Gitter und Kryptographie

Blatt 7, 09.12.2005, Abgabe 16.12.2005

$$\text{Sei } [B', \mathbf{y}] = \begin{bmatrix} 2 & & & 1 \\ & \ddots & O & \vdots \\ & O & 2 & \vdots \\ 2a_1 & \cdots & 2a_n & 2b \end{bmatrix} \in \mathbf{Z}^{(n+1)^2}.$$

$B = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbf{R}^{(n+2)\times(n+1)}$ entstehe aus $[B', \mathbf{y}]$ durch Zufügen der $n+2$-ten Zeile $(0, \ldots, 0, \sqrt{n})$.

Aufgabe 1. Zeige: $(B, \sqrt{2n}) \in \text{SVP} \Rightarrow (a_1, \ldots, a_n, b) \in$ Rucksack, sofern $\lambda_1(\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)) > \sqrt{2n}$.

Aufgabe 2. Zeige:
$(a_1, \ldots, a_n, b) \notin$ Rucksack $\Rightarrow \forall \mathbf{x} \in \mathbf{Z}^n$: $\|B'\mathbf{x} - \mathbf{y}\| \geq \sqrt{n+4}$.
Zeige konstruktiv: $\mathbf{x} \in \mathbf{Z}^n$ mit $\|B'\mathbf{x} - \mathbf{y}\| < \sqrt{n+4}$ liefert eine Rucksacklösung.

Aufgabe 3. Zeige: GAP-CVP$_{\sqrt{1+4/n}}$ ist NP-hart.
Hinweis: Benutze Aufgabe 2 und dass offenbar gilt:
$(a_1, \ldots, a_n, b) \in$ Rucksack $\Rightarrow \exists \mathbf{x} \in \mathbf{Z}^n : \|B'\mathbf{x} - \mathbf{y}\| \leq \sqrt{n}$.

Aufgabe 4. Sei $\| \ \|$ beliebige Norm mit Eichkörper K und $\mathcal{L}$ Gitter, $\dim(\mathcal{L}) = n$. Zeige :

$$\lambda_{1,\| \ \|}(\mathcal{L}) \leq 2\,\mathrm{vol}(K)^{-1/n}(\det \mathcal{L})^{1/n}.$$

Hinweis: Ersetze im Beweis von Satz 3.2.1: $V_n(\lambda_1/2)^n$ durch $\mathrm{vol}(K)(\lambda_1/2)^n$.