

$$A^{-1} = \overbrace{C_0 + C_1 X + C_2 X^2 + \cdots + C_{i-1} X^{i-1}}^{\mathrm{Rem}(A^{-1}, X^i)} + A^{-1} R X^i$$

- One step of linear lifting (iterative refinement)

Linear and quadratic lifting: the classic algorithms

Key identity in lifting to compute the inverse, that is, solve $AC = I$

$$A^{-1} = \overbrace{C_0 + C_1 X + C_2 X^2 + \cdots + C_{i-1} X^{i-1}}^{\mathrm{Rem}(A^{-1}, X^i)} + A^{-1} R X^i$$

- One step of linear lifting (iterative refinement)
  - Use (precomputed) local inverse C_0 to get next coefficient C_i
  - Set $C_i := \mathrm{Rem}(C_0 R, X)$ and update $R := (1/X)(R - AC_i)$

Linear and quadratic lifting: the classic algorithms

Key identity in lifting to compute the inverse, that is, solve $AC = I$

$$A^{-1} = \overbrace{C_0 + C_1 X + C_2 X^2 + \cdots + C_{i-1} X^{i-1}}^{\mathrm{Rem}(A^{-1}, X^i)} + A^{-1} R X^i$$

- One step of linear lifting (iterative refinement)
  - Use (precomputed) local inverse C_0 to get next coefficient C_i
  - Set $C_i := \mathrm{Rem}(C_0 R, X)$ and update $R := (1/X)(R - AC_i)$

- One step of quadratic lifting (algebraic Newton iteration)

Linear and quadratic lifting: the classic algorithms

Key identity in lifting to compute the inverse, that is, solve $AC = I$

$$A^{-1} = \overbrace{C_0 + C_1 X + C_2 X^2 + \cdots + C_{i-1} X^{i-1}}^{\mathrm{Rem}(A^{-1}, X^i)} + A^{-1} R X^i$$

- One step of linear lifting (iterative refinement)
  - Use (precomputed) local inverse C_0 to get next coefficient C_i
  - Set $C_i := \mathrm{Rem}(C_0 R, X)$ and update $R := (1/X)(R - AC_i)$

- One step of quadratic lifting (algebraic Newton iteration)
  - Use all of $C_0 + C_1 X + \cdots + C_{i-1}$ to get next i coefficients
  - Identity: $\mathrm{Rem}(A^{-1}, X^{2i}) \equiv \mathrm{Rem}(A^{-1}, X^i)(I + RX^i) \bmod X^{2i}$
  - Upate of R is similar

Intuition: High level view of lifting

Intuition: High level view of lifting

- Let $C_0 := \mathrm{Rem}(A^{-1}, X)$

Intuition: High level view of lifting

- Let $C_0 := \mathrm{Rem}(A^{-1}, X)$
- Note that AC_0 can be written as $(I - \bar{A}X) \in \mathbb{Z}^{n \times n}$

Intuition: High level view of lifting

- Let $C_0 := \mathrm{Rem}(A^{-1}, X)$
- Note that AC_0 can be written as $(I - \bar{A}X) \in \mathbb{Z}^{n \times n}$
- Note that $A^{-1} = C_0(I - \bar{A}X)^{-1}$ since $(AC_0)^{-1} = C_0^{-1}A^{-1}$

Intuition: High level view of lifting

- Let $C_0 := \mathrm{Rem}(A^{-1}, X)$
- Note that AC_0 can be written as $(I - \bar{A}X) \in \mathbb{Z}^{n \times n}$
- Note that $A^{-1} = C_0(I - \bar{A}X)^{-1}$ since $(AC_0)^{-1} = C_0^{-1}A^{-1}$

$$(I-\bar{A}X)^{-1} \equiv I+\bar{A}X+\bar{A}^2X^2+\bar{A}^3X^3+\bar{A}^4X^4+\bar{A}^5X^5+\bar{A}^6X^6+\bar{A}^7X^7 \bmod X^8$$

Intuition: High level view of lifting

- Let $C_0 := \mathrm{Rem}(A^{-1}, X)$
- Note that AC_0 can be written as $(I - \bar{A}X) \in \mathbb{Z}^{n \times n}$
- Note that $A^{-1} = C_0(I - \bar{A}X)^{-1}$ since $(AC_0)^{-1} = C_0^{-1}A^{-1}$

$$(I-\bar{A}X)^{-1} \equiv I+\bar{A}X+\bar{A}^2X^2+\bar{A}^3X^3+\bar{A}^4X^4+\bar{A}^5X^5+\bar{A}^6X^6+\bar{A}^7X^7 \bmod X^8$$

