Prof. C. P. Schnorr Wintersemester 2005/06

Gitter und Kryptographie

Blatt 10, 13.01.2006, Abgabe 20.01.2006

Aufgabe 1. Formuliere den LLL-Algorithmus zu gegebener Gram-Matrix $B^tB \in \mathbf{Z}^{n\times n}$

`EINGABE` $B^tB \in \mathbf{Z}^{n\times n}$, $1/4 \le \delta < 1$

`AUSGABE` $T \in \mathrm{GL}_n(\mathbf{Z})$, so dass BT LLL-reduziert ist.

Alle arithmetischen Schritte insbesondere die zur Berechnung der $\mu_{k,j}, \|\hat{\mathbf{b}}_k\|^2$ sollen auf $\mathbf{Z}$ operieren.

Aufgabe 2. LLL-reduziere $R_8 = \mathrm{GNF}(\Lambda_8) \in \mathbf{R}^{8\times 8}$ und bestimme $\bar{R}_8^t\bar{R}_8$ für das LLL-reduzierte $\bar{R}_8$.

$$\text{Sei } R_2 = \begin{bmatrix} \sqrt{2} & 1/\sqrt{2} \\ 0 & \sqrt{3/2} \end{bmatrix},\ V = \begin{bmatrix} 1/\sqrt{2} & 0 \\ +1/\sqrt{6} & \sqrt{2/3} \end{bmatrix}$$

$$R_4 = \begin{bmatrix} R_2 & V \\ O & \sqrt{\frac{2}{3}}R_2 \end{bmatrix},\ A = \begin{bmatrix} O & O \\ \sqrt{\frac{3}{2}}V & O \end{bmatrix},\ \bar{R}_4 = \begin{bmatrix} \frac{1}{\sqrt{2}}R_2 & \sqrt{2}V \\ O & \frac{1}{\sqrt{3}}R_2 \end{bmatrix}$$

$$R_8 = \begin{bmatrix} R_4 & A \\ O & \bar{R}_4 \end{bmatrix},\ R_{12} = \begin{bmatrix} R_4 & A & A \\ O & \bar{R}_4 & O \\ O & O & \bar{R}_4 \end{bmatrix}.$$

Aufgabe 3. Zeige für die obere linke Untermatrix $R_n \subset R_{12}$ für $n = 9, \ldots, 12$: $(\det R_n)^2 2^n = \lambda_n$ für die λ_n in table 6.1 von [CoSL88].

Aufgabe 4. Zeige $\lambda_1^2(\mathcal{L}(R_{12})) = 2$.

Hinweis: Für die Spalten $\mathbf{y} \neq \mathbf{0}$ von $\begin{bmatrix} A \\ O \end{bmatrix}$ gilt $\|\mathbf{y} - \mathcal{L}(R_8)\| = 1$. Ferner gilt $R_n^tR_n \in \frac{1}{2}\mathbf{Z}^{n\times n}$. Schliesse daraus $\lambda_1^2(\mathcal{L}(R_9)) = \lambda_1^2(\mathcal{L}(R_{10})) = 2$ wie in Aufgabe 1, Blatt 9. Folgere $\lambda_1^2(\mathcal{L}(R_{10})) = \lambda_1^2(\mathcal{L}(R_{11})) = 2$, weil die Zeilen/Spalten 11, 12 von $R_{12}^tR_{12}$ ganzzahlig sind.