Solving Ax=b over Q

September 28, 2023 8:44 AM

Let $A \in \mathbb{Z}^{n \times m}$, $b \in \mathbb{Z}^n$

How fast can we solve $Ax=b$ for $x \in \mathbb{Q}^n$?

Cramer's Rule. Let $A^{(i)} = A$ with column i replaced by b.

Then $x_i = \frac{y_i}{D}$ where $y_i = \det(A^{(i)})$ and $D = \det(A)$.

E.g. $A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$, $b = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $A^{(1)} = \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$ $A^{(2)} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$, $x = \begin{bmatrix} 2/3 \\ -1/3 \end{bmatrix}$.

$\det(A) = 3$ $y_1 = 2$ $y_2 = -1$

How big can y_i and D be?

Suppose $|A_{ij}| < B^m$ and $|b_i| < B^m$ (m digits base B).

Hadamards bound: $|\det(A)| < \sqrt{n}^n \cdot B^{mn}$

$\log_B \sqrt{n}^n B^{mn} = n \underbrace{\log_B \sqrt{n}}_{<1} + mn < n + mn$ digits base B.

So $|\det(A)|$ and $|\det(A^{(i)})|$ of length at most $n+mn$ digits base B.

The Bareiss/Edmonds/Dickson algorithm computes the y_i and D with no fractions then $x_i = \frac{y_i}{D}$ ← gcd.

It does $O(n^3)$ integer $-, \times$, exact $\div$ on integers of size $O(mn)$ bits which gives $O(n^3 (mn)^2) = O(n^5 m^2)$.

(# ops, size, cost of $\times, \div$ is quadratic)

The Dixon/Mönck algorithm reduces this to $O(n^3 m^2)$.

Let p be a prime s.t. $p \nmid \det(A)$. Main Idea.

Solve $Ax = b \bmod p^k$ s.t. p^k is large enough so that $x \in \mathbb{Q}$ can be recovered using rational number reconstruction.

Let $x \bmod p^k = \underbrace{x_0}_{\mathbb{Z}_p^n} + \underbrace{x_1}_{\mathbb{Z}_p^n} \cdot p + x_2 \cdot p^2 + \cdots + \underbrace{x_{k-1}}_{\mathbb{Z}_p^n} \cdot p^{k-1}$ (base p rep)

E.g. $x \bmod 5^2 = \begin{bmatrix} 9 \\ 16 \end{bmatrix} = \begin{bmatrix} 4+1\cdot 5 \\ 1+3\cdot 5 \end{bmatrix} = \underbrace{\begin{bmatrix} 4 \\ 1 \end{bmatrix}}_{=x_0} + \underbrace{\begin{bmatrix} 1 \\ 3 \end{bmatrix}}_{=x_1} \cdot 5$

Step ①. Compute $A^{-1} \bmod p$. $[A \bmod p \mid I_n] \sim [I \mid A^{-1} \bmod p]$
E.E Cost $O(n^3)$ $\frac{4}{3}n^3 + \cdots$

If A^{-1} doesn't exist so $p \mid \det(A)$ then try another prime p.
If this happens 10 times then probable $\det(A) = 0$.

Step ② Solve $b - Ax \equiv 0 \bmod p^k$ for x.

$\Rightarrow$ $b - A(x_0 + x_1 \cdot p + x_2 p^2 + \cdots + x_{k-1} \cdot p^{k-1}) \equiv 0 \bmod p^k$ (*)

Solve (*) $\bmod p$ $b - A(x_0) \equiv 0 \bmod p \Rightarrow x_0 = A^{-1} \cdot \underbrace{b}_{e_0} \bmod p$.

Solve (*) $\bmod p^2$ $b - A(x_0 + x_1 p) \equiv 0 \bmod p^2$

$\Rightarrow (b - Ax_0) - Ax_1 p \equiv 0 \bmod p^2$

$\Rightarrow \underbrace{\frac{(b - Ax_0)}{p}}_{e_1} - Ax_1 \equiv 0 \bmod p$.

$\Rightarrow x_1 = A^{-1} \cdot \left(\underbrace{\frac{b - Ax_0}{p}}_{\in \mathbb{Z}} \right) \bmod p$. $x_1 = A^{-1} \cdot e_1 \bmod p$

Solve (*) $\bmod p^3$ $b - A(x_0 + x_1 p + x_2 \cdot p^2) \equiv 0 \bmod p^3$

$\Rightarrow [b - A(x_0 + x_1 \cdot p)] - Ax_2 p^2 \equiv 0 \bmod p^3$

$\mid p^2 \Rightarrow \left(\frac{b - A(x_0 + x_1 p)}{p^2} \right) - Ax_2 \equiv 0 \bmod p$.

$\Rightarrow \frac{\left(\frac{b - Ax_0}{p} \right) - Ax_1}{p} = \frac{e_1 - Ax_1}{p} = e_2$

$x_2 = A^{-1} \cdot e_2 \bmod p$.

Step ③. $e_0 = b$ $x = 0^n$

for $k = 0, 1, 2, \ldots$

$x_k = A^{-1}(e_k) \bmod p$.

$x = x + x_k \cdot p^k$.

if $k+1 \in \{1, 2, 4, 8, 16, 32, \ldots\}$ then

if $k+1 \in \{1, 2, 4, 8, 16, 32, \dots\}$ then

Let y = result of $RR(x \bmod p^k)$.

If $y \neq$ FAIL and $b - Ay = 0$ then output y.

$$e_{k+1} = \frac{e_k - Ax_k}{p} \quad \text{over } \mathbb{Z}$$

$\uparrow$ exact $\div$

① Key idea 1: Compute $A^{-1} \bmod p$ once. $\leftarrow O(n^3)$

② Key idea 2: $e_{k+1} = \frac{e_k - A \cdot x_k}{p}$ $\leftarrow O(n^2 m)$