Randomised Algorithms

Winter term 2022/2023, Exercise Sheet No. 1

Hand-out:	Mon,	17. Oct.
Hand-in:	Sun,	23. Oct.

UNIVERSITY OF PASSAU
Faculty of Computer Science and Mathematics

Dr. Duc-Cuong Dang
Prof. Dr. Dirk Sudholt

Organisation

Please sign up on Ilias at
`https://ilias.uni-passau.de/ilias/goto.php?target=crs_213934`
You are encouraged to work in a team of up to 3 students. One of your team will submit your team's work on Ilias (usually before Sunday 23:00). Solutions will be discussed in tutorial groups the following week.

The groups are:

Group 1: Tue 14:15-15:45, ITZ SR 011

Group 2: Thu 14:15-15:45, ITZ SR 011

Group 3: Thu 16:15-17:45, ITZ SR 011

Exercise 1 [6 points]

Mr Thump is a businessman with a multiple personality disorder, he has two personalities: a honest one and the other one is dishonest. Suppose you are a journalist and you want to investigate his fixed net worth N, so you slide in the same question asking N during several interviews. We assume that independently each time one of his personalities comes out: with probability $p \in (0, 1)$ he is honest and his answer will be N, otherwise with probability $1 - p$ he is dishonest and will inflate the answer to a random value strictly bigger than N.

(a) Based on n recorded answers $\{a_1, \ldots, a_n\}$, can you give the best estimation of his net worth?

(b) Can you be certain (with probability 1) that the estimation is exact for a finite number of answers?

(c) Compute numerically the probability that the estimate is exact for $p = 1/2$ and $n = 10$.

Exercise 2 [6 points]

Suppose you have an unfair coin that shows heads with probability $0 < p < 1$ and tails with probability $1 - p$. However, you do not know the value of p. Can you still simulate an event with probability $1/2$ using coin tosses?

Exercise 3 [8 points]

Suppose we modify the communication protocol (without probability amplification) to choose a prime number from the set of prime numbers smaller than n^{20} (instead of n^2). Give upper bounds for the communication complexity and the error probability, as a function of n and additionally for the concrete value $n = 10^{16}$. Compare the above algorithm with the protocol R_{10} with probability amplification in terms of communication complexity and error probability.