Prof. C. P. Schnorr Wintersemester 2005/06

Gitter und Kryptographie

Blatt 6, 02.12.2005, Abgabe 09.12.2005

Def.: Die Vektoren $\mathbf{b}_1, \ldots, \mathbf{b}_{\bar{n}} \in \mathcal{L}$ heissen *paarweise reduziert*, wenn

1. $|\langle \mathbf{b}_i, \mathbf{b}_j \rangle| \|\mathbf{b}_i\|^{-2} \leq \frac{1}{2}$ für $1 \leq j < i \leq \bar{n}$
2. $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\| \leq \cdots \leq \|\mathbf{b}_{\bar{n}}\|$.

Aufgabe 1. Erweitere Alg. 1.4.2 (Skript) zur paarweise Reduktion von Basen $\mathbf{b}_1, \ldots, \mathbf{b}_n$ auf beliebige (möglicherweise linear abhängige) $\mathbf{b}_1, \ldots, \mathbf{b}_{\bar{n}} \in \mathcal{L}$.

Zeige: Jedes Gitter $\mathcal{L}$ hat eine paarweise reduzierte Basis.

Aufgabe 2. Zeige: der erweiterte Alg. 1.4.2. führt höchstens $\sum_{i=1}^{\bar{n}} \|\mathbf{b}_i\|^2/\varepsilon$ Reduktionsschritte $\mathbf{b}_i := \mathbf{b}_i - \lceil r \rfloor \mathbf{b}_j$ mit $|r| \geq \frac{1}{2} + \varepsilon$ aus.

Ist kein solcher Reduktionsschritt ausführbar, dann gilt

$$|\langle \mathbf{b}_i, \mathbf{b}_j \rangle| \ \|\mathbf{b}_j\|^{-2} \leq \tfrac{1}{2} + \varepsilon \text{ für } 1 \leq j < i \leq \bar{n}.$$

Aufgabe 3. Zeige: Es gibt paarweise reduzierte Basen $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3 \in \mathbf{R}^3$, so dass $\|\mathbf{b}_1\| / \|\mathbf{b}_1 - \mathbf{b}_2 + \mathbf{b}_3\|$ beliebig groß ist.

Hinweis: Wähle $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ so dass $\|\mathbf{b}_1\| = \|\mathbf{b}_2\| = \|\mathbf{b}_3\|$

$$\langle \mathbf{b}_1, \mathbf{b}_2 \rangle = \tfrac{1}{2} \approx \langle \mathbf{b}_2, \mathbf{b}_3 \rangle, \ \langle \mathbf{b}_1, \mathbf{b}_3 \rangle \approx -\tfrac{1}{2}.$$

Aufgabe 4. Zeige: Rucksack $\leq_{pol}$ $\mathrm{CVP}_{\|\ \|_\infty}$.

Damit ist $\mathrm{CVP}_{\|\ \|_\infty}$ NP–vollständig.