GDO-04 21.10.19

Beweis zu Satz 1.1

zu (i):

- $\frac{3}{4}\|g^{j-1}\|_2^2 \le \|g^j + \mu_{j-1,j}\, g^{j-1}\|_2^2 \overset{\text{Gauß}}{=} \|g^j\|_2^2 + \underbrace{\mu_{j-1,j}^2}_{\le 1/4}\|g^{j-1}\|_2^2$

$$\Rightarrow \|g^{j-1}\|_2^2 \le 2\|g^j\|_2^2$$

$$\Rightarrow \|g^k\|_2^2 \le 2^{j-k}\|g^j\|_2^2 \qquad \forall\, k = 1,\dots,j \qquad (*)$$

- $\|b_j\|_2^2 = \|g^j + \sum_{k=1}^{j-1} \mu_{kj}\, g^k\|_2^2 \overset{\text{Gauß}}{=} \|g^j\|_2^2 + \sum_{k=1}^{j-1} \underbrace{\mu_{kj}^2}_{\le 1/4}\underbrace{\|g^k\|_2^2}_{\le 2^{j-k}\|g^j\|_2^2}$

$$\le \Big(1 + \sum_{k=1}^{j-1} 2^{j-k-2}\Big)\|g^j\|_2^2 \le 2^{j-1}\|g^j\|_2^2$$

$1 + \frac{1}{2} + 1 + 2 + \dots + 2^{j-3} = 2^{j-2} + \frac{1}{2}$

zu (ii):

$$\Theta(B) = \frac{\|b^1\|_2 \cdots \|b^n\|_2}{\det \Lambda} \leq \prod_{j=1}^{n} 2^{(j-1)/2} = 2^{\frac{1}{2}\sum_{j=1}^{n} j-1} = 2^{\frac{n(n-1)}{4}}$$

$\det \Lambda = \|g^1\| \cdots \|g^n\|$ (wegen $B = G \cdot R$)

$\frac{\|b^j\|_2}{\|g^j\|_2} \overset{(i)}{\leq} \sqrt{2^{j-1}} = 2^{(j-1)/2}$ ∎

Der Reduktionsalgorithmus von Lovász

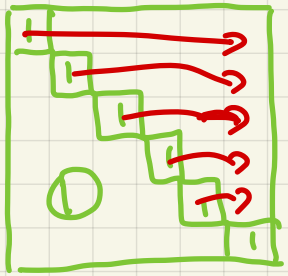
Eingabe: $B \in \mathbb{Q}^{n \times n}$ regulär

Ausgabe: Reduzierte Gitterbasis von $\Lambda(B)$.

① Bestimme die Gram-Schmidt Orthogonalisierung $G = [g^1, \ldots, g^n]$ von B und $R \in \mathbb{Q}^{n \times n}$ mit $B = GR$.

② Falls B reduziert ist, gib B aus und STOP.

③ Bestimme eine unimodulare obere Dreiecksmatrix $U \in \mathbb{Z}^{n \times n}$ mit Einsen auf der Hauptdiagonalen, so dass $\tilde{R} := R \cdot U = (\tilde{\mu}_{kj})$ eine obere Dreiecksmatrix ist mit $\tilde{\mu}_{jj} = 1 \; \forall j$ und $|\tilde{\mu}_{kj}| \leq \frac{1}{2} \; \forall 1 \leq k < j \leq n$



Sehe $\tilde{B} := B \cdot U = [\tilde{b}^1, \dots, \tilde{b}^n]$.

$\tilde{B} - G = BU - G$
$= GRU - G$
$= G(\underbrace{RU - I}_{\text{ohne } \Delta, \text{ Diag} = 0})$

Es gelten:

- $\Lambda(\tilde{B}) = \Lambda(B)$ [U unimodular]
- G ist die GS-Orthogonalisierung von $\tilde{B}$

alternativ

$$\left[\tilde{b}^j - g^j = b^j + \sum_{k=1}^{j-1} u_{kj} \cdot b^k - g^j = \underbrace{b^j - g^j}_{\in L_{j-1}} + \underbrace{\sum_{k=1}^{j-1} u_{kj} b^k}_{\in L_{j-1}}\right.$$

(U ohne Diagonalen, $u_{jj} = 1$)

$$\left. \in \lin\{g^1, \dots, g^{j-1}\} \; (= L_{j-1})\right]$$

- $\tilde{B} = B \cdot U = GRU = G\tilde{R}$

④ Falls für ein $j \in \{2, \dots, n\}$ $\|g^j + \tilde{\mu}_{j-1,j} g^{j-1}\|_2^2 < \frac{3}{4}\|g^{j-1}\|_2^2$ ist,
so vertausche in $\tilde{B}$ $\tilde{b}^{j-1}$ und $\tilde{b}^j$, nenne die neue Basis B.

⑤ Gehe zu Schritt ②.

Zu (5): Das geht, indem man eine geeignete Folge von Operationen der Art "addiere ein ganzzahliges Vielfaches einer Spalte zu einer weiter rechts stehenden Spalte" durchführt; jede solche Operation entspricht der Multiplikation (von rechts) mit einer Matrix vom Typ

$$\begin{bmatrix} 1 & & & & \\ & 1 & \lambda & & \\ & & 1 & & \\ & & & 1 & \\ & & & & \ddots \end{bmatrix}.$$

Satz 8.2: Lovász' Reduktionsalgorithmus terminiert nach polynomial in $\langle B \rangle$ vielen Schritten.

Beweis: • Wir können annehmen, dass die Eingabe-Gitterbasis ganzzahlig ist (Skalieren mit Hauptnenner vorher, Rückskalieren hinterher), und dann alle während des Algorithmus erzeugten Gitterbasen ganzzahlig sind.

- Für $A \in \mathbb{Z}^{n \times n}$ regulär & für $j \in [n]$

$$V_j(A) := \left| \det\left(A_{*[j]}^T \cdot A_{*[j]} \right) \right| \in \mathbb{N}$$

(Quadrat des j-dimensionalen Volumens der von den ersten j Spalten von A aufgespannten Parallelepipeds.); ist $G = [g^1, \dots, g^n]$ die Gram-Schmidt Orthogonalisierung von A, so ist

$$V_j(A) = V_j(G) = \|g^1\|_2^2 \cdot \dots \cdot \|g^j\|_2^2 \qquad (**)$$

Sei

$$\Phi(A) := \prod_{j=1}^{n} V_j(A) \; .$$