Prof. C. P. Schnorr Sommersemester 2014

Gitter und Kryptographie

Blatt 10, 25.06.2014, Abgabe 02.07.2014

Aufgabe 1. Sind die Gitter $\mathcal{L}(\mathbf{B})$ mit Gram–Matrizen

$$\mathbf{B}^t\mathbf{B} = \begin{bmatrix} 2 & 1 & & \\ 1 & 2 & 1 & \\ & 1 & 2 & 1 \\ & & 1 & 2 \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{bmatrix}$$

kritisch (d.h. $\lambda_1^2 = \gamma_4 \det(\mathcal{L}(\mathbf{B}))^{2/4}$)? Berechne $\det(\mathbf{B}^t\mathbf{B})$.

Aufgabe 2. Zeige: Für jede k–reduzierte Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ gilt

$$\|\mathbf{b}_1\| \le \gamma_k^{\frac{n-1}{k-1}} M \quad \text{für} \quad M := \max(\|\widehat{\mathbf{b}}_{n-k+2}\|, \ldots, \|\widehat{\mathbf{b}}_n\|).$$

Hinweis: Beweis von Lemma 6.4.5 Skript.

Aufgabe 3. Folgere aus Aufgabe 2 dass

$$\|\mathbf{b}_1\| \le \gamma_k^{\frac{n-1}{k-1}} \lambda_1 \quad \text{für jede } k\text{–reduzierte Basis } \mathbf{b}_1, \ldots, \mathbf{b}_n.$$

Hinweis: Beweis von Korollar 6.4.6 Skript.

5 Punkte pro Aufgabe