

**Gitter und Kryptographie**

Blatt 9, 14.12.2007, Abgabe 21.12.2007

$$\text{Sei } (B', \mathbf{y}) = \begin{pmatrix} 2 & & & 1 \\ & \ddots & O & \vdots \\ & O & 2 & 1 \\ Na_1 & \cdots & Na_n & Nb \end{pmatrix} \in \mathbb{Z}^{(n+1)^2}.$$

**Aufgabe 1.** Zeige für  $N \geq 2$ :

$$(a_1, \dots, a_n, b) \notin \text{Rucksack} \Rightarrow \forall \mathbf{x} \in \mathbb{Z}^n: \|B'\mathbf{x} - \mathbf{y}\| \geq \sqrt{n+4}.$$

Zeige konstruktiv:  $\mathbf{x} \in \mathbb{Z}^n$  mit  $\|B'\mathbf{x} - \mathbf{y}\| < \sqrt{n+4}$  liefert eine Rucksacklösung.

**Aufgabe 2.** Zeige: GAP-CVP $_{\sqrt{1+4/n}}$  ist NP-hart.*Hinweis:* Benutze Aufgabe 1 und dass offenbar gilt:

$$(a_1, \dots, a_n, b) \in \text{Rucksack} \Rightarrow \exists \mathbf{x} \in \mathbb{Z}^n: \|B'\mathbf{x} - \mathbf{y}\| \leq \sqrt{n}.$$

**Aufgabe 3.** Sei  $\|\cdot\|$  beliebige Norm mit Eichkörper  $K$  und  $\mathcal{L}$  Gitter,  $\dim(\mathcal{L}) = n$ . Zeige:  $\lambda_{1, \|\cdot\|}^n(\mathcal{L}) \leq 2^n \text{vol}(K)^{-1} \det \mathcal{L}$ .*Hinweis:* Ersetze im Beweis von Satz 3.2.1:  $V_n(\lambda_1/2)^n$  durch  $\text{vol}(K)(\lambda_1/2)^n$ .

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

**Aufgabe 4.** Zeige unter der Annahme  $\lambda_1(\mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_n)) > \sqrt{2n}$ :

$$\text{für } N \geq n: (B, \sqrt{2n}) \in \text{SVP} \Leftrightarrow (a_1, \dots, a_n, b) \in \text{Rucksack}.$$