Solving Ax=b

September 24, 2021 8:16 AM

Let $A \in \mathbb{Z}^{n\times n}$, $b \in \mathbb{Z}^n$, $|A_{ij}| < B^m$, $|b_i| < B^m$.
How fast can we solve $Ax=b$ for $x \in \mathbb{Q}^n$?
How big are the integers in x?

Cramers Rule Let $A = [A_1|A_2|\cdots|A_n]$ and $A^{(i)} = [A_1|\cdots|b|\cdots A_n]$ (ith column.)
Then $x_i = y_i/\det(A)$ where $y_i = \det(A^{(i)})$.

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

$\Rightarrow x = \begin{bmatrix} 2/3 \\ -1/3 \end{bmatrix}$ $y_1 = \det(A^{(1)}) = 2$ $y_2 = \det(A^{(2)}) = -1$

Recall Hadamards Bound for A $|A_{ij}| < B^m$ and $|b_i| < B^m$

$\det(A) \le \sqrt{n}^n B^{mn}$ and $\det(A^{(i)}) \le \sqrt{n}^n B^{mn}$

$\log_B(\sqrt{n}^n B^{mn}) = mn + n\underbrace{\boxed{\log_B \sqrt{n}}}_{}^{<1} \le mn+n$ digits base B

Therefore both determinants $\sim mn$ digits base B.

Size of $[A|b] \le (n^2+n)m$ digits $\in O(mn^2)$
Size of $x \le n\,2(mn+n)$ digits. $\in O(mn^2)$.

Modular Algorithm. Takahasi & Ishibashi 1961 Cabay 1971.

1. For primes $p_1, p_2, \ldots, p_k$ s.t. $\prod p_i > 2\max(\det(A), \det(A^{(i)})$
   solve $\boxed{Ax = b \bmod p_j}$ for $x^{(j)} \in \mathbb{Z}_{p_j}^n$ and $d^{(j)} \in \mathbb{Z}_{p_j} = \det(A) \bmod p_j$.

   $[A|b] \sim \left[\begin{array}{cccc|c} x & x & x & x & y \\ 0 & x & x & x & y \\ 0 & 0 & x & x & y \\ 0 & 0 & 0 & x & y \end{array}\right]$ using $O(n^3)$ arith. ops mod p_j using Gaussian Elim.

2. $d = \det(A) = \mathrm{CRT}((d^{(j)}, p_j) : 1 \le j \le k)$.
   $y_i = \mathrm{CRT}((d^{(j)} \cdot x_i^{(j)} \bmod p_j, p_j) : 1 \le j \le k)$.
   $(x_i = y_i/d) \bmod p_j$

3. Construct $x_i = y_i/d$. Requires removing $\gcd(y_i, d)$.

Cost: $O(mn)O(n^3) + O(mn)\underbrace{(n^2+n)}_{A\ \ b}\underbrace{O(m)}_{\bmod p_j} + \underbrace{(n+1)}_{y_i\ \ d}\underbrace{O(mn)^2}_{\text{CRT}} + \underbrace{n}_{\# y_i}\underbrace{O(mn)^2}_{\text{size}}^{\text{Euclid}}$

Cost: $\underbrace{O(mn)\,O(n^3)}_{\text{G.E.}} + \underbrace{\underset{\uparrow \#\text{primes}}{O(mn)}\,(\underset{\uparrow \#\text{integers}}{n^2+n})\,O(m)}_{\phi_p} + \underbrace{(n+1)\,O(mn)}_{\text{CRT}} + \underset{\uparrow \# y_i}{n}\,O(\underset{\uparrow \text{size}}{m^2})$

$\in O(n^4 m + m^2 n^3)$. Bareiss costs $O(n^5 m^2)$

<u>p-adic lifting + rational reconstruction.</u> Dixon 1982
Mönck & Carter 1979.

Let p be a prime s.t. $p \nmid \det(A)$.
Solve $Ax = b \bmod p^k$ s.t. p^k is large enough so that $x \in \mathbb{Q}^n$ can be recovered using rational reconstruction.

Let $\underset{\mathbb{Q}^n}{\underset{\cap}{x}} \bmod p^k = \underset{\mathbb{Z}_p^n}{\underset{\cap}{x_0}} + \underset{\mathbb{Z}_p^n}{\underset{\cap}{x_1}} \cdot p + x_2 \cdot p^2 + \dots + x_{k-1} p^{k-1} + \dots$ (Base p rep.)

Step (1) Compute $A^{-1} \bmod p$ via $[A \mid I] \overset{\text{GE}}{\sim} [I \mid A^{-1}]$ in $O(n^3)$ ops.
If $A^{-1} \bmod p$ does not exist $\overset{?}{\Longrightarrow} \det(A) = 0$.
Check if $\det(A) = 0 \bmod$ a second prime.

$|\det(A)| < n^{\sqrt{n}} B^{mn}$

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

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

$k=1$ Solve $b - Ax_0 \equiv 0 \bmod p^1 \Rightarrow x_0 = A^{-1} \underset{e_0}{b} \bmod p$

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

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

$|p$

$\Rightarrow \frac{b - Ax_0}{p} - Ax_1 \equiv 0 \bmod p$

$\Rightarrow x_1 = A^{-1} \cdot \left(\underset{\uparrow e_1}{\frac{b - Ax_0}{p}}\right) \bmod p$.

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

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

$|p^2 \Rightarrow \frac{b - A(x_0 + x_1 p)}{p^2} - Ax_2 \equiv 0 \bmod p^1$

$\Rightarrow \frac{b - Ax_0}{\ } - Ax_1 \quad Ax_2 \equiv 0 \bmod p^1$

$$\Rightarrow \quad e_2 \rightarrow \frac{\frac{b - Ax_0}{p} - Ax_1}{p} - Ax_2 \equiv 0 \mod p^1$$

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

Step ②

$e_0 \leftarrow b$

$x \leftarrow 0^n$

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

$x_k \leftarrow A^{-1} \cdot e_k \mod p.$

$x \leftarrow x + x_k p^k$ // $k=0 \Rightarrow Ax \equiv 0 \mod p$

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

$y :=$ result of $RR(x \mod p^k)$.

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

$e_{k+1} \leftarrow \frac{e_k - Ax_k}{p}$ ← exact ÷ in $\mathbb{Z}$.

Key idea 1. Compute A^{-1} once $O(n^3)$ and reuse A^{-1}

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

matrix × vector $O(n^2)$.

② Key idea 2.

$$e_{k+1} = \frac{e_k - A \cdot x_k}{p}$$

$m \cdot 1 \cdot n^2$

$n \cdot 1$

Exercise

Analyze the running time for $|A_{ij}| < B^m$ $|b_i| < B^m$.

Assume $k = L$ lifting steps to recover x.

In general $L \in O(mn)$.