§ 1 Coding length and the ellipsoid method

(1) For \( \alpha = \nu / q \in \mathbb{Q} \) with \( \frac{23}{10} \leq \alpha \), let

\[ \nu, q \in \mathbb{Z} \text{ coprimi} \]

\[ \text{size} (\alpha) := 1 + \left[ \log_2 (|\nu| + 1) \right] + \left[ \log_2 (|q| + 1) \right] \]

Also, for \( c = (c_1, \ldots, c_n) \in \mathbb{Q}^n \)

\[ \text{size} (c) := n + \text{size} (c_1) + \ldots + \text{size} (c_n) \]

and, for \( A = (a_{i,j}) \in \mathbb{Q}^{m \times n} \),

\[ \text{hit} (A) := mn + \sum_{i,j} \text{size} (a_{i,j}) \]

Further

\[ \text{size} (\alpha X \leq \beta) := 1 + \text{size} (\alpha) + \text{size} (\beta) \]

\[ \text{size} (\alpha X \leq \beta) := 1 + \text{size} (\alpha) + \text{size} (\beta) \]

b) Proof. Let \( A \in \mathbb{Q}^{m \times n} \) with \( \text{hit} (A) = \sigma \).

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

Proof. Let \( A = (a_{i,j} / q_{i,j})_{i,j} \) where

\[ a_{i,j}, q_{i,j} \in \mathbb{Z} \text{ coprimi and } q_{i,j} > 0 \]

Further, let \( \det A = \nu / q \) with

\[ \Rightarrow \ q \leq \prod_{i,j} q_{i,j} < 2^{\sigma-1} \]

Also \( \det A \leq \prod_{i,j} (|a_{i,j}| + 1) \)
Ink Huh At.
atE
II. ftp.jltt) Gigs 2 “
⇒ site (det A)
   = 1 + \log_2 (|\text{det} A| + 1) \log_2 (|\text{det} A| + 1) < 2^{n-1}
⇒ site (det A)

\begin{align*}
\Rightarrow |\text{det} A| &< 2^{n-1} \\
\Rightarrow \text{site } (\text{det } A) \\
&= 1 + \log_2 (|\text{det} A| + 1) \log_2 (|\text{det} A| + 1) < 2^{n-1}
\end{align*}

\[ \text{c) Car For } A \in \text{GL}_n \mathbb{Q} \text{ we have} \]
\[ \text{site } (A^{-1}) \in \text{poly } (\text{site } (A)) \]

\[ \text{d) Car Let } A \in \mathbb{Q}^{m \times n} \text{ and } b \in \mathbb{Q}^m. \]

If \( AX = b \) has a solution then there is a solution \( x \in \mathbb{Q}^n \) with
\[ \text{site } (x) \in \text{poly } (\text{site } (AX = b)) \]

\[ \text{Proof. Assume that } A \text{ has linearly independent rows, and } A = (A_1, A_2) \text{ with } A_2 \text{ non-singular. Then} \]
\[ x_0 = (A_1^{-1} b, 0) \text{ is a solution, and the claim follows from c).} \]

\[ \text{e) Car The linear equation problem} \]
\[ \text{"Given } A \text{ and } b \text{ rational, does } AX = b \text{ have a solution?"} \]

\[ \text{has a good characterisation.} \]
Proof. If answer positive then d) provides a certificate of polynomial size. Suppose $Ax = b$ does not leave a solution $\Rightarrow \exists x, y$ with $yA = 0$ and $yb = 1$. (Ex)

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

4) Cor 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 $q$. If $Ax = b$ has a solution then

$$\{ x \mid Ax = b \} = \{ x_0 + \lambda_1 x_1 + \ldots + \lambda_n x_n \mid \lambda_i \in \mathbb{Q} \}$$

for certain $x_0, x_1, \ldots, x_n \in \mathbb{Q}^n$ of size at most $4n^2q$.

Proof. By Cramer's rule, the coefficients $x_0, x_1, \ldots, x_n$ can be described as quotients of the determinants of $[A \ b]$ of order $\leq m$. By b) these determinants have size $\leq 2nq \Rightarrow$ each coeff of $x_i$ has size $\leq 4nq \Rightarrow$ size $(x_i) \leq 4n^2q$. $\square$

© 2018 Michael Joswig (TU Berlin)
(2) a) Gaussian elimination transforms a given matrix $A$ into the standard form
\[
\begin{bmatrix}
B & C \\
0 & 0
\end{bmatrix}
\]
where $B$ is a non-triangular upper triangular matrix by row operations $A_{i,j} \to A_{i,j} + \lambda A_{j,j}$, and permutation of rows/columns.

Rewriting this further reduction to
\[
\begin{bmatrix}
\Delta & D \\
0 & 0
\end{bmatrix}
\]
where $\Delta$ is a scalar matrix necessary/nuke.

b) Thus (Edmonds 1967)
For a rational Gaussian 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 $D_k = (d_{i,j})$ $A_{k+1} = \begin{bmatrix} B_k & C_k \\ 0 & D_k \end{bmatrix}$ where $B_k$ non-singular upper triangular of order $k$
Then \( A_{n+1} \) obtained from \( A_n \) by row operation with pivot element \( \delta_{11} \neq 0 \) (as we assumed that no testing was necessary).

To show: \( \text{size} (A_{n+1}) \leq \text{poly size} (A) \).

We have

\[
\delta_{ij} = \frac{\det((A_{k+1})_{i,\ldots,k})}{\det((A_{k})_{i,\ldots,k})} = B_{k+1, i, \ldots, k}
\]

Submatrix induced by selection of rows / cols

\[
= \det (A_{1, \ldots, k+1}) / \det (A_{1, \ldots, k})
\]

\[ \Rightarrow \text{size} (\delta_{ij}) \leq 4 \ \text{size} (A). \]

Prop. b)

Since each entry of \( B_{k+1} \) and \( C_{k+1} \) have been coefficients of \( D_j \) for some \( j \geq k \), the claim follows.

c) The following problems are polynomially solvable:

i) determining the rank of a (rational) matrix

ii) computing the rank of a matrix

iii) finding the inverse of a matrix

iv) testing vectors for linear independence

v) solving a system of linear equations.

© 2018 Michael Joswig (TU Berlin)