IP 9.4.19

1. Lineare Diophantische Gleichungssysteme und Gitter

Satz 1.1 (Lineare Algebra)

Seien $A \in \mathbb{Q}^{m \times n}$, $b \in \mathbb{Q}^m$.

(i) Entweder

$\exists x \in \mathbb{Q}^n : Ax = b$ — Zertifikat für Lösbarkeit

oder

$\exists y \in \mathbb{Q}^m : y^T A = 0_n$, $\langle y, b \rangle = -1 \quad (\neq 0)$ — Zertifikat für Unlösbarkeit

("exklusiv oder" — "aber nicht beides")

(ii) Es gibt linear unabhängige $x^{(1)}, \dots, x^{(t)} \in \mathbb{Q}^n$ $\left(t = n - \operatorname{rang}(A)\right)$, so dass für alle $x^{(0)} \in \mathbb{Q}^n$ mit $Ax^{(0)} = b$ gilt:

$$\{x \in \mathbb{R}^n : Ax = b\} = \underbrace{x^{(0)} + \operatorname{lin}\{x^{(1)}, \dots, x^{(t)}\}}_{\text{von } x^{(1)}, \dots, x^{(t)} \text{ aufgespannter Unterraum}}$$

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

Für $A = (A_1, A_2)$ mit regulärer Matrix $A_1 \in \mathbb{Q}^{m \times m}$
(ggfs. vorher redundante Zeilen von $Ax = b$, so dass $\operatorname{rang}(A) = m$ ist,
und sortiere die Variablen geeignet):

$$\boxed{Ax = b} \iff (A_1, A_2) \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = b \iff A_1 x_1 + A_2 x_2 = b \quad | \cdot A_1^{-1}$$

$$\iff x_1 + A_1^{-1} A_2 x_2 = A_1^{-1} b \iff \boxed{x_1 = A_1^{-1} b - A_1^{-1} A_2 x_2}$$

Man kann also wählen:

$$x^{(0)} := \left(A_1^{-1} b, \mathbb{0}_{n-m} \right)$$

$$x^{(i)} := \left(A_1^{-1} \cdot (A_2)_{*,i}, \underbrace{-e_i}_{\in \mathbb{R}^{n-m}} \right)$$

Bem.: Satz 1.1 gilt analog für jeden Körper statt $\mathbb{Q}$.

Cramer's Regel

Seien $\mathbb{K}$ ein beliebiger Körper und $M \in \mathbb{K}^{k \times k}$ mit $\det(M) \neq 0$.
Dann ist die (i,j)-te Komponente von M^{-1}

$$\left(M^{-1}\right)_{i,j} = (-1)^{i+1} \cdot \frac{\det\left(\hat{M}(i,j)\right)}{\det(M)} \qquad \left(i,j \in [k]\right)$$

wobei $\hat{M}(i,j)$ die Matrix ist, welche aus M durch Streichen der i-ten Zeile und der j-ten Spalte entsteht.

Insbesondere: $M \in \mathbb{Q}^{k \times k}$, $\det(M) \neq 0 \Rightarrow M^{-1} \in \mathbb{Q}^{k \times k}$

Kodierungslängen von Determinanten

Für $A \in \mathbb{Q}^{n \times n}$ ist $\langle \det(A) \rangle \leq 2\langle A \rangle$

[Übungen]

Korollar

Zurückgeben x bzw. y in Satz 1.1 (i) und Parametrisierungsvektoren $x^{(0)}, x^{(1)}, \ldots, x^{(t)}$ in Satz 1.1 (ii) können so gewählt werden, dass ihre Komponenten polynomial in $\langle A, b \rangle$ beschränkte Kodierungslänge haben.

Satz 1.2 (Lineare Optimierung)

Seien $A \in \mathbb{Q}^{m \times n}$, $b \in \mathbb{Q}^m$.

