GDO-07 29.10.19

Korollar 1.6: Es gibt einen Algorithmus, der in Polynomialzeit für $A \in \mathbb{Q}^{m\times n}$ und $b \in \mathbb{Q}^m$, so dass $P^{\leq}(A,b)$ ein volldimensionales Polytop ist, einen ganzzahligen Punkt $\bar{x} \in P^{\leq}(A,b) \cap \mathbb{Z}^n$ oder ein $d \in \mathbb{Z}^n \setminus \{0\}$ mit

$$w_d\left(P^{\leq}(A,b)\right) \leq n\cdot(n+1)\cdot 2^{\frac{n(n-1)}{4}}$$

bestimmt.

Beweis: • Wende zunächst den Algorithmus aus Satz 1.5 an.

• Wende dann Algorithmus E auf $E\left((n+1)C, a\right)$ an
[es gilt $E\left((n+1)C, a\right) \subseteq P^{\leq}(A,b) \subseteq E(C,a)$]

• Erhalten wir ein $\bar{x} \in E\left((n+1)C, a\right) \cap \mathbb{Z}^n \left(\subseteq P^{\leq}(A,b) \cap \mathbb{Z}^n\right)$, so gib $\bar{x}$ aus und halte.

- Ansonsten erhalten wir $d \in \mathbb{Z}^n \setminus \{0\}$ mit

$$w_d\big(E((n+1)C, a)\big) \le n \cdot 2^{\frac{n(n-1)}{4}}$$

- Es gilt $w_d\big(E(C,a)\big) = (n+1) \cdot w_d\big(E((n+1)C, a)\big)$

[Für $\beta > 0$:

$$\max/\min \{\langle d, x\rangle : x \in E(\beta C, a)\}$$

$$= \max/\min \Big\{\langle d, x\rangle : \underbrace{\|\beta C(x-a)\| \le 1}_{\Updownarrow \; \underbrace{\|C(x-a)\|}_{\|Cx - Ca\|} \le \frac{1}{\beta}}\Big\}$$

$$= \max/\min \Big\{\langle d, C^{-1}y + a\rangle : \|y\| \le \frac{1}{\beta}\Big\}$$

$$= \langle d, a\rangle + \max/\min \Big\{\langle d^T C^{-1}, y\rangle : \|y\| \le \frac{1}{\beta}\Big\}$$

$$= \langle d, a \rangle +/- \frac{\|d^T C^{-1}\|}{\beta}$$

Also $w_d\big(E(\beta C, a)\big) = \frac{2}{\beta}\|d^T C^{-1}\|$]

Wegen $P^{\leq}(A,b) \subseteq E\big((n+1)C, a\big)$ ist also $w_d\big(P^{\leq}(A,b)\big) \leq n \cdot (n+1) \cdot 2^{\frac{n(n-1)}{4}}$. $\boxtimes$

<u>Satz 1.7:</u> Es gibt einen Algorithmus, der zu $A \in \mathbb{Q}^{m \times n}$ und $b \in \mathbb{Q}^m$ in Polynomialzeit $\tilde{A} \in \mathbb{Q}^{\tilde{m} \times \tilde{n}}$ und $\tilde{b} \in \mathbb{Q}^{\tilde{m}}$ mit $\tilde{n} \leq n$ (und $\tilde{m} \leq m$) berechnet, so dass $P^{\leq}(\tilde{A}, \tilde{b})$ ein volldimensionales Polytop ist mit

$$P^{\leq}(\tilde{A}, \tilde{b}) \cap \mathbb{Z}^{\tilde{n}} \neq \emptyset \iff P^{\leq}(A,b) \cap \mathbb{Z}^n \neq \emptyset$$

(und aus $\lambda \in P^{\leq}(\tilde{A}, \tilde{b}) \cap \mathbb{Z}^{\tilde{n}}$ kann man in Polynomialzeit $x \in P^{\leq}(A,b) \cap \mathbb{Z}^n$ berechnen).

Beweis: • Es gibt ein Polynom q, so dass für alle $A \in \mathbb{Q}^{m \times n}$, $b \in \mathbb{Q}^n$ gilt: Falls $P^{\leq}(A,b) \cap \mathbb{Z}^n \neq \emptyset$, so gibt es

$$\bar{x} \in P^{\leq}(A,b) \cap \mathbb{Z}^n \quad \text{und} \quad \langle \bar{x} \rangle \leq q(\langle A,b \rangle)$$

(siehe Vorlesung IP).

