Solving systems of linear equations over integers

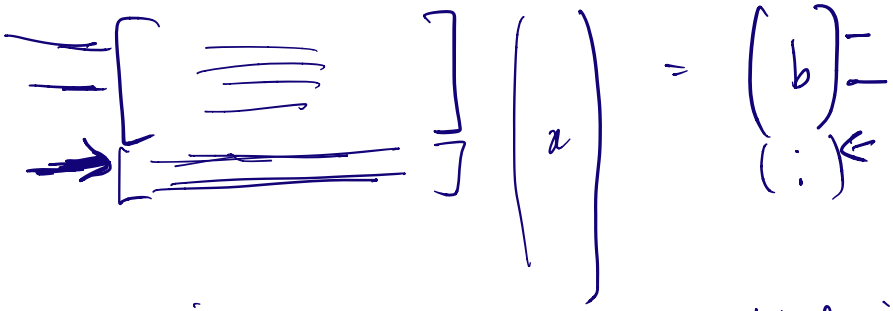
$A \in \mathbb{Z}^{m \times n}$ $\quad b \in \mathbb{Z}^m$

all entries are $\leq t$ bits.

PROBLEM Find all $x \in \mathbb{Z}^n$ s.t.

$Ax = b$.

- First: Make A have full row rank. over $\mathbb{Q}$.



If w_i is a row of A that is a certain linear combination of the remaining rows w_j of A, then

① if b_i is the same linear combination of the corresponding b_j's, then we can throw away the i^{th} row of A, i^{th} entry of b in our system of eqns.

② if not, then the system has no solutions.

Step 2

$$\underbrace{\begin{bmatrix} | & | & & | \\ a_1 & a_2 & \cdots & a_n \\ | & | & & | \end{bmatrix}}_{A} \begin{pmatrix} x \end{pmatrix} = \begin{pmatrix} b \end{pmatrix}$$

Operations on columns of A so that the $\underset{\uparrow}{2}$-column span stays unchanged

① replace column a_i with $a_i + \underline{=} a_j$ for $j \neq i$

$k \in \mathbb{Z}$.

(2) $a_i \to -a_i$

(3) Swap columns.

Using these operations, we can make A lower triangular.

For such an A,
checking if there is a solution to $Ax = b$ is just some divisibility checks. (Can find x_i's one by one).

$a_{11} \mid b_1$

$a_{22} \mid b_2 - a_{21} \cdot \left(\frac{b_1}{a_{11}}\right)$

$\vdots$

Special case:

If $m = 1$,

$A = [\quad\quad\quad]$

and column operations make it

$= [d\ 0\ 0\ \cdots\ 0]$

where d = GCD of entries of A.

Existence of column operations to make A lower triangular

First focus on the first row.

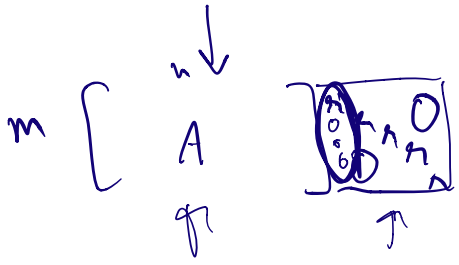
By Euclid's GCD alg., we can make it $(d\ 0\ 0 \cdots 0)$

Then ignore the first row and column and repeat.

Efficient algorithm

$\lceil\ n\ \rceil$

$m \begin{bmatrix} A \end{bmatrix}$



with the same column span.

Take some m columns from S that are linearly independent.

A_S is invertible.

$$A_S \cdot \operatorname{adj}(A_S) = \begin{bmatrix} \det(A_S) & & 0 \\ & \ddots & \\ 0 & & \det(A_S) \end{bmatrix}$$

So for b, all columns are in the $\mathbb{Z}$-column span of A.

Algorithm for checking if $\mathbb{Z}$-column span of A contains b.

1. Compute S, A_S, $\det(A_S)$ as above.

2. For each $i \in [m]$,
record the $\mathbb{Z}$-linear combination of the original columns of A that sum up to $i \to \begin{pmatrix} \vdots \\ \det(A_S) \\ \vdots \end{pmatrix} = w_i$

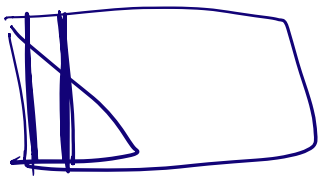
3. For each $i \in [m]$.
Focus on the bottom right $(m-i+1) \times (n-i+1)$ submatrix of A.

Do column operations to make the top row of this submatrix

$$[* \; 0 \; 0 \; \cdots \; 0]$$
($n-i+1$)

Along the way, if any entry of the matrix is $> \det(A_S)/2$ in absolute value, reduce it using w_i.

At the end we have a LT matrix (possibly different from what we could have gotten without using the w_j).

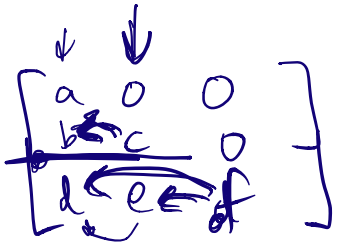


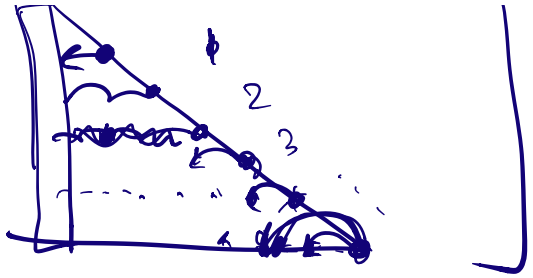
If we also ask that the final A has:

1. $A_{ii} > 0$.
2. $A_{ij} \in [0, A_{ii} - 1]$ for $i > j$

then the final Lower triangular A is canonically associated with the $\mathbb{Z}$-column span of A.

This is the Hermite-Normal-Form of A.




1
2
3
4