- Linear lifting

- Quadratic lifting

Intuition: High level view of lifting

- Let $C_0 := \mathrm{Rem}(A^{-1}, X)$
- Note that AC_0 can be written as $(I - \bar{A}X) \in \mathbb{Z}^{n \times n}$
- Note that $A^{-1} = C_0(I - \bar{A}X)^{-1}$ since $(AC_0)^{-1} = C_0^{-1}A^{-1}$

$$(I-\bar{A}X)^{-1} \equiv I+\bar{A}X+\bar{A}^2X^2+\bar{A}^3X^3+\bar{A}^4X^4+\bar{A}^5X^5+\bar{A}^6X^6+\bar{A}^7X^7 \bmod X^8$$

- Linear lifting

$$((((((\bar{A}X + I)\bar{A}X + I)\bar{A}X + I)\bar{A}X + I)\bar{A}X + I)\bar{A}X + I)\bar{A}X + I$$

- Quadratic lifting

Intuition: High level view of lifting

- Let $C_0 := \mathrm{Rem}(A^{-1}, X)$
- Note that AC_0 can be written as $(I - \bar{A}X) \in \mathbb{Z}^{n \times n}$
- Note that $A^{-1} = C_0(I - \bar{A}X)^{-1}$ since $(AC_0)^{-1} = C_0^{-1}A^{-1}$

$$(I-\bar{A}X)^{-1} \equiv I+\bar{A}X+\bar{A}^2X^2+\bar{A}^3X^3+\bar{A}^4X^4+\bar{A}^5X^5+\bar{A}^6X^6+\bar{A}^7X^7 \bmod X^8$$

- Linear lifting

$$((((((\bar{A}X + I)\bar{A}X + I)\bar{A}X + I)\bar{A}X + I)\bar{A}X + I)\bar{A}X + I)\bar{A}X + I$$

- Quadratic lifting

$$(\bar{A}^4X^4 + 1)(\bar{A}^2X^2 + 1)(\bar{A}X + 1)$$

Double-plus-one lifting

- Interleave quadratic with linear lifting

- This gives D and R, where $A^{-1} = D + A^{-1}RX^k$ and

$$D = (\cdots((\qquad\qquad\qquad\qquad)(I + *X^3) + *X^6)(I + *X^7) + *X^{14})\cdots)$$

Double-plus-one lifting

- Interleave quadratic with linear lifting
  - Initialize $B = \mathrm{Rem}(A^{-1}, X)$

- This gives D and R, where $A^{-1} = D + A^{-1}RX^k$ and

$$D = (\cdots((B \qquad\qquad\qquad\qquad)(I + *X^3) + *X^6)(I + *X^7) + *X^{14})\cdots)$$

Double-plus-one lifting

- Interleave quadratic with linear lifting
  - Initialize $B = \mathrm{Rem}(A^{-1}, X)$
  - Do one step of quadratic lifting

- This gives D and R, where $A^{-1} = D + A^{-1}RX^k$ and

$$D = (\cdots((B(I + *X) \qquad)(I + *X^3) + *X^6)(I + *X^7) + *X^{14})\cdots)$$

Double-plus-one lifting

- Interleave quadratic with linear lifting
  - Initialize $B = \mathrm{Rem}(A^{-1}, X)$
  - Do one step of quadratic lifting
  - Do one step of linear lifting

- This gives D and R, where $A^{-1} = D + A^{-1}RX^k$ and

$$D = (\cdots((B(I + *X) + *X^2)(I + *X^3) + *X^6)(I + *X^7) + *X^{14})\cdots)$$

Double-plus-one lifting

- Interleave quadratic with linear lifting
  - Initialize $B = \mathrm{Rem}(A^{-1}, X)$
  - Do one step of quadratic lifting
  - Do one step of linear lifting
  - Repeat up to precision $X^{\Theta(n)}$
- This gives D and R, where $A^{-1} = D + A^{-1}RX^k$ and

$$D = (\cdots((B(I + *X) + *X^2)(I + *X^3) + *X^6)(I + *X^7) + *X^{14})\cdots)$$

Double-plus-one lifting

- Interleave quadratic with linear lifting
  - Initialize $B = \mathrm{Rem}(A^{-1}, X)$
  - Do one step of quadratic lifting
  - Do one step of linear lifting
  - Repeat up to precision $X^{\Theta(n)}$
- This gives D and R, where $A^{-1} = D + A^{-1}RX^k$ and

$$D = (\cdots((B(I + *X) + *X^2)(I + *X^3) + *X^6)(I + *X^7) + *X^{14})\cdots)$$

  - Each $* \in \mathbb{Z}^{n \times n}$ has $|| * || < X$
  - Straight line formula for $A^{-1} \bmod X^k$ with only $O(\log n)$ terms

