Prof. C. P. Schnorr Wintersemester 2005/06

Gitter und Kryptographie

Blatt 11, 20.01.2006, Abgabe 27.01.2006

Aufgabe 1. Sei $R = [r_{i,j}]_{1\le i,j\le n} = [\mathbf{r}_1, \ldots, \mathbf{r}_n] \in \mathbf{R}^{n\times n}$ LLL–reduzierte GNF zu $\delta, 0 < \delta < 1/4$ und $\alpha := (1/4-\delta)^{-1}$. Zu gegebenem $\mathbf{y} = \sum_{i=1}^n s_i\mathbf{r}_i \in \mathbf{R}^n$ kann man leicht ein $\mathbf{z} = \sum_{i=1}^n t_i\mathbf{r}_i \in \mathcal{L}(R)$ bestimmen (wie?) so, dass $|s_i - t_i| \le 1/2$ für $i = 1, \ldots, n$. Zeige : $\|\mathbf{y}-\mathbf{z}\| \le (\sum_{i=0}^{n-1} \alpha^i)\, \|\mathbf{y} - \mathcal{L}(R)\|$.

Hinweis: Sei $z' = \sum_{i=1}^n t'_i\mathbf{r}_i \in \mathcal{L}(R)$ mit $\|\mathbf{y}-\mathbf{z}'\| = \|\mathbf{y}-\mathcal{L}(R)\|$. Falls $\mathbf{z} \ne \mathbf{z}'$ gilt für das grösste i mit $t_i \ne t'_i$, dass $|t'_i - s_i| \ge 1/2$.

Aufgabe 2. Sei p Primzahl, $p = 1 \bmod 8$.

Zeige: Es gibt $x, y \in \mathbf{Z}$ mit $x^2 + 2y^2 = p$.

Löse mit Gitterreduktion: $x^2 + 2y^2 = 281$ mit $x, y \in \mathbf{Z}$.

Hinweis: Ersetze in Aufgabe 1, Blatt 5 $\sqrt{-1} \bmod p$ durch $\sqrt{-2} \bmod p$.

Aufgabe 3. Zeige, dass R_3 lokal extrem ist.

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

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