GDO – 06 28.10.19

**Def.:** Für $C \in \mathbb{R}^{n \times n}$ regulär und $a \in \mathbb{R}^n$ sei:

$$E(C,a) := \{x \in \mathbb{R}^n : \|C(x-a)\|_2 \leq 1\}$$

(Ellipsoid mit Mittelpunkt $a$; Bild des Einheitsballs $E(\mathbb{I}_n, 0_n)$ unter der affinen Transformation $\mathbb{R}^n \to \mathbb{R}^n$, $y \mapsto C^{-1}y + a$.)

**Def.:** Für $\alpha \in \mathbb{R}$ sei

$$\lfloor \alpha \rceil := \begin{cases} \lfloor \alpha \rfloor, & \text{falls } \alpha - \lfloor \alpha \rfloor \leq \frac{1}{2} \\ \lceil \alpha \rceil, & \text{sonst} \end{cases};$$

für $\lambda \in \mathbb{R}^n$ sei $\lfloor \lambda \rceil := (\lfloor \lambda_1 \rceil, \ldots, \lfloor \lambda_n \rceil)$.

# Algorithmus E

**Eingabe:** $C \in \mathbb{Q}^{n\times n}$ regulär, $a \in \mathbb{Q}^n$

**Ausgabe:** $\overline{x} \in E(C,a) \cap \mathbb{Z}^n$ **oder** $d \in \mathbb{Z}^n \setminus \{0\}$ mit $w_d(E(C,a)) \leq n \cdot 2^{\frac{n(n-1)}{4}}$.

① Berechne Gitterbasis $D = [d^1, \dots, d^n] \in \mathbb{Q}^{n\times n}$ von $\Lambda(C)$ mit

$$OD(D) \leq 2^{\frac{n(n-1)}{4}} \quad \text{und} \quad \|d^n\| \geq \|d^1\|, \dots, \|d^{n-1}\|.$$

② Berechne die unimodulare Matrix $U \in \mathbb{Z}^{n\times n}$ mit $C = DU$.

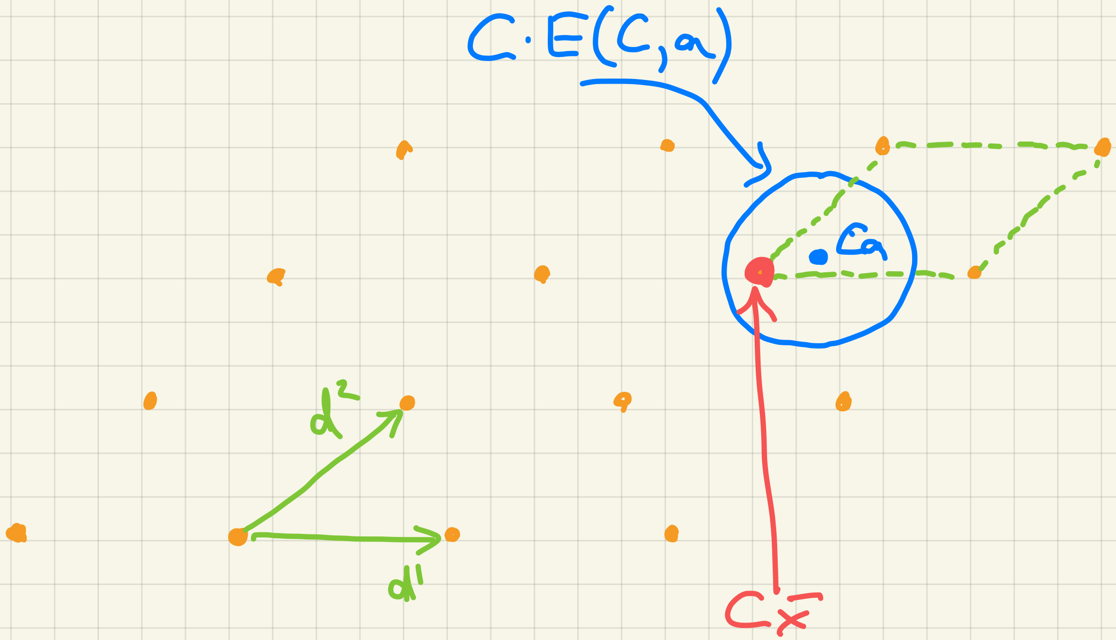
③ Berechne $\lambda = Ua$ und $\overline{x} := U^{-1} \cdot \lfloor \lambda \rceil$;

falls $\overline{x} \in E(C,a)$: Ausgabe $\overline{x}$ (stop)

sonst Ausgabe:

$$\frac{1}{\|g^n\|^2} (g^n)^T \cdot C^{-1}$$

(wobei $[g^1, \dots, g^n]$ die Gram-Schmidt Orthogonalisierung von $D$ sei)




$\Lambda(C)$

$x \longmapsto Cx$

$\mathbb{Z}^n \longrightarrow \Lambda(C)$

$Ca = D\lambda$

<u>Satz 1.3:</u> Algorithmus E arbeitet korrekt und kann so implementiert werden, dass seine Laufzeit polynomial in $\langle C\rangle + \langle a\rangle$ beschränkt ist.

