Komplexitätstheorie

Sommersemester 2019

Mario Holldack, M. Sc.
Prof. Dr. Georg Schnitger
Hannes Seiwert, M. Sc.

GOETHE
UNIVERSITÄT
FRANKFURT AM MAIN

Institut für Informatik
AG Theoretische Informatik

Übungsblatt 8

Ausgabe: 10.06.2019
Abgabe: 17.06.2019

Aufgabe 8.1 *Kollisionsresistentes Hashing und One-Way-Funktionen* (8 Punkte)

Sei $\mathcal{F} := (f_i : \{0,1\}^{n_i} \to \{0,1\}^{N_i} \mid i \in I)$ eine Familie kollisionsresistenter Hashfunktionen, wobei $I \subseteq \{0,1\}^*$ eine effizient samplebare Indexmenge und f_i für jedes $i \in I$ effizient auswertbar sei.[1]

Zeigen Sie, dass $\mathcal{F}$ eine Familie von One-Way-Funktionen ist.

Aufgabe 8.2 *Shortest Independent Vectors* ($2 + 6 = 8$ Punkte)

a) Sei $A \in \mathbb{Z}^{n \times n}$ eine unimodulare Matrix. Zeigen Sie: Die inverse Matrix A^{-1} ist unimodular.

Hinweis: Sei M eine invertierbare Matrix. Für jede Zeile i und jede Spalte j sei $M^{(i,j)}$ die Matrix, die aus M entsteht, indem Zeile i und Spalte j entfernt werden. Die Adjunkte $\mathrm{adj}(M)$ ist eine Matrix mit den Einträgen

$$\mathrm{adj}(M)_{i,j} = (-1)^{i+j} \cdot \det(M^{(i,j)}).$$

Verwenden Sie die Cramersche Regel

$$M^{-1} = \tfrac{1}{\det(M)} \cdot \mathrm{adj}(M).$$

b) Die Pascal-Matrix $P^{(n)}$ ist die untere Dreiecksmatrix mit den Einträgen

$$P^{(n)}_{i,j} = \begin{cases} \binom{i}{j}, & \text{falls } 0 \le j \le i \le n-1, \\ 0, & \text{falls } 0 \le i < j \le n-1. \end{cases}$$

Bestimmen Sie eine Basis B für das Gitter $\mathcal{G}(P^{(n)})$ aus möglichst kurzen Basisvektoren, d. h. lösen Sie das Shortest-Independent-Vectors-Problem ($\mathbf{SIVP}_\gamma$ für $\gamma = 1$) für $\mathcal{G}(P^{(n)})$.

Aufgabe 8.3 *Eine obere Schranke für Shortest Vector* (8 Punkte + 5* Extrapunkte)

a) Sei $n \ge 2$. Sei $\mathcal{G} := \mathcal{G}(B)$ ein Gitter in $\mathbb{R}^n$ Zeigen Sie: Für die Länge $\lambda_1(\mathcal{G})$ eines kürzesten Basisvektors von $\mathcal{G}$ gilt

$$\lambda_1(\mathcal{G}) \le \sqrt{n} \cdot |\det(B)|^{1/n}.$$

Hinweis: Sie dürfen die folgende Aussage ohne Beweis verwenden: Sei $S \subseteq \mathbb{R}^n$ eine beliebige konvexe[2], punktsymmetrische[3] Menge mit $0 \in \mathbb{R}^n$ als Symmetriepunkt und Volumen $\mathrm{vol}(S) > 2^n \cdot |\det(B)|$. Dann enthält S einen Gitterpunkt $g \in \mathcal{G}$ mit $g \neq 0$.

b∗) Geben Sie (für beliebig große n) ein Gitter $\mathcal{G}(B) \subseteq \mathbb{R}^n$ an, für das die in a) gezeigte Schranke möglichst schlecht ist, d. h. der Approximationsfaktor

$$\alpha_n := \frac{\sqrt{n} \cdot |\det(B)|^{1/n}}{\lambda_1(\mathcal{G}(B))}$$

soll möglichst groß sein.

[1] vgl. Definition 8.4 und 8.25 im Skript

[2] Eine Menge S ist *konvex*, wenn für alle $x, y \in S$ und alle $\lambda \in [0,1]$ gilt: $\lambda x + (1-\lambda)y \in S$.

[3] Eine Menge ist *punktsymmetrisch*, wenn sie durch die Spiegelung an einem Symmetriepunkt auf sich selbst abgebildet wird.