

**Nächstes Ziel:** Finde ein Zertifikat, das zeigt, dass ein Gleichungssystem *keine* ganzzahlige Lösung hat.

### Definition

Eine  $m \times n$ -Matrix  $A$  ist in **Hermiteischer Normalform**, wenn sie in der Form  $A = [B \ 0]$  geschrieben werden kann, wobei  $B$  eine reguläre nicht-negative untere Dreiecksmatrix ist, sodass in jeder Zeile von  $B$  der Diagonaleintrag der größte Eintrag ist.

Die folgenden Modifikationen von Matrizen heißen **elementare unimodulare Spaltenoperationen**:

- Vertausche zwei Spalten.
- Multipliziere eine Spalte mit  $-1$ .
- Addiere ein ganzzahligen Vielfaches einer Spalte zu einer anderen Spalte.

Nachbesprechung Hauptseminar:

→ 4.7., 18:15 Uhr

## Theorem

Jede Matrix  $A \in \mathbb{Q}^{m \times n}$  mit Rang  $m$  kann durch eine Folge von unimodularen Spaltenoperationen in eine Matrix in Hermitescher Normalform gebracht werden.

## Korollar

Sei  $A \in \mathbb{Q}^{m \times n}$  und  $b \in \mathbb{Q}^m$ . Dann hat  $Ax = b$  genau dann eine ganzzahlige Lösung  $x$ , wenn  $b^t y$  für jedes  $y \in \mathbb{Q}^m$ , für das  $A^t y$  ganzzahlig ist, ganzzahlig ist.

Beweis: " $\Rightarrow$ ": Wenn  $x$  ganzzahlig mit  $Ax = b$  ist und  $y^t A$  ganzzahlig ist, dann ist  $\underbrace{y^t A}_\text{Satz 7.7} x = y^t b$  auch ganzzahlig.   
 Satz 7.7. Satz 7.7.

**Beweis (Fortsetzung):** “ $\Leftarrow$ ”:

Es sei  $b^t y$  ganzzahlig für jedes  $y \in \mathbb{Q}^m$ , für das  $A^t y$  ganzzahlig ist.

$\Rightarrow Ax = b$  muss zulässig sein, denn sonst gäbe es nach Farkas einen Vektor  $y \in \mathbb{Q}^m$  mit  $y^t A = 0$  und  $y^t b = -\frac{1}{2}$ .

$\Rightarrow$  Können annehmen:  $A$  hat Rang  $m$ .

Beobachtung: Die Aussage des Korollars gilt genau dann für  $A$ , wenn sie für eine Matrix  $\tilde{A}$  gilt, die aus  $A$  durch Anwendung von elementaren unimodularen Spaltenoperationen hervorgeht.

$\Rightarrow$  Wir nehmen an, dass  $A$  in Hermiteischer Normalform  $A = [B \ 0]$  ist.

$\Rightarrow$   ~~$B^{-1}A$~~   $B^{-1} [B \ 0] = [I_m \ 0]$  ist eine ganzzahlige Matrix.

$\Rightarrow$  Nach Voraussetzung (angewandt auf die Zeilen von  $B^{-1}$ ) ist  $B^{-1}b$  ganzzahlig.

Wegen  $[B \ 0] \begin{pmatrix} B^{-1}b \\ 0 \end{pmatrix} = b$  ist der Vektor  $x := \begin{pmatrix} B^{-1}b \\ 0 \end{pmatrix}$  eine ganzzahlige Lösung von  $[B \ 0] x = b$ . □

## Theorem

Sei  $P = \{x \in \mathbb{R}^n \mid Ax \leq b\}$  mit  $A \in \mathbb{Q}^{m \times n}$  und  $b \in \mathbb{Q}^m$ . Dann sind die folgenden Aussagen äquivalent:

- (a)  $P$  ist ganzzahlig.  $P = \mathbb{Z}$
- (b) Jede Fläche von  $P$  enthält mindestens einen ganzzahligen Vektor.
- (c) Jede minimale Fläche von  $P$  enthält mindestens einen ganzzahligen Vektor.
- (d) Jede Stützhyperebene von  $P$  enthält mindestens einen ganzzahligen Vektor.
- (e) Jede rationale Stützhyperebene von  $P$  enthält mindestens einen ganzzahligen Vektor.
- (f)  $\max\{c^t x \mid x \in P\}$  wird für jeden Vektor  $c$ , für den das Maximum endlich ist, von einem ganzzahligen Vektor angenommen.  $c \in \mathbb{Z}^n$
- (g)  $\max\{c^t x \mid x \in P\}$  ist für jeden Vektor  $c$ , für den das Maximum endlich ist, ganzzahlig.  $c \in \mathbb{Z}^n$

Beweis: Leicht: „(b)  $\Leftrightarrow$  (c)“, „(b)  $\Rightarrow$  (d)“, „(d)  $\Rightarrow$  (e)“, „(d)  $\Rightarrow$  (g)“.

