Prof. C. P. Schnorr Sommersemester 2016

Gitter und Kryptographie

Blatt 9, 17.06.2016, Abgabe 24.06.2016

Aufgabe 1. Zeige: Der Algorithmus zur Semi Block $2k$-Reduktion führt bei Eingabe einer LLL-Basis $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m \times hk}$ höchstens $\frac{h^3}{12} \log_{1/\delta_B} \alpha$ Iterationen aus bis $\mathcal{D}_B \leq 1$ erreicht ist, für $\mathcal{D}_B =_{def} \prod_{\ell=1}^{h-1} (\mathcal{D}_\ell / \mathcal{D}_{\ell+1})^{h^2/4-(h/2-\ell)^2}$.
Hinweis: Skript, Satz 6.2.4, Teil **2**. Zeige für Schritt 3: $\mathcal{D}_B^{neu} \leq \delta_B^{2k^2} \mathcal{D}_B^{alt}$.

Def. Die Basis $\mathbf{B} = \mathbf{QR} \in \mathbb{R}^{m \times n}, n = hk$, ist *streng primal-dual* wenn
1. die $\mathbf{R}_\ell = [r_{lk-k+i,lk-k+i}]_{1 \leq i \leq k}$ von $\mathbf{R}$ sind HKZ–Basen für $\ell = 1, \ldots, h$ und $\mathbf{B}$ ist längenreduziert,

2. $\max_T \bar{r}_{k\ell+1,k\ell+1} \leq (1+\varepsilon) r_{k\ell+1,k\ell+1}$ für ein $\ell = \ell_{max}$ das $\mathcal{D}_\ell / \mathcal{D}_{\ell+1}$ maximiert. $\max_T \bar{r}^2_{k\ell+1,k+1}$ maximiert $\bar{r}^2_{k\ell+1,k\ell+1}$ von $[\bar{r}_{i,j}]_{k\ell-k+1<i,j\leq k\ell+1} :=$ GNF$(\mathbf{R}'_\ell \mathbf{T})$ über alle $\mathbf{T} \in \mathrm{GL}_k(\mathbb{Z})$. Dabei ist $\mathbf{R}'_\ell = [r_{i,j}]_{k\ell-k+2 \leq i,j \leq k\ell+1}$.

Aufgabe 2. Zeige dass für jede streng primal–duale Basis gilt

$$\mathcal{D}_\ell^{1/k} \leq \big((1+\varepsilon)\gamma_k\big)^{\frac{2k}{k-1}} \mathcal{D}_{\ell+1}^{1/k} \qquad \text{für } \ell = 1, \ldots, h-1 \ .$$

Dies ersetzt $\alpha \gamma_k^2$ in den Schranken für primal–duale Basen durch $\big((1+\varepsilon)\,\gamma_k\big)^{\frac{2k}{k-1}}$.
Hinweis: Benutze den Beweis von Satz 6.3.4 (6.7)ff.

Aufgabe 3: Zeige: **GAP-CVP**$_{\sqrt{1+8/n}}$ ist **NP**–hart.
Hinweis: Satz 7.2.3 Skript

6 Punkte pro Aufgabe