Martin Ziegler

Ausgabe am 26.1.2011
Abzugeben am 9.2.2011 11h40

# Komplexitätstheorie

WS 2010/2011, Aufgabenzettel #12

**AUFGABE 30:** (**Schwartz-Zippel**)

Ein multivariates Polynom $p \in \mathbb{Z}[X_1,\ldots,X_n]$ in dichter Darstellung ist eine Aufzählung seiner Koeffizienten, lexikographisch geordnet nach dem Grad* der zugehörigen Monome; eines in knapper Darstellung ist ein Ausdruck über $0,1,+,-,\times,X_1,\ldots,X_n$.

a) Wie 'groß' ist das $n$-variate Polynom $\prod_{j=1}^{n}(1+X_j)$ in knapper Darstellung, wie groß in dichter? Was ist sein Gesamt-, was sein Maximalgrad? Wie 'groß' ist das $n^2$-variate Polynom $\det\left((X_{ij})_{i,j}\right)$ in knapper Darstellung, was ist sein Gesamt-, was sein Maximalgrad?

b) Zeigen Sie, dass für ein $n$-variates Polynom gilt: Maximalgrad $\leq$ Gesamtgrad $\leq n\cdot$Maximalgrad.
Ein $n$-variates Polynom in knapper Darstellung der Länge $d$ hat Gesamtgrad höchstens $d$.
Ein $n$-variates Polynom vom Maximalgrad $d$ hat $\leq (d+1)^n$ Monome in dichter Darstellung.

c) Zeigen Sie: Zwei Polynome $p,q$ sind gleich genau dann, wenn ihre dichten Darstellungen übereinstimmen. Geben Sie zwei verschiedene knappe Darstellungen des gleichen Polynoms an. Geben Sie ein $0 \neq p \in \mathbb{Z}[X,Y]$ an, das unendlich viele Nullstellen besitzt.

d) Sei $\mathbb{F}$ ein Integritätsring und $0 \neq p \in \mathbb{F}[X_1,\ldots,X_n]$ vom Gesamtgrad$\leq d$ sowie $S \subseteq \mathbb{F}$. Rate zufällig, gleichmäßig und unabhängig, $x_1,\ldots,x_n \in S$. Dann gilt $p(x_1,\ldots,x_n)=0$ mit Wahrscheinlichkeit $\leq d/|S|$. Tipp: Induktion nach $n$ und verwenden Sie bedingte Wahrscheinlichkeiten.

e) Beschreiben und analysieren Sie einen $\mathcal{RP}$-Algorithmus für folgendes Problem:

Gegeben multivariate Polynome $p,q$ in knapper Darstellung, ist $p \neq q$?

f) Und für folgendes Problem:

Gegeben $n \in \mathbb{N}$ und $n$-variate Polynome $p_{i,j}$ für $1 \leq i,j \leq n$; ist $\det\left((p_{i,j})_{i,j}\right) \neq 0$?

*Der Gesamtgrad von $X^k \cdot Y^\ell$ ist $k+\ell$, der Maximalgrad $\max(k,\ell)$.

**AUFGABE 31:** (**Schönhage'79**)

Ein Straight-Line Program $S$ der Länge $N$ (über dem Ring $R$ mit Variablen $X_1,\ldots,X_m$) ist eine endliche Folge von Operationen $Z_k := 1$, $Z_k := 0$, $Z_k := -Z_j$, $Z_k := Z_j + Z_i$ und $Z_k := Z_j \cdot Z_i$ mit $i,j<k$, wobei $(Z_0, Z_{-1},\ldots,Z_{-m+1}) := (X_1,\ldots,X_m)$. Bei Belegung von $X_1,\ldots,X_m$ mit Werten aus $R$ berechnet es induktiv $Z_1, Z_2,\ldots,Z_N$. Wir schreiben $Z_N = S(X_1,\ldots,X_m)$.

a) Beschreiben Sie ein möglichst kurzes SLP in einer Variablen $X$, das $X^n$ berechnet.
Wie lange braucht es, um $2^{2^n}$ zu berechnen?

b) Geben Sie ein möglichst kurzes[†] SLP über $\mathbb{Z}$ in 0 Variablen an, das $n!$ berechnet.

c) Ein variablenfreies SLP der Länge $N$ hat $|S()| \le 2^{2^N}$.

d) Es gibt höchstens $2^N$ verschiedene Primzahlen, die $S() \neq 0$ teilen.

e) Ist $S() \neq 0$, so gibt es mindestens $2^N$ Zahlen $m < 2^{3N}$ mit $S() \neq 0 \bmod m$.
Tipp: Primzahlsatz von Hadamard/de La Vallée Poussin.

f) Beschreiben und analysieren Sie einen effizienten (randomisierten oder deterministischen) Algorithmus für das folgende Entscheidungsproblem:

$$\{\langle S_1, S_2\rangle : S_1, S_2 \text{ SLPs in 0 Variablen mit } S_1() \neq S_2()\}$$

**AUFGABE 32:**

a) Zeigen Sie, dass das folgende Problem in $\mathcal{P}^{\text{CLIQUE}}$ liegt, also in polynomieller Zeit entschieden werden kann durch eine deterministische Maschine, die CLIQUE als Orakel befragt:

> Gegeben ein Graph, hat die maximale enthaltene Clique ungerade Größe?

b) Zeigen Sie, dass das folgende Problem MINCIRCUIT in $\text{co}\mathcal{NP}^{\text{SAT}}$ liegt:

> Gegeben ein Schaltkreis $C(X_1,\ldots,X_n)$. Dann gibt es keinen echt kleineren Schaltkreis, der die gleiche Funktion $\{0,1\}^n \to \{0,1\}$ berechnet.

Liegt das Problem in $\mathcal{NP}$? in $\text{co}\mathcal{NP}$?

c) Sei $\ell \in \mathbb{N}$. Zeigen Sie, dass das folgende Problem in $\mathcal{P}^{\text{SAT}}$ liegt:

> Gegeben eine Boole'sche Funktion $\varphi(X_1,\ldots,X_n)$;
> gibt es einen Schaltkreis mit maximal $\ell$ Gattern, der $\varphi$ berechnet?

Liegt das Problem in $\mathcal{NP}$? in $\text{co}\mathcal{NP}$?

d) Seien $\mathcal{B}, \mathcal{C} \supseteq \mathcal{P}$ Klassen von Sprachen und $C$ sei $\mathcal{C}$-vollständig bzgl. Polynomialzeitreduktion. Dann gilt $\mathcal{B}^{\mathcal{C}} = \mathcal{B}^{C}$.

e) Zeigen Sie: $\mathcal{NP} \cup \text{co}\mathcal{NP} \subseteq \mathcal{P}^{\mathcal{NP}}$.

f) Falls $\mathcal{NP} \cup \text{co}\mathcal{NP} = \mathcal{P}^{\mathcal{NP}}$, so folgt $\mathcal{NP} = \text{co}\mathcal{NP}$.
Tipp: Betrachten Sie $(\{0\} \times A) \cup (\{1\} \times A^{\complement})$.

[†] Der Weltrekord liegt bei $\mathcal{O}(\sqrt{n} \cdot \text{polylog}\, n)$...