• Also: $P^{\leq}(A,b) \cap \mathbb{Z}^n \neq \emptyset \iff$

$$\boxed{\left(P^{\leq}(A,b) \cap [-M,M]^n\right)} \cap \mathbb{Z}^n \neq \emptyset \quad \leftarrow \text{Polytop}$$

(und $M := 2^{q(\langle A,b \rangle)}$)

• Wir müssen also nur den Fall betrachten, dass $P^{\leq}(A,b)$ beschränkt, also ein Polytop ist.

• Mittels Lösen der LP's

$$\min \{ \langle A_{i*}, x \rangle : Ax \leq b \} \qquad (i \in [m])$$

kann man in Polynomialzeit

$$\mathrm{Eq}(P^{\le}(A,b)) = \{i \in [m] : \langle A_{i*}, x\rangle = b_i \text{ für alle } x \in P^{\le}(A,b)\}$$

("Equation set")

bestimmen; bezeichne mit $Cx = d$ das System $\langle A_{i*}, x\rangle = b_i$ $(i \in \mathrm{Eq}(P^{\le}(A,b)))$.

- Dann ist $\mathrm{aff}(P^{\le}(A,b)) = \{x \in \mathbb{R}^n : Cx = d\}$.
- Wende den Algorithmus (aus Kap. 1 der IP-VL) für die Bestimmung der Lösungsmenge eines Diophantischen linearen Gleichungssystems auf $Cx = d$ an.
- Falls $\{x \in \mathbb{Z}^n : Cx = d\} = \emptyset$: Wähle $\tilde{A}x \le \tilde{b}$ als $\frac{1}{4} \le x \le \frac{3}{4}$ $(P^{\le}(A,b) \cap \mathbb{Z}^n = \emptyset = P^{\le}(\tilde{A},\tilde{b}) \cap \mathbb{Z}^{\tilde{n}}$ mit $\tilde{n} = 1)$.
- Andernfalls liefert der Algorithmus $x^{(0)}, x^{(1)}, \dots, x^{(t)} \in \mathbb{Z}^n$ mit

- $t = n - \mathrm{Rang}(C) = \dim\left(P^{\leq}(A,b)\right)$
- $\{x \in \mathbb{Z}^n : Cx = d\} = x^{(0)} + \left\{\sum_{i=1}^{t} \lambda_i x^{(i)} : \lambda_1, \dots, \lambda_t \in \mathbb{Z}\right\}$ (*)

$$\left(= x^{(0)} + \Lambda\{x^{(1)}, \dots, x^{(t)}\}\right)$$

- $\underbrace{\{x \in \mathbb{R}^n : Cx = d\}}_{\substack{\shortparallel \\ \mathrm{aff}(P^{\leq}(A,b))}} = x^{(0)} + \left\{\sum_{i=1}^{t} \lambda_i x^{(i)} : \lambda_1, \dots, \lambda_t \in \mathbb{R}\right\}$ (**)

$$\left(= x^{(0)} + \mathrm{lin}\{x^{(1)}, \dots, x^{(t)}\}\right)$$

- Wähle $\tilde{A}\lambda \leq \tilde{b}$ als das System $A \cdot \left(x^{(0)} + \sum_{i=1}^{t} \lambda_i x^{(i)}\right) \leq b$ (also $P^{\leq}(\tilde{A}, \tilde{b}) \subseteq \mathbb{R}^{\tilde{n}}$ mit $\tilde{n} = t$).
- Wegen (*) ist $P^{\leq}(A,b) \cap \mathbb{Z}^n = \varphi\left(P^{\leq}(\tilde{A},\tilde{b}) \cap \mathbb{Z}^{\tilde{n}}\right)$ mit

$$\varphi(\lambda) := x^{(0)} + \sum_{i=1}^{t} \lambda_i x^{(i)}$$

- Wegen (**) ist $P^{\leq}(A,b) = \varphi\left(P^{\leq}(\tilde{A},\tilde{b})\right)$;

da φ affiner Isomorphismus ist $[x^{(1)}, \dots, x^{(t)}$ sind linear unabhängig$]$,

ist $\dim(\underbrace{P^{\leq}(\tilde{A}, \tilde{b})}_{\subseteq \mathbb{R}^{\tilde{n}}}) = \dim(P^{\leq}(A, b)) = t = \tilde{n}$

$\boxtimes$