Prof. C. P. Schnorr Sommersemester 2016

Gitter und Kryptographie

Blatt 5, 13.05.2016, Abgabe 20.05.2016

Aufgabe 1. Sei $\mathbf{R}_8$ (Skript, Seite 23) die GNF des Gitters Λ_8 und $\mathbf{y} = (0,0,0,1,0,0,0,0)^t$. Zeige: $\min\{\|\mathbf{y}-\mathbf{x}\|, \mathbf{x} \in \mathcal{L}(\mathbf{R}_8)\} = 1$.

Hinweis: $[\mathbf{R}_8, \mathbf{y}]^t[\mathbf{R}_8, \mathbf{y}] \in \frac{1}{2}\mathbb{Z}^{9\times 9}$, $\|\mathbf{y}\| = 1$. Argumentiere wie in Lemma 2.2.3 des Skripts, benutze nicht dass $\lambda_1^2 = 2$ für $\mathcal{L}(\mathbf{R}_9)$.

Aufgabe 2. Zeige für die folgende Basis: 1. $\|\mathbf{b}_1\|^2 = \alpha^{\frac{n-1}{2}} \det(\mathcal{L})^{2/n}$.

2. Die Basis ist LLL-reduziert für δ und $\alpha = (\delta - \frac{1}{4})^{-1}$:

$$[\mathbf{b}_1, \ldots, \mathbf{b}_n] = \begin{bmatrix} 1 & 1/2 & 0 & \cdots & \cdots & 0 \\ 0 & \rho & \rho/2 & \cdots & \cdots & \vdots \\ \vdots & \ddots & \rho^2 & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ \vdots & & & \ddots & \rho^{n-2} & \rho^{n-2}/2 \\ 0 & \cdots & \cdots & \cdots & 0 & \rho^{n-1} \end{bmatrix} \in \mathbb{R}^{n\times n},\ \rho := 1/\sqrt{\alpha}.$$

(Damit ist die Schranke für $\|\mathbf{b}_1\|^2$ von Korollar 4.1.5 (1) scharf.)

Aufgabe 3. (Worst Case Gitterbasis zur Gauss-Reduktion $\| \ \| = \| \ \|_2$)

Sei $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{R}^n$ reduzierte Basis, $\mu_{2,1} \geq 0$, $[\mathbf{b}_k, \mathbf{b}_{k+1}] := [\mathbf{b}_1, \mathbf{b}_2] \begin{bmatrix} 0 & 1 \\ & \\ 1 & 2 \end{bmatrix}^{k-1}$.

Zeige für $k = 2, 3, \ldots$: 1. $\lceil \frac{\langle \mathbf{b}_{k+1}, \mathbf{b}_k \rangle}{\langle \mathbf{b}_k, \mathbf{b}_k \rangle} \rfloor = 2$, $\|\mathbf{b}_k\| \leq \|\mathbf{b}_{k+1}\|$.

2. Die Basis $\mathbf{b}_k, \mathbf{b}_{k+1}$ ist wohlgeordnet, d.h. $\|\mathbf{b}_k\| \leq \|\mathbf{b}_k - \mathbf{b}_{k+1}\| \leq \|\mathbf{b}_{k+1}\|$.
und wird in einer Runde der Gauss-Reduktion in $\mathbf{b}_{k-1}, \mathbf{b}_k$ transformiert.

Hinweis : Satz 3.2.1 im Skript beweist, dass $[\mathbf{b}_k, \mathbf{b}_{k+1}]$, *minimale* k-te Vorgängerbasis zu $\mathbf{b}_1, \mathbf{b}_2$ ist.

Punktzahl für Aufgabe 1, 2, 3 : 5, 5, 8

Lemma 2.2.3 Sei $\mathbf{B} = [\mathbf{b}_1, ..., \mathbf{b}_n]$ Basis von $\mathcal{L}$, $\mathbf{B}^t\mathbf{B} \in k^{n\times n}$, $k > 0$ und ${\mathbf{b}_1}^2, \cdots, {\mathbf{b}_n}^2 \in 2k\,\mathbb{N}$. Sei ferner $\widetilde{\mathbf{b}} \in \mathcal{L}$, $\widetilde{\mathbf{b}} \notin \mathcal{L}$, $\mathbf{B}^t\,\widetilde{\mathbf{b}} \in \frac{k}{2}^n$ und $||\widetilde{\mathbf{b}}||^2 \in k\,\mathbb{N}$. Dann gilt

1. $\lambda_1^2(\mathcal{L}(\mathbf{B})) \in 2k\,\mathbb{N}$ 2. $||\mathcal{L} - \widetilde{\mathbf{b}}||^2 \geq k$.

