Solving systems of linear equations over the integers.

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

want to find (all) $x \in \mathbb{Z}^n$ s.t.

$$Ax = b.$$

Easier than this:

$\mathbb{Z}$'s replaced by $\mathbb{Q}$'s.

Each entry of A, b is an $\leq t$ bit rational number

$$\left[\ A\ \right]\left(x\right) = \left(b\right)$$

numerator, denominator $\in \mathbb{Z}$ are $\leq 2^t \cdot m$ abs value

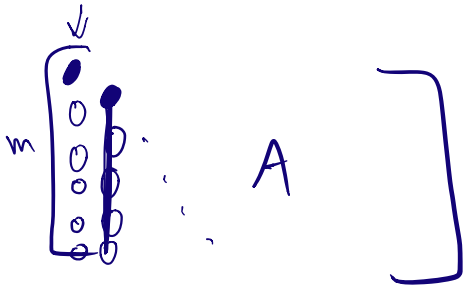
$\Updownarrow$ (possibly reordering columns).

$$\left(P\ A\right) \quad x = \quad P\ b$$

for invertible $m \times m$ P

where PA = upper triangular

Then read out entries of x in order. $x_n \cdots x_1$



mn entry operations per column

$\Rightarrow$

So totally $\leq O(mn^2)$ operations on rational numbers.

Question How complicated do the numbers get?

Claim All intermediate numbers are $\leq$ poly (t, m, n) bit rational numbers.

If M is a $k \times k$ square matrix with

entries being $\leq t$-bit rational numbers,

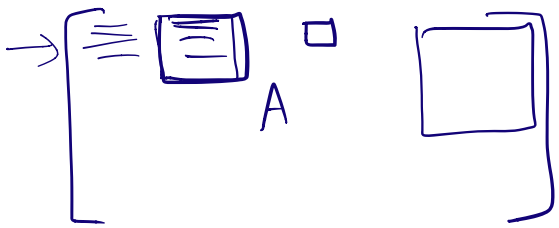
then $\det(M)$ is a $\leq O(k^2 t)$ bit rational number.

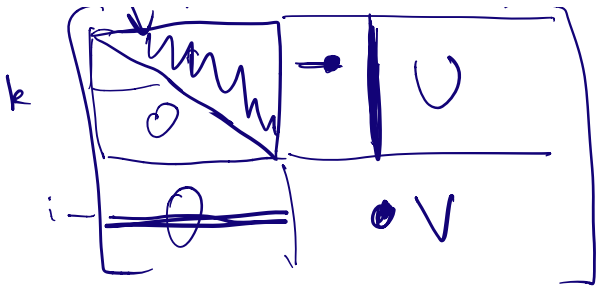
Proof $\det(M) = \frac{\text{numerator}}{\text{common denominator}}$

$\text{num} \leq k! \left[(2^t)^{k^2}\right]$ which is $\leq k \log k + k^2 t$ bits

$\text{denom} \leq (2^t)^{k^2}$ which is $\leq k^2 t$ bits

$\leq O(k^2 t)$ bits





Entry $V_{ij} = \det\left(\begin{array}{cc} B_k & \text{col } j \text{ of } U \\ \text{row } i \text{ of } V & V_{ij} \end{array}\right) \Big/ \det(B_k)$

$\det(B_k)$ // $\det$ (top left $k \times k$ submatrix of A)

$= \pm$ corresponding sub det of A.

V_{ij} = ratio of subdeterminants of A

and so is a $\leq$ poly(t, m, n) bit rational number

Another algorithm.

Do things in $\mathbb{F}_p$ for a single

very large p, ensuring that Gaussian elimination does not blow up.

Need to connect it back to $\mathbb{Q}$.

Equation

$$\Rightarrow a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = b$$

$$a_1, \ldots a_n, b \in \mathbb{Z}.$$

Q. When is there $x_1, \ldots, x_n$ s.t. this holds?

Ans: When $GCD(a_1, \ldots, a_n) \mid b$.

$$A x = b.$$

Space of solutions looks like

$$x_0 + \{ x : Ax = 0 \}.$$

$\in \mathbb{Z}^n$

↙

We get a lattice in $\mathbb{Z}^n$.

Lattices

$L \subseteq \mathbb{R}^n$ is a lattice if it is a discrete subgroup.

Thm

Every lattice in $\mathbb{R}^n$ has a basis of $\leq n$ elements.

ie. $\{\vec{a}_1, \dots \vec{a}_m\} \subseteq L$ s.t.

$$L = \left\{ \sum \vec{a}_i x_i \ : \ x_i \in \mathbb{Z} \right\}.$$

and $\vec{a}_i$ linearly independent over $\mathbb{R}$.

Smith Normal form

$M \in \mathbb{Z}^{m \times n}$

then $\exists$ P, Q s.t.

$$P \in GL_m(\mathbb{Z})$$
$$Q \in GL_n(\mathbb{Z})$$

$$PMQ = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$$ D diagonal $n \times n$.

PMQ: $(m \times m)$ $(m \times n)$ $n \times n$; $\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$: $m \times n$

$$L = \{ Mx : x \in \mathbb{Z}^n \} \subseteq \mathbb{Z}^m.$$

$$= \{ MQx : x \in \mathbb{Z}^n \} \subseteq \mathbb{Z}^m.$$

$$PL = \{ PMQx : x \in \mathbb{Z}^n \} \subseteq \mathbb{Z}^m$$

$$= \left\{ \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix} x : x \in \mathbb{Z}^n \right\}$$

$$L = P^{-1} \cdot \{ (x_1 d_1, x_2 d_2, \ldots, x_n d_n) : x \in \mathbb{Z}^n \}$$

$\Rightarrow$

$$\subseteq \mathbb{Z}^m$$

$n \leq m$

shows that L has a basis of size n.