Komplexitätstheorie

Sommersemester 2020

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

GOETHE UNIVERSITÄT
FRANKFURT AM MAIN

Institut für Informatik
AG Theoretische Informatik

Übungsblatt 4

Ausgabe: 18.05.2020
Abgabe: 25.05.2020

Die Abgabe erfolgt per E-Mail an Hannes Seiwert (`seiwert@em.uni-frankfurt.de`).

Aufgabe 4.1 *Randomisierte Komplexitätsklassen* (4 + 4 = 8 Punkte)

Zeigen Sie:

a) $\texttt{ZPP} = \texttt{RP} \cap \texttt{coRP}$

b) $\bigcup_{k\in\mathbb{N}} \texttt{RTIME}_{\frac{1}{2}-2^{-n^k},\frac{1}{2}+2^{-n^k}}(n^k) = \texttt{PP}$

Kommentar: Zum Vergleich, es gilt $\bigcup_{k\in\mathbb{N}} \texttt{RTIME}_{\frac{1}{2}-n^{-k},\frac{1}{2}+n^{-k}}(n^k) = \texttt{BPP}$.

Aufgabe 4.2 *Gleichheitstest für Polynome* (5 + 3 = 8 Punkte)

a) Sei $p = p(x_1, \ldots, x_n)$ ein n-stelliges Polynom über einem Körper $\mathbb{F}$ vom Grad[1] d, das sich vom Nullpolynom unterscheide. Sei S eine endliche Teilmenge von $\mathbb{F}$.

Zeigen Sie: $\text{prob}_{a\in S^n}\big[\, p(a) = 0 \,\big] \leq \frac{d}{|S|}$

Hinweis: Zeigen Sie per Induktion über n, dass p höchstens $d|S|^{n-1}$ Nullstellen in S^n besitzt.

b) Ein unbekanntes n-stelliges Polynom p vom Grad d über dem Körper $\mathbb{R}$ sei gegeben, wobei n und d bekannt seien.

Entwerfen Sie einen `coRP`-Algorithmus, der entscheidet, ob $p \equiv 0$ gilt, d. h. ob p das Nullpolynom ist. Der Algorithmus hat dabei nur Blackbox-Zugriff auf p, d. h. für eine Anfrage der Form $\alpha \in \mathbb{R}^n$ liefert ein Orakel die Antwort $p(\alpha)$ in Zeit $t_p \leq \text{poly}(n)$.

Aufgabe 4.3 *Bipartites perfektes Matching liegt in* `RNC` (8 Punkte)

Ein *randomisierter* Schaltkreis besitzt zusätzlich zu den Eingabegattern Gatter mit Zufallsbits. Die Klasse `RNC` (Randomized Nick's Class) enthält alle Sprachen, die durch uniforme randomisierte Schaltkreisfamilien der Größe $\text{poly}(n)$ und Tiefe poly-log(n) mit höchstens $\text{poly}(n)$ vielen Zufallsbits und beidseitigem Fehler höchstens 1/3 entschieden werden können.

Sei $n \in \mathbb{N}$. Wir betrachten bipartite Graphen $G = (L, R, E)$ mit Knotenmengen $L = R = \{1, \ldots, n\}$ und Kantenmenge $E \subseteq L \times R$. Ein solcher Graph G sei durch seine „bipartite Adjazenzmatrix" A gegeben, wobei $A = \big(a_{i,j}\big)_{i\in L, j\in R}$ und $a_{i,j} = 1$, wenn $(i, j) \in E$, und $a_{i,j} = 0$, sonst.

Ein *perfektes Matching* $M \subseteq E$ ist eine Menge von n Kanten, in der jeder Knoten zu genau einer Kante inzident ist. Wir definieren die Sprache

$$\text{BPM} := \big\{G = (L, R, E) : \text{ G besitzt ein perfektes Matching}\big\}.$$

[1] Der Grad eines Polynoms p ist der höchste Grad eines Monoms in p. Der Grad eines Monoms $m = c\prod_{i=1}^{n} x_i^{k_i}$ ist $\sum_{i=1}^{n} k_i$.

Zeigen Sie: BPM $\in$ RNC.

Hinweis: Wenden Sie Aufgabe 4.2 an. Bringen Sie die Determinante

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$$

mit der Existenz perfekter Matchings in G in Verbindung. Wie verhält sich $\det(A)$, wenn G gar kein, genau ein bzw. mehrere perfekte Matchings besitzt? Konstruieren Sie ausgehend von $\det(A)$ ein n^2-stelliges Polynom $p = p(x_{1,1}, x_{1,2}, \ldots, x_{n,n})$ über $\mathbb{R}$, sodass $p \equiv 0$ genau dann gilt, wenn G kein perfektes Matching besitzt.
Sie dürfen ohne Beweis verwenden, dass die Berechnung der Determinante $\det(R)$ einer beliebigen reellwertigen[2] $n \times n$-Matrix R in NC liegt.

Kommentar: Wir haben in der Vorlesung auch den „großen Bruder“ der Determinante kennengelernt, die *Permanente*

$$\operatorname{perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)} \; .$$

Könnten wir die Permanente effizient berechnen, dann wäre die Existenz perfekter Matchings gar kein Problem. Vieles deutet aber daraufhin, dass die Berechnung der Permanente (sogar für 0-1-wertige Matrizen) extrem schwierig ist!

[2]Natürlich vorausgesetzt, die reellen Komponenten der Matrix besitzen nicht zu viele Bits. Diese Einschränkung darf im Rahmen dieser Aufgabe aber vernachlässigt werden.