Prof. C. P. Schnorr Sommersemester 2016

Gitter und Kryptographie

Blatt 7, 27.05.2016, Abgabe 03.06.2016

Aufgabe 1: Sei $\mathcal{L}_{\mathbf{a}} = \mathcal{L}(\mathbf{B}_{\mathbf{a}})$, $\mathbf{a} \in [1, A]^n$ das Gitter von Kor. 5.4.1. Zeige: Nach Randomisieren von a_j zu $a_j^* \in_R [1, A]$, $A > 2^{n/0{,}9408}$ und $\mathcal{L}_{\mathbf{a}}$ zu $\mathcal{L}_{\mathbf{a}^*}$ gilt: Mit Ws $1 - o(1)$ bzgl. a_j^* gibt es in $\mathcal{L}_{\mathbf{a}^*}$ keinen Vektor $\mathbf{b} = \sum_{i \neq j} y_i \mathbf{b}_i + y_j \mathbf{b}_j^*$ mit $||\mathbf{b}||^2 \leq n/4$ mit $y_j \neq 0$. *Hinweis:* Beweis zu Kor. 5.4.1 und Satz 5.3.1.

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

Aufgabe 2. Zeige mit Le. 2.2.3 dass $\lambda_1^2 \in \mathbb{N}$ für $\mathcal{L}(\mathbf{R'}_{10})$. Beweise $\lambda_1^2 = 1$.

Aufgabe 3: Sei $\mathbf{B} = \begin{bmatrix} \mathbf{I}_n \\ \mathbf{a} \end{bmatrix} \in \mathbb{R}^{(n+1) \times n}$ mit $\mathbf{a} = (a_1, \ldots, a_n)$

Zeige: $\det \mathbf{B}^t\mathbf{B} = 1 + \sum_{i=1}^n a_i^2$.

Hinweis: $\mathbf{B}^t\mathbf{B}$ hat die Eigenwerte 1 $(n-1)$–mal sowie $1 + \sum_{i=1}^n a_i^2$ einmal zu Eigenvektoren $(-a_2, a_1, 0, \ldots, 0)^t, \ldots, (-a_n, \ldots, a_1)^t$, $(\mathrm{a}_1, a_2, \ldots, a_{n-1}, a_n)^t \in \mathbb{R}^n$. **Punktzahl 6 pro Aufgabe**