„(a)  $\Rightarrow$  (b)“: Sei  $P$  ganzzeilig.

Sei  $F = P \cap H$  eine Fläche von  $P$ ,

wobei:  $H = \{x \in \mathbb{R}^L : C^T x = d\}$  eine Stütz-

hyperebene von  $\mathcal{P}$  sei. Dabei sei  $d = \max\{C^T x : x \in P\}$

$\Rightarrow$  Jedes  $z \in F$  ist konvexkombination

von ganzzeiligen Vertices  $v_1, \dots, v_k \in P$ .

Falls  $v_j \in P(F)$ , dann gilt  $c^T v_j \leq d$  für  
 $j \in \{1, \dots, k\}$ . Wegen  $c^T z = d$  müsste es  
dann ein  $j \in \{1, \dots, k\}$  mit  $c^T v_j = d$  geben.

$\Rightarrow$  Alle  $v_1, \dots, v_k$  liegen in  $F$ .

$\Rightarrow$   $F$  enthält einen ganzzahlige Vektor.

“(K)  $\Rightarrow$  H)”: Folgt daraus, dass lineare Zielfunktionen immer in einer Minimalfläche  
realisiert werden.



"(H)  $\Rightarrow$  (a)" Es gelte (H), aber  $P \neq P_I$

$\Rightarrow$  Es gibt ein  $x^* \in P \setminus P_I$ .

$P$  rational  $\Rightarrow P_I$  ist Polyeder.

$\Rightarrow$  Es gibt eine Ungleichung  $a^T x \leq \beta$ ,

die von den Vertices in  $P_I$  erfüllt

wird, aber nicht von  $x^*$ .

$\Rightarrow a^T x^* > \beta$

Widerspruch zu (H), weil  $\{a^T x : x \in P\}$   
endlich ist.

Wissen  $(a), (b), (c)$  und  $(f)$  sind äquivalent.

„ $(e) \Rightarrow (c)$ “ können annehmen:  $A, b$  ganzzahlg.

Sei  $F = \{x \in \mathbb{R}^n : A'x = b\}$  eine minimale

Fläche von  $P$ , wobei  $A'x \leq b'$  ein Teil-

system von  $Ax \leq b$  sei.

Wenn es keinen ganzzahligen Vektor  $x$

mit  $A'x = b'$  gibt, dann gibt es nach

dem Lemma von Farkas einen rationalen

Vektor  $\gamma$ , sodass  $c := A^T \gamma$  ganzzahlig ist, während  $\delta := \gamma^T b$  nicht ganzzahlig ist.

Wir können annehmen, dass alle Einträge von  $\gamma$  positiv sind (sonst addiere eine geeignete ganzzahligen Vektor zu  $\gamma$ )

$\Rightarrow H := \{x \in \mathbb{R}^n : c^T x = \delta\}$  enthält keine ganzzahligen Vektor.

Wir zeigen  $H \cap P = F$ , was folgt, dass

$H$  eine Stützhyperebene von  $P$  ist,

die keine ganzzahligen Punkte enthält.

Nach Konstruktion gilt  $F \subseteq H$

z.z.:  $H \cap P \subseteq F$ . Sei  $x \in H \cap P$ .

$$\Rightarrow y^t A'x = c^t x = d = y^t b'$$

$$\Rightarrow y^t (A'x - b') = 0$$

Weil alle Einträge von  $y'$  positiv sind,

folgt  $A'x = b' \Rightarrow x \in F$ .

"(8)  $\Rightarrow$  (e)" Sei:  $H := \{x \in \mathbb{R}^n : e^x = \delta\}$  eine  
rationale Stützhyperfläche von  $P$  mit  
 $\max\{e^x : x \in P\} = \delta$ .

Annahme:  $H$  enthält keinen ganzzahligen  
Lektor.

Widers. kon.

$\Rightarrow$  Es gibt ein  $\delta > 0$  mit  $\delta \in \mathbb{Z}$  gan-  
zählig und  $\delta \delta$  nicht ganzzählig.

$\Rightarrow \max\{\delta \delta^x : x \in P\} = \delta \max\{e^x : x \in P\}$   
 $= \delta \cdot \delta \notin \mathbb{Z} \Rightarrow$  (8) ist nicht erfüllt.  $\square$

Definition:

Ein rationales Polyeder ist ein Polyeder,  $P$   
für das es eine Matrix  $A \in \mathbb{Q}^{m \times n}$ , und  
einen Vektor,  $b \in \mathbb{Q}^m$  mit  $P = \{x \in \mathbb{R}^n : Ax \leq b\}$   
gibt.