Double-plus-one lifting

- Interleave quadratic with linear lifting
  - Initialize $B = \mathrm{Rem}(A^{-1}, X)$
  - Do one step of quadratic lifting
  - Do one step of linear lifting
  - Repeat up to precision $X^{\Theta(n)}$
- This gives D and R, where $A^{-1} = D + A^{-1}RX^k$ and

$$D = (\cdots((B(I + *X) + *X^2)(I + *X^3) + *X^6)(I + *X^7) + *X^{14})\cdots)$$

  - Each $* \in \mathbb{Z}^{n \times n}$ has $|| * || < X$
  - Straight line formula for $A^{-1} \bmod X^k$ with only $O(\log n)$ terms
- D is called a sparse inverse expansion

Double-plus-one lifting

- Interleave quadratic with linear lifting
  - Initialize $B = \mathrm{Rem}(A^{-1}, X)$
  - Do one step of quadratic lifting
  - Do one step of linear lifting
  - Repeat up to precision $X^{\Theta(n)}$
- This gives D and R, where $A^{-1} = D + A^{-1}RX^k$ and

$$D = (\cdots((B(I + *X) + *X^2)(I + *X^3) + *X^6)(I + *X^7) + *X^{14})\cdots)$$

  - Each $* \in \mathbb{Z}^{n \times n}$ has $|| * || < X$
  - Straight line formula for $A^{-1} \bmod X^k$ with only $O(\log n)$ terms

- D is called a sparse inverse expansion
- D and R computed in time $O(n^\omega \, \mathrm{M}(\log n + \log ||A||) \log n)$

Double-plus-one lifting: Example

Double-plus-one lifting: Example

Consider $A = 413$ and $X = 1000$

Local inverse is $\mathrm{Rem}(A^{-1}, X) = 477$

Double-plus-one lifting: Example

Consider $A = 413$ and $X = 1000$

Local inverse is $\mathrm{Rem}(A^{-1}, X) = 477$

$$A^{-1} \quad = \quad 477 + A^{-1}(-197)X$$

Double-plus-one lifting: Example

Consider $A = 413$ and $X = 1000$

Local inverse is $\mathrm{Rem}(A^{-1}, X) = 477$

$$\begin{aligned} A^{-1} &= 477 + A^{-1}(-197)X \\ &= 477(1 + (-197)X) + A^{-1}(\underline{38809})X^2 \end{aligned}$$

Double-plus-one lifting: Example

Consider $A = 413$ and $X = 1000$

Local inverse is $\mathrm{Rem}(A^{-1}, X) = 477$

$$\begin{aligned} A^{-1} &= 477 + A^{-1}(-197)X \\ &= 477(1 + (-197)X) + A^{-1}(\underline{38809})X^2 \\ &= 477(1 + (-197)X) + (892)X^2 + A^{-1}(330)X^3 \end{aligned}$$

Double-plus-one lifting: Example

Consider $A = 413$ and $X = 1000$

Local inverse is $\mathrm{Rem}(A^{-1}, X) = 477$

$$
\begin{aligned}
A^{-1} &= 477 + A^{-1}(-197)X \\
&= 477(1 + (-197)X) + A^{-1}(\underline{38809})X^2 \\
&= 477(1 + (-197)X) + (892)X^2 + A^{-1}(330)X^3 \\
&= (477(1 + (-197)X) + (892)X^2)(1 + (330)X^3) + A^{-1}(\underline{10890})X^7
\end{aligned}
$$

Matrix times a fat vector

- Applying a sparse inverse expansion requires multiplications like

$$\underset{A}{\begin{bmatrix} 6 & 9 & 5 & 1 & 3 \\ 5 & 4 & 0 & 7 & 4 \\ 9 & 1 & 1 & 3 & 7 \\ 2 & 8 & 9 & 1 & 7 \\ 9 & 8 & 0 & 5 & 6 \end{bmatrix}} \underset{B}{\begin{bmatrix} 82370 \\ 69325 \\ 64878 \\ 91700 \\ 28043 \end{bmatrix}}$$