(i) Entweder $\exists x \in \mathbb{R}^n : Ax = b,\ x \geq 0_n$

oder $\exists y \in \mathbb{R}^m : y^T A \geq 0_n^T,\ \langle y, b \rangle = -1$

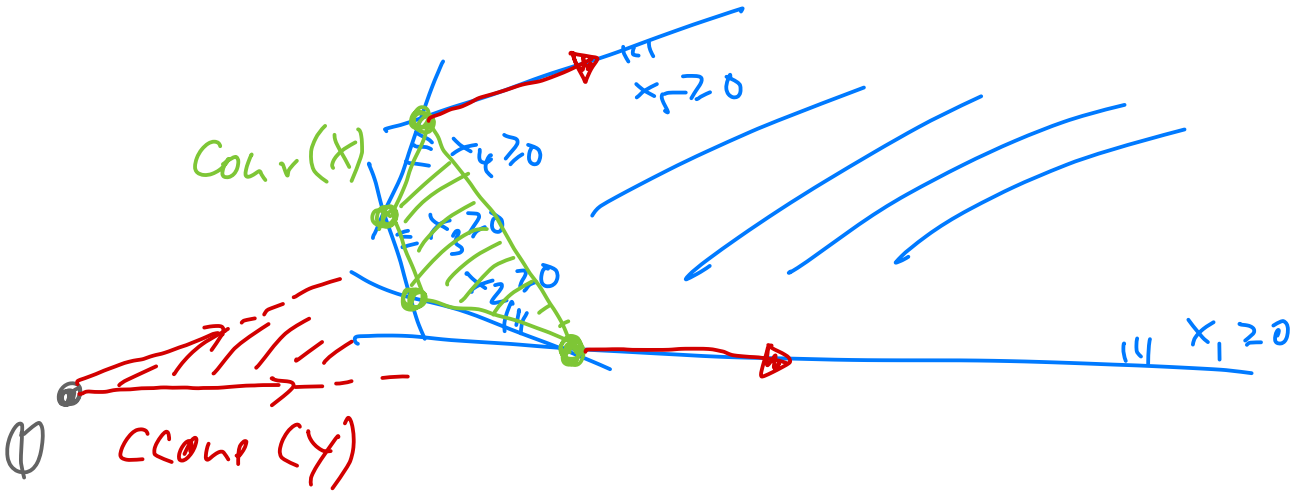
(⇝ Farkas-Lemma)

$\left\{ \sum_{y \in Y} \mu_y \cdot y : \mu_y \geq 0 \ \forall y \in Y \right\}$ "konvex-konische Hülle"

(ii) Es gibt endliche Mengen $X, Y \subseteq \mathbb{Q}^n$ mit

$$\{x \in \mathbb{R}^n : Ax = b,\ x \geq 0_n\} = \boxed{\mathrm{conv}(X)} + \boxed{\mathrm{ccone}(Y)}$$

"konvexe Hülle" $= \left\{ \sum_{x \in X} \lambda_x \cdot x : \lambda_x \geq 0 \ \forall x \in X,\ \sum_{x \in X} \lambda_x = 1 \right\}$



$\mathbb{R}^5 \geq \{x \in \mathbb{R}^n : Ax = b\}$

Bemerkungen

- Die Zertifikate x und y aus Satz 2.1 (i) sowie die Variablen in X und Y in Satz 2.1 (ii) können so gewählt werden, dass ihre Komponenten polynomial in $\langle A, b \rangle$ beschränkte Kodierungslängen haben.

  Also: $|X|$ und $|Y|$ können i.A. nicht polynomial in $\langle A, b \rangle$ beschränkt werden.

- Satz 2.1 gilt analog für $\mathbb{R}$ statt $\mathbb{Q}$.

Definition: Sei $X \subseteq \mathbb{R}^n$, $|X| < \infty$.

(i) $$\Lambda(X) := \left\{ \sum_{x \in X} \lambda_x \cdot x : \lambda_x \in \mathbb{Z} \quad \forall x \in X \right\}$$

ist die von X erzeugte additive Untergruppe von $\mathbb{R}^n$ (oder: der von X erzeugte $\mathbb{Z}$-Untermodul von $\mathbb{R}^n$).

(ii) Ist X linear unabhängig, so heißt $\Lambda := \Lambda(X)$ ein "Gitter" (engl.: lattice) und X heißt dann eine Gitterbasis von Λ.

Notation: Für $A \in \mathbb{R}^{m \times n}$: $\Lambda(A) := \Lambda\left(\{A_{*,1}, \dots, A_{*,n}\}\right)$

Beispiele:

- $\Lambda\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = \mathbb{Z}^2 = \Lambda\left(\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\right) = \Lambda\left(\begin{bmatrix} 1 & 1 & -4 \\ 1 & 2 & 5 \end{bmatrix}\right)$
- $\mathbb{Z}^1 = \mathbb{Z} = \Lambda(\{1\}) = \Lambda(\{2, 3\})$