

Gitter und Kryptographie

Blatt 5, 16.11.2007, Abgabe 23.11.2007

Def. Sei $R \in \mathbb{R}^{n \times n}$ GNF und $D_\sigma \in \mathbb{Z}^{n \times n}$ Diagonalmatrix mit Diagonale $(\sigma_1, \dots, \sigma_n) \in \{\pm 1\}^n$. Dann ist die quadratische Form f_A mit $A = R^t D_\sigma R \in \mathbb{R}^{n \times n}$ eine *LLL-Form* zu δ , $\frac{1}{4} < \delta \leq 1$, wenn R eine LLL-Basis zu δ ist.

Aufgabe 1. Modifiziere Alg. 3 zur LLL-Reduktion, so dass eine gegebene Form f_A , $A = A^t \in \mathbb{Z}^{n \times n}$ in eine LLL-Form $f_{T^t A T}$ transformiert wird. Wie werden die Vorzeichen $\sigma_1, \dots, \sigma_n$ und die GNF $R = (r_{i,j})$ berechnet und verändert?

Aufgabe 2. Sei $A = R^t D_\sigma R \in \mathbb{R}^{n \times n}$, R GNF und D_σ mit Diagonale $\sigma \in \{\pm 1\}^n$. Zeige:

1. Die Vertauschung von $\text{col}(k-1, A), \text{col}(k, A)$ und $\text{row}(k-1, A), \text{row}(k, A)$ lässt $\sigma_{k-1} + \sigma_k, \sigma_{k-1}\sigma_k, r_{k-1,k-1}r_{k,k}$ und $\sigma_i, r_{i,i}$ für $i \neq k, k-1$ unverändert.
2. Für $A' := T^t A T$ mit $T \in \text{GL}_n(\mathbb{Z})$ gilt $\sum_{i=1}^n \sigma_i = \sum_{i=1}^n \sigma'_i$, damit ist die 'Signatur' $\#\{i \mid \sigma_i = 1\}$ invariant gegen Äquivalenztransformationen T .

Aufgabe 3. Zeige:

1. Folgende Basis ist LLL-reduziert für δ und $\alpha = (\delta - \frac{1}{4})^{-1}$, $\rho := 1/\sqrt{\alpha}$:

$$(\mathbf{b}_1, \dots, \mathbf{b}_n) = \begin{pmatrix} 1 & 1/2 & 0 & \dots & \dots & 0 \\ 0 & \rho & \rho/2 & \dots & \dots & \vdots \\ \vdots & \ddots & \rho^2 & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ \vdots & & & \ddots & \rho^{n-2} & \rho^{n-2}/2 \\ 0 & \dots & \dots & \dots & 0 & \rho^{n-1} \end{pmatrix} \in \mathbb{R}^{n \times n}.$$

2. $\|\mathbf{b}_1\|^2 = \alpha^{\frac{n-1}{2}} \det(\mathcal{L})^{2/n}$.

(Damit ist die Schranke für $\|\mathbf{b}_1\|^2$ von Korollar 4.5 (1) scharf.)