Matrix times a fat vector

- Applying a sparse inverse expansion requires multiplications like

$$\underset{A}{\begin{bmatrix} 6 & 9 & 5 & 1 & 3 \\ 5 & 4 & 0 & 7 & 4 \\ 9 & 1 & 1 & 3 & 7 \\ 2 & 8 & 9 & 1 & 7 \\ 9 & 8 & 0 & 5 & 6 \end{bmatrix}} \underset{B}{\begin{bmatrix} 82370 \\ 69325 \\ 64878 \\ 91700 \\ 28043 \end{bmatrix}}$$

- Reduce to matrix multiplication: expand, multiply

$$AB = \underset{A}{\begin{bmatrix} 6 & 9 & 5 & 1 & 3 \\ 5 & 4 & 0 & 7 & 4 \\ 9 & 1 & 1 & 3 & 7 \\ 2 & 8 & 9 & 1 & 7 \\ 9 & 8 & 0 & 5 & 6 \end{bmatrix}} \underset{\bar{B}}{\begin{bmatrix} 8 & 2 & 3 & 7 & 0 \\ 6 & 9 & 3 & 2 & 5 \\ 6 & 4 & 8 & 7 & 8 \\ 9 & 1 & 7 & 0 & 0 \\ 2 & 8 & 0 & 4 & 3 \end{bmatrix}}$$

Matrix times a fat vector

- Applying a sparse inverse expansion requires multiplications like

$$\underset{A}{\begin{bmatrix} 6 & 9 & 5 & 1 & 3 \\ 5 & 4 & 0 & 7 & 4 \\ 9 & 1 & 1 & 3 & 7 \\ 2 & 8 & 9 & 1 & 7 \\ 9 & 8 & 0 & 5 & 6 \end{bmatrix}} \underset{B}{\begin{bmatrix} 82370 \\ 69325 \\ 64878 \\ 91700 \\ 28043 \end{bmatrix}}$$

- Reduce to matrix multiplication: expand, multiply, compress

$$AB = \underset{A}{\begin{bmatrix} 6 & 9 & 5 & 1 & 3 \\ 5 & 4 & 0 & 7 & 4 \\ 9 & 1 & 1 & 3 & 7 \\ 2 & 8 & 9 & 1 & 7 \\ 9 & 8 & 0 & 5 & 6 \end{bmatrix}} \underset{\bar{B}}{\begin{bmatrix} 8 & 2 & 3 & 7 & 0 \\ 6 & 9 & 3 & 2 & 5 \\ 6 & 4 & 8 & 7 & 8 \\ 9 & 1 & 7 & 0 & 0 \\ 2 & 8 & 0 & 4 & 3 \end{bmatrix}} \begin{bmatrix} 10^4 \\ 10^3 \\ 10^2 \\ 10^1 \\ 1 \end{bmatrix}$$

Matrix times a fat vector

- Applying a sparse inverse expansion requires multiplications like

$$\underset{A}{\begin{bmatrix} 6 & 9 & 5 & 1 & 3 \\ 5 & 4 & 0 & 7 & 4 \\ 9 & 1 & 1 & 3 & 7 \\ 2 & 8 & 9 & 1 & 7 \\ 9 & 8 & 0 & 5 & 6 \end{bmatrix}} \underset{B}{\begin{bmatrix} 82370 \\ 69325 \\ 64878 \\ 91700 \\ 28043 \end{bmatrix}}$$

- Reduce to matrix multiplication: expand, multiply, compress

$$AB = \underset{A}{\begin{bmatrix} 6 & 9 & 5 & 1 & 3 \\ 5 & 4 & 0 & 7 & 4 \\ 9 & 1 & 1 & 3 & 7 \\ 2 & 8 & 9 & 1 & 7 \\ 9 & 8 & 0 & 5 & 6 \end{bmatrix}} \underset{\bar{B}}{\begin{bmatrix} 8 & 2 & 3 & 7 & 0 \\ 6 & 9 & 3 & 2 & 5 \\ 6 & 4 & 8 & 7 & 8 \\ 9 & 1 & 7 & 0 & 0 \\ 2 & 8 & 0 & 4 & 3 \end{bmatrix}} \begin{bmatrix} 10^4 \\ 10^3 \\ 10^2 \\ 10^1 \\ 1 \end{bmatrix}$$

- In this example B has one column and full precision $d \in O(n)$
  If B had m column the precision should be $d \in O(n/m)$.

