Prof. C. P. Schnorr Sommersemester 2009

Blatt 8, 10.06.2009, Abgabe Mittwoch, 17.06.2009

Gitter und Kryptographie

$$\text{Setze} \qquad [B', \mathbf{y}] := \begin{bmatrix} 2 & & & & 1 \\ & \ddots & & & \vdots \\ & & \ddots & & \vdots \\ & & & 2 & 1 \\ Na_1 & \cdots & \cdots & Na_n & Nb \end{bmatrix} \in \mathbb{Z}^{(n+1)^2}.$$

Aufgabe 1: Zeige für $N \geq 3$:

$$(a_1, \ldots, a_n, b) \notin \text{ Rucksack } \Rightarrow \ \forall x \in \mathbb{Z}^n : B'\mathbf{x} - \mathbf{y}\| \geq \sqrt{n+8}\ .$$

Zeige konstruktiv: $\mathbf{x} \in \mathbb{Z}^n$ mit $\|B'\mathbf{x} - \mathbf{y}\| < \sqrt{n+8}$ liefert Rucksacklösung.

Aufgabe 2: Zeige GAP-CVP$_{\sqrt{1+8/n}}$ ist NP–hart.
Hinweis: Benutze Aufgabe 1 und dass offenbar gilt:

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

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

Aufgabe 3. Zeige für $N \geq n$:

$$(B, \sqrt{n+1}) \in \text{SVP} \Leftrightarrow (a_1, \ldots, a_n, b) \in \text{Rucksack},$$

sofern $\lambda_1(\mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_n)) > \sqrt{n+1}$.