Beweis. Offenbar gilt für $\mathbf{b} = \sum_{i=1}^n t_i\mathbf{b}_i \in \mathcal{L}$, $\mathbf{b} \neq \mathbf{0}$, $t_i \in$ dass

$$||\mathbf{b}||^2 = \mathbf{b}\mathbf{b} = \textstyle\sum_{1\leq i,j\leq n} t_it_j\mathbf{b}_i\mathbf{b}_j = \sum_{i=1}^n t_i^2||\mathbf{b}_i||^2 + 2\sum_{j<i} t_it_j\mathbf{b}_i\mathbf{b}_j \in 2k\,.$$

Somit gilt 1. Zum Beweis von 2. setze $\mathbf{b}_{n+1} := \widetilde{\mathbf{b}}$. Dann gilt

$$||\mathbf{b} - \widetilde{\mathbf{b}}||^2 = \mathbf{b} - \widetilde{\mathbf{b}}\mathbf{b} - \widetilde{\mathbf{b}} = \textstyle\sum_{i=1}^{n+1} t_i^2\|\mathbf{b}_i\|^2 + 2\sum_{1\leq i<j\leq n+1} t_it_j\mathbf{b}_i\mathbf{b}_j \in k$$

und somit $||\mathcal{L} - \widetilde{\mathbf{b}}||^2 \geq k$. □

Fakt. $\lambda_1^2 = 2$ für die Matrix $\mathbf{R}_n$ der ersten $n \leq 8$ Zeilen und Spalten von $\mathbf{R}_8$.

Beweis. Für $\mathbf{R}_8$ gilt $\mathbf{R}_8^t\mathbf{R}_8 \in \mathbb{Z}^{n\times n}$, $||\mathbf{r}_1||^2, ..., ||\mathbf{r}_n||^2 = 2$. Nach Lemma 0.0.1 , Teil 1 folgt für $k = 1$ dass $\lambda_1^2 = 2$ für $\mathcal{L}(\mathbf{R}_n)$, für $n = 1, ..., 8$. □

Wir erweitern die GNF $\mathbf{R}_8$ wie folgt zu $\mathbf{R}_{10}$. Es bezeichnet nun $\mathbf{R}_n = [\mathbf{r}_1, ..., \mathbf{r}_n]$ die Untermatrix der ersten n Zeilen und Spalten von $\mathbf{R}_{10}$.

$$\mathbf{R}_{10} := \sqrt{2}\begin{bmatrix} 1 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \sqrt{\frac{3}{4}} & \frac{1}{\sqrt{12}} & \sqrt{\frac{1}{3}} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{\frac{2}{3}} & \sqrt{\frac{1}{6}} & \sqrt{\frac{3}{8}} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{2}} & 0 & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{8}} & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 0 & 0 & \sqrt{\frac{3}{8}} & \frac{1}{\sqrt{6}} & \sqrt{\frac{2}{3}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{12}} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{8}} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \sqrt{\frac{3}{8}} \end{bmatrix}, \quad \det\mathbf{R}_{10} = \sqrt{3}/2.$$

Korollar 2.2.4 Für $\mathcal{L}(\mathbf{R}_9)$ und $\mathcal{L}(\mathbf{R}_{10})$ gilt $\lambda_1^2 = 2$.

Beweis. $\lambda_1^2(\mathcal{L}(\mathbf{R}_9)) = 2$: Der Fakt zeigt $\lambda_1^2(\mathcal{L}(\mathbf{R}_8)) = 2$. Wegen $\mathbf{R}_9^t\mathbf{R}_9 \in \frac{1}{2}\mathbb{Z}^9$ gilt nach Lemma 0.0.1 Teil 1, mit $k = \frac{1}{2}$ dass $\lambda_1^2(\mathcal{L}(\mathbf{R}_9)) \in k\,\mathbb{N}$. Â Es ist nur noch zu zeigen, dass für alle $\mathbf{r} = \sum_{i=1}^{9} t_i\mathbf{r}_i \in \mathcal{L}(\mathbf{R}_9)$ mit $t_9 \neq 0$ gilt dass $||\mathbf{r}||^2 > 1$. Für $|t_9| \geq 2$ folgt dies aus $||\mathbf{r}||^2 \geq t_9^2\,||\pi_9(\mathbf{r}_9)||^2 \geq 4$. Für $t_9 = 1$ wenden wir Lemma 2.2.3 Teil 1 an auf $\mathbf{B} = \mathbf{R}_8$ und $\widetilde{\mathbf{b}} = \widetilde{\mathbf{r}} := \mathbf{r}_9 - \pi_9(\mathbf{r}_9) = (0,0,0,0,1,0,0,0)^t \in \mathcal{L}(\mathbf{R}_8)$. Es gilt $\mathbf{R}_8^t\,\widetilde{\mathbf{r}} \in \frac{1}{2}^8$, $\mathbf{r}_6\widetilde{\mathbf{r}} = \frac{1}{2}$, $||\widetilde{\mathbf{r}}||^2 = 1$. Lemma 0.0.1, Teil 2 zeigt für $k = 1$ dass $||\mathcal{L}(\mathbf{R}_8) - \widetilde{\mathbf{r}}||^2 \geq 1$ und somit folgt $||\mathbf{r}||^2 \geq ||\mathcal{L}(\mathbf{R}_8) - \widetilde{\mathbf{r}}||^2 + ||\pi_9(\mathbf{r}_9)||^2 \geq 2$.