System solving via the sparse inverse expansion

System solving via the sparse inverse expansion

Recall our goal: For precison $k \in \Theta(n)$ compute $A^{-1}b \bmod X^k$

System solving via the sparse inverse expansion

Recall our goal: For precison $k \in \Theta(n)$ compute $A^{-1}b \bmod X^k$

- Sparse inverse expansion satisfies $A^{-1} = D + A^{-1}RX^k$

System solving via the sparse inverse expansion

Recall our goal: For precison $k \in \Theta(n)$ compute $A^{-1}b \bmod X^k$

- Sparse inverse expansion satisfies $A^{-1} = D + A^{-1}RX^k$
- Thus $A^{-1}b \equiv Db \bmod X^k$ where

$$D = (\cdots((B(I + *X) + *X^2)(I + *X^3) + *X^6)(I + *X^7) + *X^{14})\cdots)$$

System solving via the sparse inverse expansion

Recall our goal: For precison $k \in \Theta(n)$ compute $A^{-1}b \bmod X^k$

- Sparse inverse expansion satisfies $A^{-1} = D + A^{-1}RX^k$
- Thus $A^{-1}b \equiv Db \bmod X^k$ where

$$D = (\cdots((B(I + *X) + *X^2)(I + *X^3) + *X^6)(I + *X^7) + *X^{14})\cdots)$$

- Premultiply b by D, taking advantage of structure

System solving via the sparse inverse expansion

Recall our goal: For precison $k \in \Theta(n)$ compute $A^{-1}b \bmod X^k$

- Sparse inverse expansion satisfies $A^{-1} = D + A^{-1}RX^k$
- Thus $A^{-1}b \equiv Db \bmod X^k$ where

$$D = (\cdots((B(I + *X) + *X^2)(I + *X^3) + *X^6)(I + *X^7) + *X^{14})\cdots)$$

- Premultiply b by D, taking advantage of structure
- Requires $O(\log n)$ multiplications by powers of X (cheap)

System solving via the sparse inverse expansion

Recall our goal: For precison $k \in \Theta(n)$ compute $A^{-1}b \bmod X^k$

- Sparse inverse expansion satisfies $A^{-1} = D + A^{-1}RX^k$
- Thus $A^{-1}b \equiv Db \bmod X^k$ where

$$D = (\cdots((B(I + *X) + *X^2)(I + *X^3) + *X^6)(I + *X^7) + *X^{14})\cdots)$$

- Premultiply b by D, taking advantage of structure
- Requires $O(\log n)$ multiplications by powers of X (cheap)
- Requires $O(\log n)$ multiplications by matrices $*$
  $\rightarrow$ use partial-linearization/matrix-multiply/compression idea on previous slide

System solving via the sparse inverse expansion

Recall our goal: For precison $k \in \Theta(n)$ compute $A^{-1}b \bmod X^k$

- Sparse inverse expansion satisfies $A^{-1} = D + A^{-1}RX^k$
- Thus $A^{-1}b \equiv Db \bmod X^k$ where

$$D = (\cdots((B(I + *X) + *X^2)(I + *X^3) + *X^6)(I + *X^7) + *X^{14})\cdots)$$

- Premultiply b by D, taking advantage of structure
- Requires $O(\log n)$ multiplications by powers of X (cheap)
- Requires $O(\log n)$ multiplications by matrices $*$
  $\rightarrow$ use partial-linearization/matrix-multiply/compression idea on previous slide
- Reduce module X^k after every multiplication

System solving via the sparse inverse expansion

Recall our goal: For precison $k \in \Theta(n)$ compute $A^{-1}b \bmod X^k$

- Sparse inverse expansion satisfies $A^{-1} = D + A^{-1}RX^k$
- Thus $A^{-1}b \equiv Db \bmod X^k$ where

$$D = (\cdots((B(I + *X) + *X^2)(I + *X^3) + *X^6)(I + *X^7) + *X^{14})\cdots)$$

- Premultiply b by D, taking advantage of structure
- Requires $O(\log n)$ multiplications by powers of X (cheap)
- Requires $O(\log n)$ multiplications by matrices $*$
  $\rightarrow$ use partial-linearization/matrix-multiply/compression idea on previous slide
- Reduce module X^k after every multiplication