<u>Beweis:</u> Die Laufzeitaussage folgt unmittelbar aus Satz 1.1 und Satz 1.2.

Zum Nachweis der Korrektheit genügt es, zu zeigen:

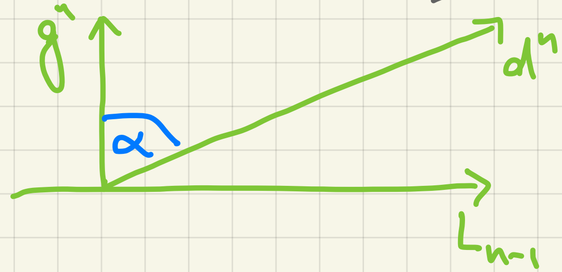
a) $d \in \mathbb{Z}^n \setminus \{0\}$

b) Falls $\bar{x} \notin E(C,a)$, so ist

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

Zu a):

$$d = \frac{1}{\|g^n\|^2}(g^n)^T C = \underbrace{\boxed{\frac{1}{\|g^n\|^2}(g^n)^T D}}_{= e_n^T} U \in \mathbb{Z}^n \quad [U \in \mathbb{Z}^{n \times n}]$$




$$d \neq 0, \text{ da } C \text{ regulär}, \ g^n \neq 0$$

$$\langle d^n, g^n \rangle = \cancel{\|d^n\|} \cdot \|g^n\| \cdot \underbrace{\cos(\alpha)}_{\frac{\|g^n\|}{\cancel{\|d^n\|}}}$$

$$= \|g^n\|^2$$

Zu b):

$$\max/\min \left\{ \langle d, x \rangle : \underbrace{x \in E(C,a)}_{\Leftrightarrow \ \|C(x-a)\| \leq 1} \right\}$$

$$= \max/\min \left\{ \langle d, C^{-1}y + a \rangle : \|y\| \leq 1 \right\}$$

$$= \langle d, a \rangle + \max/\min \left\{ \underbrace{\langle d, C^{-1}y \rangle}_{(d^T C^{-1})y} : \|y\| \leq 1 \right\} = \langle d, a \rangle +/- \|d^T C^{-1}\|$$

Also $w_d(E(C,a)) \leq 2\|d^T C^{-1}\| = 2 \cdot \frac{1}{\|g^n\|^2} \cdot \|g^n\| = \frac{2}{\|g^n\|} \qquad (*)$

$$\bullet\ \bar{x} \notin E(C,a) \Rightarrow 1 < \|C(\bar{x}-a)\| = \|C(U^{-1}\lfloor\lambda\rceil - U^{-1}\lambda\|$$

$$= \|CU^{-1}(\lfloor\lambda\rceil - \lambda)\|$$

$$= \|D(\lfloor\lambda\rceil - \lambda)\|$$

$$= \Big\|\sum_{j=1}^{n} d^i \underbrace{(\lfloor\lambda_i\rceil - \lambda_i)}_{\in[0,\frac{1}{2}]}\Big\|$$

$$\leq \sum_{j=1}^{n} \frac{1}{2} \underbrace{\|d^i\|}_{\leq \|d^n\|}$$

$$\leq \frac{n}{2}\|d^n\| \qquad (**)$$

$$\bullet\ 2^{\frac{n(n-1)}{4}} \geq OD(D) = \prod_{j=1}^{n} \underbrace{\frac{\|d^j\|}{\|g^j\|}}_{\geq 1} \geq \frac{\|d^n\|}{\|g^n\|} \Rightarrow \|g^n\| \geq 2^{-\frac{n(n-1)}{4}} \cdot \|d^n\|$$

Also $w_d(E(C,a)) \underset{(*)}{\leq} \frac{2}{\|g^n\|} \leq \frac{2}{2^{-\frac{n(n-1)}{4}} \cdot \|d^n\|} \underset{(**)}{\leq} \frac{2}{2^{-\frac{n(n-1)}{4}} \cdot \frac{2}{n}}$

$$= n \cdot 2^{\frac{n(n-1)}{4}}$$

$\boxed{\Xi}$

<u>Bemerkung</u>: Satz 1.3 impliziert für rationale Ellipsoide Kinchine's Flatness Theorem.

<u>Satz 1.4</u> [LÖWNER / JOHN]

Für jede volldimensionale, konvexe, kompakte Menge $K \subseteq \mathbb{R}^n$ gibt es ein Ellipsoid $E \subseteq \mathbb{R}^n$ mit Mittelpunkt $a \in \mathbb{R}^n$ und

$$\frac{1}{n}(E - a) + a \subseteq K \subseteq E .$$

**Satz 1.5** [GOFFIN]

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, $C \in \mathbb{Q}^{n \times n}$ und $a \in \mathbb{Q}^{n}$ berechnet mit

$$\frac{1}{n+1}\left(E(C,a)-a\right)+a \subseteq P^{\leq}(A,b) \subseteq E(C,a).$$