Gitter und Kryptographie

Blatt 9, 17.06.2009, Abgabe Mittwoch, 24.06.2009

Aufgabe 1. Sind die Gitter $\mathcal{L}(B)$ mit Gram–Matrizen

$$B^tB = \begin{bmatrix} 2 & 1 & & \\ 1 & 2 & 1 & \\ & 1 & 2 & 1 \\ & & 1 & 2 \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{bmatrix}$$

kritisch? Berechne $R = \mathrm{GNF}(B)$.

Def. Die Basis $B = \mathrm{QR} \in \mathbb{R}^{m\times n}, n = hk$, ist *primal–dual*$^+$ wenn

1. die Blöcke R_ℓ von R HKZ–Basen sind für $\ell = 1, \ldots, h$,

2. $\bar r_{k\ell+1,k\ell+1} \le (1+\varepsilon) r_{k\ell+1,k\ell+1}$ für $\ell = 1, \ldots, h-1$, dabei bezeichne $\bar r_{k\ell+1,k+1} = \max_T r'_{k\ell+1,k\ell+1}$ von $[r'_{i,j}]_{k\ell-k+1<i,j\le k\ell+1} := \mathrm{GNF}([r_{i,j}]_{k\ell-k+1<i,j\le k\ell+1}T)$ über alle $T \in \mathrm{GL}_k(\mathbb{Z})$.

Aufgabe 2. Zeige dass für jede primal–duale$^+$ Basis gilt

$$\mathcal{D}_\ell^{1/k} \le \big((1+\varepsilon)\gamma_k\big)^{\frac{2k}{k-1}} \mathcal{D}_{\ell+1}^{1/k} \qquad \text{für } \ell = 1, \ldots, h-1\ .$$

Damit wird der Wert $\alpha\gamma_k^2$ in den Schranken für primal–duale Basen ersetzt durch $\big((1+\varepsilon)\gamma_k\big)^{\frac{2k}{k-1}}$. $\mathcal{D}_\ell$ bezeichnet $\det R_\ell^2$.

Aufgabe 3. Zeige dass für jede primal–duale$^+$ Basis gilt

1. $\|\mathbf{b}_1\|^2 \le \big((1+\varepsilon)\gamma_k\big)^{\frac{n-1}{k-1}} (\det \mathcal{L})^{2/n}$,

2. $\|\mathbf{b}_1\| \le \big((1+\varepsilon)\gamma_k\big)^{\frac{n-k}{k-1}} \lambda_1$.

Hinweis: Benutze die Ungleichung von Aufgabe 2.