Total cost: $O(n^\omega \, \mathrm{M}(\log n + \log ||A||) \log n)$

Tool: **Fast-Linear-Solving**

- Given:
  - $A \in \mathbb{Z}^{n \times n}$ and $B \in \mathbb{Z}^{n \times m}$
  - $X \in \mathbb{Z}_{>0}$

    Note: require $X \perp \det A$ and $\log X \in O(\log n + \log ||A||)$
- Compute:
  - $\mathrm{Rem}(A^{-1}B, X^d)$
- Comprimise:
  - $m \times d \in O(n)$

Fast-Linear-Solving costs $O(n^\omega \, \mathrm{M}(\log n + \log ||A||) \log n)$

Integrality certification: Introduction

Integrality certification: Introduction

- Consider A^{-1} with long numerators but short common denominator:

$$A^{-1} = \begin{bmatrix} \frac{5704601}{5} & \frac{4161255391}{510} & \frac{1748100427}{170} \\ \frac{660900133}{34} & \frac{134849071}{85} & \frac{4225592701}{255} \\ \frac{1482484381}{102} & \frac{4530893609}{255} & \frac{1142612851}{170} \end{bmatrix}$$

Integrality certification: Introduction

- Consider A^{-1} with long numerators but short common denominator:

$$A^{-1} = \begin{bmatrix} \frac{5704601}{5} & \frac{4161255391}{510} & \frac{1748100427}{170} \\ \frac{660900133}{34} & \frac{134849071}{85} & \frac{4225592701}{255} \\ \frac{1482484381}{102} & \frac{4530893609}{255} & \frac{1142612851}{170} \end{bmatrix}$$

- A common denominator is $s = 510$.

Integrality certification: Introduction

- Consider A^{-1} with long numerators but short common denominator:

$$A^{-1} = \begin{bmatrix} \frac{5704601}{5} & \frac{4161255391}{510} & \frac{1748100427}{170} \\ \frac{660900133}{34} & \frac{134849071}{85} & \frac{4225592701}{255} \\ \frac{1482484381}{102} & \frac{4530893609}{255} & \frac{1142612851}{170} \end{bmatrix}$$

- A common denominator is $s = 510$. Can thus decompose as

$$A^{-1} = \overbrace{\begin{bmatrix} 1140920 & 8159324 & 10282943 \\ 19438239 & 1586459 & 16570951 \\ 14534160 & 17768210 & 6721252 \end{bmatrix}}^{Q} + \overbrace{\begin{bmatrix} 102 & 151 & 351 \\ 105 & 336 & 392 \\ 305 & 118 & 33 \end{bmatrix}}^{C} \frac{1}{510}$$

Integrality certification: Introduction

- Consider A^{-1} with long numerators but short common denominator:

$$A^{-1} = \begin{bmatrix} \frac{5704601}{5} & \frac{4161255391}{510} & \frac{1748100427}{170} \\ \frac{660900133}{34} & \frac{134849071}{85} & \frac{4225592701}{255} \\ \frac{1482484381}{102} & \frac{4530893609}{255} & \frac{1142612851}{170} \end{bmatrix}$$

- A common denominator is $s = 510$. Can thus decompose as

$$A^{-1} = \overbrace{\begin{bmatrix} 1140920 & 8159324 & 10282943 \\ 19438239 & 1586459 & 16570951 \\ 14534160 & 17768210 & 6721252 \end{bmatrix}}^{Q} + \overbrace{\begin{bmatrix} 102 & 151 & 351 \\ 105 & 336 & 392 \\ 305 & 118 & 33 \end{bmatrix}}^{C} \frac{1}{510}$$

- We don't care about Q, only the remainder C

Integrality certification: Introduction

- Consider A^{-1} with long numerators but short common denominator:

$$A^{-1} = \begin{bmatrix} \frac{5704601}{5} & \frac{4161255391}{510} & \frac{1748100427}{170} \\ \frac{660900133}{34} & \frac{134849071}{85} & \frac{4225592701}{255} \\ \frac{1482484381}{102} & \frac{4530893609}{255} & \frac{1142612851}{170} \end{bmatrix}$$

- A common denominator is $s = 510$. Can thus decompose as

$$A^{-1} = \overbrace{\begin{bmatrix} 1140920 & 8159324 & 10282943 \\ 19438239 & 1586459 & 16570951 \\ 14534160 & 17768210 & 6721252 \end{bmatrix}}^{Q} + \overbrace{\begin{bmatrix} 102 & 151 & 351 \\ 105 & 336 & 392 \\ 305 & 118 & 33 \end{bmatrix}}^{C} \frac{1}{510}$$

- We don't care about Q, only the remainder C
- How to determine if sA^{-1} is integral?

