Prof. C. P. Schnorr Sommersemester 2016

Gitter und Kryptographie

Blatt 6, 20.05.2016, Abgabe 27.06.2016

Definition. Das *duale* (polare oder reziproke) Gitter $\mathcal{L}^*$ zum Gitter $\mathcal{L}$ ist

$$\mathcal{L}^* = \{\mathbf{x} \in \text{span}(\mathcal{L}) \mid \langle \mathbf{x}, \mathbf{b}\rangle \in \mathbb{Z} \text{ für alle } \mathbf{b} \in \mathcal{L}\}.$$

Sei $\mathbf{R}_8 = [\mathbf{r}_1, ..., \mathbf{r}_8] \in \mathbb{R}^{8\times 8}$ die GNF (Skript Seite 21).

Aufgabe 1. Zeige

1. $\mathcal{L} = \mathcal{L}^*$ für $\mathcal{L} = \mathcal{L}(\mathbf{R}_8)$.
2. Es gibt keine Gram–Matrix $\mathbf{R}_9^t\mathbf{R}_9$ mit derselben Form wie $\mathbf{R}_i^t\mathbf{R}_i$ für $i = 1, \ldots, 8$ wegen $\mathcal{L}(\mathbf{R}_8) = \mathcal{L}(\mathbf{R}_8)^*$.

Aufgabe 2. Erweitere $\mathbf{R}_8 = [\mathbf{r}_1, ..., \mathbf{r}_8]$ zur GNF $\mathbf{R}_{10} = [\mathbf{r}_1, ..., \mathbf{r}_8, \mathbf{r}_9, \mathbf{r}_{10}]$
$\mathbf{r}_9 = (0,0,0,0,1,0,0,0,1,0)^t$, $\mathbf{r}_{10} = (0,0,0,0,1,0,0,0,\frac{1}{2}, \sqrt{3/4})^t$,

1. Zeige $\lambda_1^2(\mathcal{L}(\mathbf{R}_{10})) = 2$ (mit Lemma 2.2.3 und $\mathcal{L}(\mathbf{R}_8) = \mathcal{L}(\mathbf{R}_8)^*$)
2. Berechne $\gamma(\mathcal{L}(\mathbf{R}_{10}))$

Aufgabe 3. Vergleiche und bestätige die Mazo, Odlyzko Schranke

$K_n =_{def} |\{\mathbf{x} \in \mathbb{Z}^n + (\frac{1}{2}, \cdots, \frac{1}{2}) \cdot \{0,1\} \ : \ \|\mathbf{x}\| \le \frac{1}{2}\sqrt{n}\}| \le 2^{c_0' n}, \ c_0' = 1,0629$

1. Volumenheuristik: Berechne c_0'' mit $\frac{1}{2}K_n \le V_n(\frac{1}{2}\sqrt{n})^n \approx 2^{c_0'' n} \le K_n$.

2. Zeige $K_n \ge 2^n + \frac{n!}{(n-n/4)!\ (n/4)!} \cdot 2^{n/4} \ge 2^{1.058\, n}$.

Punktzahl 6 pro Aufgabe

$$\mathbf{R}_{10} = \frac{1}{\sqrt{2}} \begin{bmatrix} 2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \sqrt{3} & \frac{1}{\sqrt{3}} & \frac{2}{\sqrt{3}} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{\frac{8}{3}} & \sqrt{\frac{2}{3}} & \sqrt{\frac{3}{2}} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{2} & \frac{1}{\sqrt{2}} & \sqrt{2} & 0 & 0 & 0 & \sqrt{2} \\ 0 & 0 & 0 & 0 & \sqrt{2} & \frac{1}{\sqrt{2}} & \sqrt{2} & 0 & \sqrt{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & \sqrt{\frac{3}{2}} & \sqrt{\frac{2}{3}} & \sqrt{\frac{8}{3}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{2}{\sqrt{3}} & \frac{1}{\sqrt{3}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \sqrt{2} & \sqrt{\frac{1}{2}} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \sqrt{\frac{3}{2}} \end{bmatrix}$$