Prof. C. P. Schnorr Wintersemester 2005/06

Gitter und Kryptographie

Blatt 2, 4.11.2005, Abgabe 11.11.2005

Def. Eine Basis $\mathbf{a}, \mathbf{b} \in \mathbf{R}^m$ heisst *reduziert* zur Norm $\| \|$, wenn $\|\mathbf{a}\|, \|\mathbf{b}\| \leq \|\mathbf{a} \pm \mathbf{b}\|$. Die Basis $\mathbf{a}, \mathbf{b}$ heisst *wohlgeordnet*, wenn $\|\mathbf{a}\| \leq \|\mathbf{a} - \mathbf{b}\| < \|\mathbf{b}\|$.

Aufgabe 1. Zeige, eine beliebige Basis $\mathbf{a}, \mathbf{b} \in \mathbf{R}^n$ führt zu einer Basis $\mathbf{a}, \mathbf{b}$ derart, dass $\|\mathbf{a}\| \leq \|\mathbf{b}\|$, $\|\mathbf{a} - \mathbf{b}\| \leq \|\mathbf{a} + \mathbf{b}\|$, indem man gegebenenfalls $\mathbf{a}, \mathbf{b}$ vertauscht und $\mathbf{b} := \pm\mathbf{b}$ setzt. Zeige, dass die so transformierte Basis entweder reduziert oder wohlgeordnet ist.

Aufgabe 2. 1. Beweise Theorem 1.2 [MG02]

(Existenz von Gittervektoren $\mathbf{v}_1, \ldots, \mathbf{v}_n$ mit $\lambda_i = \|\mathbf{v}_i\|$ für $i = 1, \ldots, n$).

2. Erläutere die Gitter Seite 126 [MG02], für die $\mathbf{v}_1, \ldots, \mathbf{v}_n$ keine Basis ist. Weshalb nicht?

Hinweis: [MG02] Micciancio, Goldwasser: Complexity of lattice problems: a cryptographic perspective. Kluwer (2002).

Aufgabe 3. Verifiziere den Beweis von Theorem 2.2 [MG02] und behandele die Fälle, in denen $r \geq s \geq 0$ nicht gilt.

Aufgabe 4. Betrachte zur MV-Identifikation die stat. Differenz $\triangle$ zwischen $(\mathcal{P}, \mathcal{V}^*)$ und $\mathcal{S}^{\nu^*}$, $\triangle \leq 2 \cdot (1 - \beta(2/\gamma))^k$ nach Thm 5 [MV03]. Zeige:

1. $\beta(\varepsilon) \geq 1 - \varepsilon\sqrt{n}$ *,
2. $\triangle \leq 2 \cdot 2^{-k}$ für $\beta(\varepsilon) \geq 1 - \varepsilon\sqrt{N}$ und $\gamma \geq 4\sqrt{n}$.

$\beta(\varepsilon)$ ist das relative Volumen des Durchschnitts zweier Einheitskugeln im $\mathbf{R}^n$ mit Abstand ε.

$(*)$: Goldreich, Goldwasser, J. Comput. System Science 60 (2000), 540-563.