§1 Coding length and the ellipsoid method

23.10.18

(1) For $\alpha = p/q \in \mathbb{Q}$ with $p, q \in \mathbb{Z}$ coprime

a) let

$$\text{size}(\alpha) := 1 + \lceil \log_2(|p|+1) \rceil + \lceil \log_2(|q|+1) \rceil .$$

Also, for $c = (\gamma_1, \dots, \gamma_n) \in \mathbb{Q}^n$:

$$\text{size}(c) := n + \text{size}(\gamma_1) + \dots + \text{size}(\gamma_n)$$

and, for $A = (\alpha_{ij}) \in \mathbb{Q}^{m \times n}$:

$$\text{size}(A) := mn + \sum_{i,j} \text{size}(\alpha_{ij})$$

Further

$$\text{size}(a x \le \beta) := 1 + \text{size}(a) + \text{size}(\beta)$$

$$\text{size}(Ax \le b) := 1 + \text{size}(A) + \text{size}(b)$$

b) <u>Prop</u> Let $A \in \mathbb{Q}^{n \times n}$ with $\text{size}(A) = \sigma$.

Then $\text{size}(\det A) < 2\sigma$.

Proof. Let $A = (p_{ij} / q_{ij})_{i,j}$ where

$p_{ij}, q_{ij} \in \mathbb{Z}$ coprime and $q_{ij} > 0$.

Further, let $\det A = p/q$ with ...

$$\Longrightarrow \quad q \le \prod_{i,j}^{n} q_{ij} < 2^{\sigma - 1}$$

Leibniz + det / size

Also $|\det A| \le \prod_{i,j} (|p_{ij}| + 1)$

$$\Rightarrow |p| = |\det A| \cdot q \leq \prod_{i,j} (|p_{ij}|+1)\, q_{ij} < 2^{\sigma - 1}$$

$\Rightarrow$ size $(\det A)$

$$= 1 + \lceil \log_2(|p|+1) \rceil + \lceil \log_2(|q|+1) \rceil < 2\sigma.$$

$\square$

c) <u>Cor</u> For $A \in GL_n \mathbb{Q}$ we have

size $(A^{-1}) \in$ poly (size (A))

d) <u>Cor</u> Let $A \in \mathbb{Q}^{m \times n}$ and $b \in \mathbb{Q}^m$.

If $Ax = b$ has a solution then there is a solution $x \in \mathbb{Q}^n$ with

size $(x) \in$ poly (size $(Ax=b)$)

Proof. Assume that A has linearly independent rows, and $A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$ with A_1 nonsingular. Then

$$x_0 = \begin{pmatrix} A_1^{-1} b \\ 0 \end{pmatrix}$$ is a solution, and

the claim follows from c). $\square$

e) <u>Cor</u> The decision problem

"Given A and b rational, does $Ax = b$ have a solution?"

has a good characterization.

Proof.

If answer positive then d) provides a certificate of polynomial size.

Suppose $Ax = b$ does <u>not</u> have a solution

$\Leftrightarrow$ ex. y with $yA = 0$ and $yb = 1$.

Ex

Again by d) there is such a y of polynomial size. $\square$

f) <u>Cor</u> Let $A \in \mathbb{Q}^{m \times n}$ and $b \in \mathbb{Q}^m$ such that each row of $[A\ b]$ has size at most φ. If $Ax = b$ has a solution then

$$\{x \mid Ax = b\} = \{x_0 + \lambda_1 x_1 + \dots + \lambda_t x_t \mid \lambda_i \in \mathbb{Q}\}$$

for certain $x_0, x_1, \dots, x_t \in \mathbb{Q}^n$ of size at most $4n^2\varphi$.

Proof. By Cramer's rule the coefficients of $x_0, x_1, \dots, x_t$ can be described as quotients of subdeterminants of $[A\ b]$ of order $\leq n$. By b) these determinants have size $\leq 2n\varphi$ $\Rightarrow$ each coeff of x_i has size $\leq 4n\varphi$ $\Rightarrow$ $\text{size}(x_i) \leq 4n^2\varphi$. $\square$

(2) a) Gauß elimination transforms a given matrix A into the standard form

$\begin{bmatrix} B & C \\ 0 & 0 \end{bmatrix}$: where B is nonsingular upper triangular

by row operations $a_{i,\cdot} \mapsto a_{i,\cdot} + \lambda a_{j,\cdot}$ and permutations of rows / columns.

Rem Sometimes further reduction to

$\begin{bmatrix} \Delta & D \\ 0 & 0 \end{bmatrix}$ where Δ diagonal matrix necessary / useful.

b) Thm (Edmonds 1967)

For A rational Gauß elimination is a polynomial time algorithm.

Proof. W.l.o.g. assume that no permutations of rows or columns are necessary. Polynomially many arithmetic operations suffice, $O(n^3)$ i.e. polynomial in the arithmetic model.

The procedure generates matrices

$A_0 := A, A_1, A_2, \ldots$ where $D_k = (\delta_{ij})$

$A_k = \begin{bmatrix} B_k & C_k \\ 0 & D_k \end{bmatrix}$ where B_k non-singular upper triang of order k

then A_{k+1} obtained from A_k by row operation with pivot element $\delta_{11} \neq 0$ (as we assumed that no sorting necessary)

To show: $\operatorname{size}(A_k) \in \operatorname{poly} \operatorname{size}(A)$.

We have

$$\delta_{ij} = \det\left((A_k)^{1,\dots,k,k+i}_{1,\dots,k,k+j}\right) / \underbrace{\det\left((A_k)^{1,\dots,k}_{1,\dots,k}\right)}_{= B_k}$$

submatrix induced by selection of rows / cols

$$= \det\left(A^{1,\dots,k,k+i}_{1,\dots,k,k+j}\right) / \det\left(A^{1,\dots,k}_{1,\dots,k}\right)$$

$$\Longrightarrow \quad \operatorname{size}(\delta_{ij}) \leq 4 \operatorname{size}(A).$$

Prop. b)

Since each entry of B_k and C_k have been coefficients of D_j for some $j < k$ the claim follows. $\square$

c) <u>Cor</u> The following problems are polynomially solvable.

i) determining the rank of a (rational) matrix

ii) — " — the rank of a matrix

iii) — " — the inverse of a matrix [Ren]

iv) testing vectors for linear independence

v) solving a system of linear equations.

decision problem!