Prof. Juraj Hromkovič
Juraj.Hromkovic@inf.ethz.ch

Design of Randomized Algorithms

Final Exam

The exam of the course "Design of Randomized Algorithms" (21. April 2008 – 24. April 2008) consists of the following set of exercises. Please send your solutions to **Prof. Carlo Mereghetti** <mereghetti@dsi.unimi.it> until **1. June 2008**.

Final Exam Exercise 1

Use the method described in the lecture to modify the algorithm LV_{10} from Example 2.4.44 in such a way that the output "?" does not occur. Then, analyze the expected communication complexity of your Las Vegas protocol with forbidden "?".

Def. 1 Protocol LV_{10} from example 2.4.44.

Initial situation: R_I has ten strings, $x_1, \ldots, x_{10}$, $x_i \in \{0,1\}^n$ for all i and R_{II} has ten strings, $y_1, \ldots, y_{10}$, $y_i \in \{0,1\}^n$ for all i.

Phase 1: R_I uniformly chooses 10 primes, $p_1, \ldots, p_{10}$, from $PRIM(n^2)$ at random.

Phase 2: R_I computes

$$S_i = Number(x_i) \bmod p_i$$

for $i = 1, \ldots, 10$ and sends

$$p_1, \ldots p_{10}, s_1, \ldots, s_{10}$$

to R_{II}.

Phase 3: R_{II} computes

$$q_i = Number(y_i) \bmod p_i$$

for all i. If $s_i \neq q_i$ for all i, then R_{II} knows with certainty that $x_i \neq y_i$ for all i and outputs "0" (reject). Else, let J be the smallest integer from $\{1, \ldots, 10\}$, such that $s_j = q_j$. Then R_{II} sends the whole string y_j to R_I.

Phase 4: R_I compares x_j with y_j bit by bit. If $x_j = y_j$, then R_I outputs "1" (accept). If $x_j \neq y_j$, then R_I outputs "?".

Final Exam Exercise 2

Let A be a randomized algorithm computing a function F with $Prob(A(x) = F(x)) \geq 1/3$ for every argument x of F. Assume that one is aware of the fact that $Prob(A(x) = \alpha) \leq 1/4$ for every wrong result α (i.e., that the probability of computing any specific wrong result is at most 1/4). Can this knowledge be used to design a useful randomized algorithm for F?

Final Exam Exercise 3

Let us consider the following communication task. R_I has got a sequence $x_1, \ldots, x_n$ of strings, $x_i \in \{0,1\}^n$ for $i = 1, 2, \ldots, n$. R_{II} has got a sequence $y_1, y_2, \ldots, y_n$ of strings, $y_i \in \{0,1\}^n$ for $i = 1, 2, \ldots, n$. The question is whether there exists a $j \in \{1, 2, \ldots, n\}$ such that $x_j = y_j$. One

can prove that any deterministic protocol solving this task has a communication complexity of at least n^2. Design a Las Vegas protocol that solves this problem with expected communication complexity in $O(n \log n)$.

Final Exam Exercise 4

Consider the communication protocol R presented in Section 1.2 for the comparison of two binary strings (of the contents of two databases).[1] Let p be a prime and let $a = a_1 a_2 \dots a_n$, $a_i \in \{0,1\}$ for $i = 1, \dots, n$, be a binary string. Consider the polynomial P_a of a single variable x defined over $\mathbb{Z}_p$ as follows.

$$P_a(x) = \sum_{i=1}^{n} a_i x^{i-1}.$$

Apply the idea of algorithm AQP[2] in order to design a one-side-error Monte Carlo protocol for the comparison of two n bit strings $a = a_1 a_2 \dots a_n$ and $b = b_1 b_2 \dots b_n$. What effect does the choice of p have on the error probability and on the communication complexity? Compare the results with the complexity and the success probability of the protocol R from Section 1.2.

Final Exam Exercise 5

Let S be a randomly chosen group of persons. How large has S to be in order to assure

$$Prob(\text{two persons from } S \text{ were born on the same day}) \geq \frac{1}{2}?$$

To answer this question, consider the indicator variable X defined by

$$X(S) = \begin{cases} 1 & \text{if there are two persons in } S \text{ with the same birthday} \\ 0 & else \end{cases}.$$

Assume that the birthdays are uniformly distributed over the year and nobody was born on February 29. Estimate $E[X]$ as a function of $|S|$.

Final Exam Exercise 6

The following theorem has been formulated on the lecture (Theorem 6.2.2):

> For every odd $n \in \mathbb{N}$ such that $(n-1)/2$ is odd it holds that: If n is not prime, then $a^{(n-1)/2} \bmod n \notin \{1, n-1\}$ holds for at least one half of elements a in range $\{1, 2, \dots, n-1\}$.

We proved this claim for the case $n = p \cdot q$ such that the greatest common divisor of p and q is 1. Prove it for the case $n = p^d$, where p is a prime.

[1] The randomized protocol R for equity chooses witnesses among the primes from range 1 to n^2. It has probability of error at most $\frac{2 \ln n}{n}$ and communication complexity at most $4\lceil \log_2 n \rceil$ (for n large enough).

[2] Algorithm for solving the equivalence of two polynomials presented in the lecture: The polynomial variables are assigned random values (all arithmetic is done in a finite field $\mathbb{Z}_p$), both polynomials are evaluated and the values are compared.