Integrality certification: Introduction

- Consider A^{-1} with long numerators but short common denominator:

$$A^{-1} = \begin{bmatrix} \frac{5704601}{5} & \frac{4161255391}{510} & \frac{1748100427}{170} \\ \frac{660900133}{34} & \frac{134849071}{85} & \frac{4225592701}{255} \\ \frac{1482484381}{102} & \frac{4530893609}{255} & \frac{1142612851}{170} \end{bmatrix}$$

- A common denominator is $s = 510$. Can thus decompose as

$$A^{-1} = \overbrace{\begin{bmatrix} 1140920 & 8159324 & 10282943 \\ 19438239 & 1586459 & 16570951 \\ 14534160 & 17768210 & 6721252 \end{bmatrix}}^{Q} + \overbrace{\begin{bmatrix} 102 & 151 & 351 \\ 105 & 336 & 392 \\ 305 & 118 & 33 \end{bmatrix}}^{C} \frac{1}{510}$$

- We don't care about Q, only the remainder C
- How to determine if sA^{-1} is integral?
- If it is, how can we compute C quickly?

  $\rightarrow$ Using all of A^{-1} and C for clarity. Usually, we want just a projection Cb

Integrality certification: Main ideas

Integrality certification: Main ideas

- Every fraction can be written as an integer and proper fraction

$$\frac{4161244391}{511} = 8143335 + \frac{206}{511}$$

Integrality certification: Main ideas

- Every fraction can be written as an integer and proper fraction

$$\frac{4161244391}{511} = 8143335 + \frac{206}{511}$$

- We can compute 206 by multiplying the left hand size by 511 and then taking the result modulo 511

Integrality certification: Main ideas

- Every fraction can be written as an integer and proper fraction

$$\frac{4161244391}{511} = 8143335 + \frac{206}{511}$$

- We can compute 206 by multiplying the left hand size by 511 and then taking the result modulo 511
- A similar identity holds with X-adic expansions, eg, $X = 10$

$$\frac{4161244391}{511} = 829745596868884540117424973081 - \frac{424}{511}(10)^{30}$$

Integrality certification: Main ideas

- Every fraction can be written as an integer and proper fraction

$$\frac{4161244391}{511} = 8143335 + \frac{206}{511}$$

- We can compute 206 by multiplying the left hand size by 511 and then taking the result modulo 511
- A similar identity holds with X-adic expansions, eg, $X = 10$

$$\frac{4161244391}{511} = 829745596868884540117424973081 - \frac{424}{511}(10)^{30}$$

- Multiply last equation by 511

$$4161244391 = 424000000000000000000004161244391 - 424(10)^{30}$$

Integrality certification: Main ideas

- Every fraction can be written as an integer and proper fraction

$$\frac{4161244391}{511} = 8143335 + \frac{206}{511}$$

- We can compute 206 by multiplying the left hand size by 511 and then taking the result modulo 511
- A similar identity holds with X-adic expansions, eg, $X = 10$

$$\frac{4161244391}{511} = 829745596868884540117424973081 - \frac{424}{511}(10)^{30}$$

- Multiply last equation by 511

$$4161244391 = 424000000000000000000004161244391 - 424(10)^{30}$$

- Multiply last equation by 511

$$4161244391 = 829745596868884540117424973081(511) - 424(10)^{30}$$

Integrality certification: Connection with high-order residue

Any rational vector $v \in \mathbb{Q}^{n\times 1}$ with denominator $s \in \mathbb{Z}_{>0}$ has an integral $q \in \mathbb{Z}^{n\times 1}$ and a fractional part $c \in (\mathbb{Z}/s)^{n\times 1}$ such that

$$v = q + \frac{1}{s}c.$$

Integrality certification: Connection with high-order residue

Any rational vector $v \in \mathbb{Q}^{n\times 1}$ with denominator $s \in \mathbb{Z}_{>0}$ has an integral $q \in \mathbb{Z}^{n\times 1}$ and a fractional part $c \in (\mathbb{Z}/s)^{n\times 1}$ such that

$$v = q + \frac{1}{s}c.$$

Example

$$A^{-1}b = \begin{matrix} v \\ \left[\begin{array}{c} \frac{8779881118476697407}{11711} \\ \frac{3610327141445948005}{23422} \\ \frac{5416863976649117543}{11711} \\ \frac{13839883865944116065}{23422} \end{array}\right] \end{matrix}$$

