IP 23.4.19

Korollar 1.7: Für jede Matrix $A \in \mathbb{Q}^{m \times n}$ mit $\operatorname{rang}(A) = m$ gibt es eine unimodulare Matrix $U \in \mathbb{Z}^{n \times n}$ mit $HNF(A) = A \cdot U$; eine solche Matrix U kann man in polynomial in $\langle A \rangle$ berechnet zu finden.

Beweis: Satz 1.4 $\Rightarrow$ Es gibt eine Folge ω von EBOP's mit

$$HNF(A) = \omega(A) = \omega(A \cdot I_n) = A \cdot \underbrace{\omega(I_n)}_{\text{unimodular nach Satz 1.6}}$$

□

Satz 1.8: Es gibt einen Algorithmus, der zu $A \in \mathbb{Q}^{m \times n}$, $b \in \mathbb{Q}^m$ in Polynomialzeit folgendes bestimmt:

(i) Falls $Ax = b$ keine ganzzahlige Lösung besitzt:

$$y \in \mathbb{Q}^m \text{ mit } y^T A \in \mathbb{Z}^n, \langle y, b \rangle \notin \mathbb{Z}$$

(ii) Andernfalls: $x^{(0)}, x^{(1)}, \dots, x^{(t)} \in \mathbb{Z}^n$ mit $t = n - \operatorname{rang}(A)$, $x^{(1)}, \dots, x^{(t)}$ linear unabhängig, so dass

$$\{x \in \mathbb{Z}^n : Ax = b\} = x^{(0)} + \Lambda\{x^{(1)}, \dots, x^{(t)}\}$$

$$= \left\{ x^{(0)} + \sum_{i=1}^{t} \lambda_i x^{(i)} : \lambda_i \in \mathbb{Z} \ \forall i \in [t] \right\}$$

Bemerkungen:

- Satz 1.8 liefert eine gute Charakterisierung für lineare diophantische Gleichungssysteme (analog zu Satz 1.1(i) für lineare Gleichungssysteme):

  Entweder $\exists x \in \mathbb{Z}^n : Ax = b$

  oder $\exists y \in \mathbb{Q}^m : y^T A \in \mathbb{Z}^n, \langle y, b \rangle \notin \mathbb{Z}$

  (aber nicht beides: $Ax = b \Rightarrow \underbrace{x^T A}_{\in \mathbb{Z}^n} \underbrace{x}_{\in \mathbb{Z}^n} = \underbrace{\langle y, b \rangle}_{\in \mathbb{Z}}$ ↯)

  $\langle x \rangle$ polynomial beschr. in $\langle A, b \rangle$

  $\langle y \rangle$ polynomial beschr. in $\langle A, b \rangle$

- Satz 1.8(ii) liefert uns zu Satz 1.1(ii) analoge Parametrisierung der Lösungsräume linear diophantischer Gleichungssysteme.

- Beachte: $x^{(1)}, \dots, x^{(t)}$ in Satz 1.8(ii) ist eine sehr spezielle ganzzahlige Basis von $\ker(A)$.

Beweis zu Satz 1.8:

1. Schritt: Führe Gauß-Elimination für (A, b) durch

- falls $Ax = b$ (reell) unlösbar: Bestimme $y \in \mathbb{Q}^m$ mit:

$$y^T A = 0_n \in \mathbb{Z}^n \quad \text{und} \quad \langle y, b \rangle = \frac{1}{2} \notin \mathbb{Z}$$

- Andernfalls können redundante Zeilen so können annehmen: $\operatorname{rang}(A) = m$

2. Schritt: Bestimme $U \in \mathbb{Z}^{n \times n}$ unimodular mit

$$A \cdot U = HNF(A) = [B, 0], \quad B \in \mathbb{Q}^{m \times m}$$

- Für alle $x \in \mathbb{R}^n$ mit $U^{-1} x =: z = \begin{bmatrix} z' \\ z'' \end{bmatrix}$, $z' \in \mathbb{R}^m$, $z'' \in \mathbb{R}^{n-m}$ gilt:

$$\begin{array}{ccccccc} Ax = b & & AUz = b & & [B, 0] \cdot \begin{bmatrix} z' \\ z'' \end{bmatrix} = b & & z' = B^{-1} b \\ \Leftrightarrow & & \Leftrightarrow & & & & \Leftrightarrow \\ x \in \mathbb{Z}^n & & z \in \mathbb{Z}^n & & z' \in \mathbb{Z}^m, \; z'' \in \mathbb{Z}^{n-m} & & B^{-1} b \in \mathbb{Z}^m, \; z'' \in \mathbb{Z}^{n-m} \end{array}$$

- Falls $Ax = b$ keine ganzzahlige Lösung hat, gibt es also eine Zeile $y \in \mathbb{Q}^m$ von B^{-1} (z.B. die i-te) mit $\langle y, b \rangle = (B^{-1}b)_i \notin \mathbb{Z}$, aber

$$y^T A = y^T \cdot [B, 0] \cdot U^{-1} = [e_i^T, 0_{n-m}] \cdot U^{-1} = (U^{-1})_{i,*} \in \mathbb{Z}^n$$

(U unimodular)

- Andernfalls ist $B^{-1}b \in \mathbb{Z}^m$ und (mit $U = [U', U'']$, $U' \in \mathbb{Z}^{m \times m}$, $U'' \in \mathbb{Z}^{m \times (n-m)}$)

$$\{x \in \mathbb{Z}^n : Ax = b\} = \left\{ [U', U''] \cdot \begin{bmatrix} z' \\ z'' \end{bmatrix} : z' = B^{-1}b,\ z'' \in \mathbb{Z}^{n-m} \right\}$$

$$= \left\{ U' \cdot B^{-1}b + U'' \cdot z'' : z'' \in \mathbb{Z}^{n-m} \right\}$$

und wir können wählen:

$x^{(0)} := B^{-1}b$, $x^{(1)}, \dots, x^{(k)}$: Spalten von U'' ∎