Martin Ziegler
Carsten Rösnick

Distributed on 2012-01-26
Solutions to be submitted by 2012-02-02 14h25

Complexity Theory

WS 2011/2012, Exercise Sheet #11

EXERCISE 29: **(Schwartz-Zippel)**

A multivariate polynomial $p \in \mathbb{Z}[X_1,\ldots,X_n]$ in dense encoding is an enumeration of its coefficients, lexikographically ordered according to the degree* of their corresponding monomials; one in sparse encoding is an expression over $0,1,+,-,\times,X_1,\ldots,X_n$.

a) Prove that an n-variate polynomial has maximal degree $\leq$ total degree $\leq n\cdot$maximal degree. An n–variate polynomial in dense encoding of length d has total degree at most d. An n–variate polynomial of maximal degree d consists in dense encoding of $\leq (d+1)^n$ monomials.

b) How 'large' is the n-variate polynomial $\prod_{j=1}^{n}(1+X_j)$ in sparse encoding, how large in dense encoding? Determine its total and maximal degree.

c) Determine the total and maximal degree and size of the dense encoding of the n^2–variate polynomial $\det\big((X_{ij})_{i,j}\big)$. Analyze the LU decomposition algorithm to obtain a 'small' sparse encoding. How small?

d) Prove: Two polynomials p,q are equal iff their dense encodings coincide. Specify two different sparse encodings of the same polynomial. Specify a non-zero $p \in \mathbb{Z}[X,Y]$ with infinitely many roots.

e) Let $\mathbb{F}$ denote an integral domain and $0 \neq p \in \mathbb{F}[X_1,\ldots,X_n]$ a polynomial of total degree$\leq d$ and $S \subseteq \mathbb{F}$. With respect to $x_1,\ldots,x_n \in S$ guessed uniformly independently at random, prove that $p(x_1,\ldots,x_n) = 0$ holds with probability $\leq d/|S|$. Hint: Induction w.r.t. n using conditional probabilities.

f) Describe and analyze an $\mathcal{RP}$ algorithmus for the following problem:

   Given multivariate polynomials p,q in spares representation, does $p \neq q$ hold?

g) And for the following problem:

   Given $n \in \mathbb{N}$ and n-variate polynomials $p_{i,j}$ for $1 \leq i,j \leq n$, is $\det\big((p_{i,j})_{i,j}\big) \neq 0$?

---

*$X^k \cdot Y^\ell$ has total degree $k+\ell$ and maximal degree $\max(k,\ell)$.

EXERCISE 30: **(Schönhage'79)**

A Straight-Line Program (SLP) S of length N (over ring R in variables $X_1,\ldots,X_m$) is an N-element sequence of operations $Z_k := 1$, $Z_k := 0$, $Z_k := -Z_j$, $Z_k := Z_j + Z_i$, and $Z_k := Z_j \cdot Z_i$ with $i,j < k$ where $(Z_0, Z_{-1}, \ldots, Z_{-m+1}) := (X_1,\ldots,X_m)$. Upon assignment to $X_1,\ldots,X_m$ values from R, S calculates inductively $Z_1, Z_2, \ldots, Z_N$. We abbreviate $Z_N = S(X_1,\ldots,X_m)$.

a) Describe a short SLP in one variable X calculating X^n. How long does it take to calculate the constant 2^{2^n}?

b) Describe a short† SLP over $\mathbb{Z}$ in 0 variables calculating $n!$

c) A variable-free SLP of length N has $|S()| \leq 2^{2^N}$.

d) There are no more than 2^N distinct primes dividing $S() \neq 0$.

e) To $S() \neq 0$ there are at least 2^N integers $m < 2^{3N}$ satisfying $S() \neq 0 \bmod m$.
Hint: Prime number theorem of Hadamard/de La Vallée Poussin.

f) Describe and analyze an efficient (randomized or deterministic) algorithm for the following decision problem:

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

EXERCISE 31:

Let $n \in \mathbb{N}$ and $R \subseteq \{0,1\}^n$. "$\oplus : \{0,1\}^2 \to \{0,1\}$" denotes *exclusive* or, that is binary addition modulo 2. For $\vec{x}, \vec{u} \in \{0,1\}^n$ write $\vec{x} \oplus \vec{u} := (x_1 \oplus u_1, \ldots, x_n \oplus u_n)$ and $X \oplus \vec{u} := \{\vec{x} \oplus \vec{u} : \vec{x} \in X\}$. For a proposition $A(\vec{u})$ with parameter $\vec{u}$, $\Pr_{\vec{u}}[A(\vec{u})]$ denotes the probability that A becomes `true` for $\vec{u} \in \{0,1\}^n$ chosen uniformly componentwise independently at random.

a) Let $\vec{y} \in \{0,1\}^n$. Prove: $\vec{y} \in R \oplus \vec{u} \Leftrightarrow \vec{u} \oplus \vec{y} \in R \Leftrightarrow \vec{u} \in R \oplus \vec{y}$.

b) $\Pr_{\vec{u}}[\vec{y} \in R \oplus \vec{u}] = \Pr_{\vec{u}}[\vec{u} \in R]$ and $\Pr_{\vec{u},\vec{v}}[\vec{y} \in (R \oplus \vec{u}) \cap (R \oplus \vec{v})] = \Pr_{\vec{u}}[\vec{y} \in R \oplus \vec{u}] \cdot \Pr_{\vec{v}}[\vec{y} \in R \oplus \vec{v}]$.

c) Let $1 \leq n \leq p < 2^n$ and $R \subseteq \{0,1\}^p$ with $\mathrm{Card}(R) \leq 2^{-n} \cdot 2^p$.
Show that no choice of $\vec{t}_1, \ldots \vec{t}_p \in \{0,1\}^p$ satisfies $\{0,1\}^p = \bigcup_{i=1}^p (R \oplus \vec{t}_1)$.

†The world record being $\mathcal{O}(\sqrt{n} \cdot \mathrm{polylog}\, n)\ldots$