Integrality certification: Connection with high-order residue

Any rational vector $v \in \mathbb{Q}^{n\times 1}$ with denominator $s \in \mathbb{Z}_{>0}$ has an integral $q \in \mathbb{Z}^{n\times 1}$ and a fractional part $c \in (\mathbb{Z}/s)^{n\times 1}$ such that

$$v = q + \frac{1}{s}c.$$

Example

$$A^{-1}b = \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} q + \frac{c}{s} \end{matrix} \begin{bmatrix} 749712331865485 + \frac{2572}{11711} \\ 154142564317562 + \frac{10841}{23422} \\ 462544955738119 + \frac{5934}{11711} \\ 590892488512685 + \frac{7995}{23422} \end{bmatrix}$$

Integrality certification: Connection with high-order residue

Any rational vector $v \in \mathbb{Q}^{n\times 1}$ with denominator $s \in \mathbb{Z}_{>0}$ has an integral $q \in \mathbb{Z}^{n\times 1}$ and a fractional part $c \in (\mathbb{Z}/s)^{n\times 1}$ such that

$$v = q + \frac{1}{s}c.$$

Example

$$A^{-1}b = \begin{matrix} \\ \\ \\ \\ \end{matrix} \begin{matrix} q + \frac{c}{s} \\ \left[\begin{array}{l} 749712331865485 + \frac{2572}{11711} \\ 154142564317562 + \frac{10841}{23422} \\ 462544955738119 + \frac{5934}{11711} \\ 590892488512685 + \frac{7995}{23422} \end{array}\right] \end{matrix}$$

Integrality certification: Connection with high-order residue

Any rational vector $v \in \mathbb{Q}^{n\times 1}$ with denominator $s \in \mathbb{Z}_{>0}$ has an integral $q \in \mathbb{Z}^{n\times 1}$ and a fractional part $c \in (\mathbb{Z}/s)^{n\times 1}$ such that

$$v = q + \frac{1}{s}c.$$

Example

$$A^{-1}b = \begin{bmatrix} q + \frac{c}{s} \\ 749712331865485 + \frac{2572}{11711} \\ 154142564317562 + \frac{10841}{23422} \\ 462544955738119 + \frac{5934}{11711} \\ 590892488512685 + \frac{7995}{23422} \end{bmatrix}$$

- Cost of computing only c/s
  $\sim$ the bitlength of s.

Integrality certification: Connection with high-order residue

Any rational vector $v \in \mathbb{Q}^{n\times 1}$ with denominator $s \in \mathbb{Z}_{>0}$ has an integral $q \in \mathbb{Z}^{n\times 1}$ and a fractional part $c \in (\mathbb{Z}/s)^{n\times 1}$ such that

$$v = q + \frac{1}{s}c.$$

Example

$$A^{-1}b = \begin{bmatrix} q + \frac{c}{s} \\ 749712331865485 + \frac{2572}{11711} \\ 154142564317562 + \frac{10841}{23422} \\ 462544955738119 + \frac{5934}{11711} \\ 590892488512685 + \frac{7995}{23422} \end{bmatrix}$$

- Cost of computing only c/s $\sim$ the bitlength of s.

- Let R be a high order residue: $A^{-1} = D + A^{-1}RX^k$
- Compute $sA^{-1}Rb$, which will have length $O(\log s + \log ||b||)$, then reduce modulo s

Tool: **Fast-Integrality-Cert**

- Given:
  - $A \in \mathbb{Z}^{n \times n}$ and $B \in \mathbb{Z}^{n \times m}$
  - $s \in \mathbb{Z}_{>0}$
  - $X \in \mathbb{Z}_{>0}$

    Note: require $X \perp \det A$ and $\log X \in O(\log n + \log ||A||)$
- Compute:
  - Determine if $sA^{-1}B$ is integral. If so, return $\mathrm{Rem}(sA^{-1}B, s)$
- Compromises:
  - $m \times d \in O(n)$
  - $m \times (\log s + \log ||B||) \in O(n(\log n + \log ||A||))$

Fast-Integrality-Cert costs $O(n^{\omega}\, \mathrm{M}(\log n + \log ||A||) \log n)$