Randomised Algorithms
Winter term 2022/2023, Exercise Sheet No. 1

Authors:
Ben Ayad, Mohamed Ayoub
Kamzon, Noureddine

October 23, 2022

Exercise 1.

(a) *The best estimate is* $\min\{a_1, \ldots, a_n\}$

If at least one sample was honest, the estimate would be exact, otherwise, if all samples were dishonest, the smallest sample would be the closest to N*, since all the answers would be strictly bigger than* N*.*

(b) *The probability that the estimate is correct can be expressed as follows:*

$$\begin{aligned}\mathbb{P}(\{\textit{The estimate is correct}\}) &= \mathbb{P}(\{\textit{At least one sample was honest}\}) \\ &= 1 - \mathbb{P}(\{\textit{All answers are dishonest}\}) \\ &= 1 - (1-p)^n\end{aligned}$$

Setting this probability to 1, would mean that $(1-p)^n = 0$*, i.e.,* p *= 1.*

(c) *For* $n = 10$ *and* $p = 0.5$*, we have* $\mathbb{P}(\{\textit{The estimate is correct}\}) = 1 - (1-p)^n$*, and hence,* $\mathbb{P}(\{\textit{The estimate is correct}\}) = 0.999$*.*

Exercise 2.

We toss the coin twice, let H_1 *and* H_2 *be the random variables associated with each toss, we are interested in the following event:* $\mathbb{P}[H_1|(H_1\&\bar{H}_2)or(\bar{H}_1\&H_2)]$*, meaning, the probability that* H_1 *was heads knowing that only one of the coin tosses was head.* ***This event has a probability of 1/2.***

$$\begin{aligned}\mathbb{P}(H_1|(H_1\bar{H}_2)or(\bar{H}_1H_2)) &= \frac{\mathbb{P}[H_1 and((H_1\bar{H}_2)or(\bar{H}_1H_2))]}{\mathbb{P}((H_1\bar{H}_2)or(\bar{H}_1H_2))} \\ &= \frac{\mathbb{P}[(H_1\bar{H}_2)]}{\mathbb{P}((H_1\bar{H}_2)or(\bar{H}_1H_2))} \\ &= \frac{p(1-p)}{2p(1-p)} \\ &= \frac{1}{2}\end{aligned}$$

Exercise 3.
We assume that $n > 9$ throughout this exercise, and use the results of that we have established in class during the first session.
Case: Choosing $p < n^{20}$

- *Upper bound on the communication complexity :*

  We have $s < p < n^{20}$, meaning we would need at most $2\lceil\log_2(n^{20})\rceil \leq 40\lceil\log_2(n)\rceil$
  For $n = 10^{16}$, we get the following upper bound: $40 * 16 * 4 = 2560$ bits

- *Upper bound on the error :*

  We still have $x - y < 2^n$, and hence, the number of bad prime numbers is still at most $n-1$. On the other hand, the spaces of choices of primes got bigger, $|primes(n^{20})|$

$$\begin{aligned}\mathbb{P}(An\ incorrect\ answer) &\leq \frac{n-1}{|primes(n^{20})|}\\ &\leq \frac{(n-1)ln(n^{20})}{n^{20}}\\ &\leq \frac{20(n-1)ln(n)}{n^{20}}\end{aligned}$$

For $n = 10^{16}$, we can easily get the following upper bound: 10^{-300}
Case: Protocol R_{10}

- *Upper bound on the communication complexity :*

  Assuming $p < n^2$, the communication complexity would simply be multiplied by 10, i.e., 256 bits$*$ $10 = 2560$ bits.

- *Upper bound on the error :*

$$\begin{aligned}\mathbb{P}(R_{10}\ making\ an\ error) &= \mathbb{P}[\{p_i\ making\ an\ error\ for\ all\ i \in \{1, \ldots, 10\}\}]\\ &= \prod_{i=1}^{10} \mathbb{P}[\{p_i\ making\ an\ error\ \}]\\ &\leq \prod_{i=1}^{10} \frac{2ln(n)}{n}\\ &= \frac{2^{10}ln(n)^{10}}{n^{10}}\end{aligned}$$

Each choice of p_i is independent from the others, which justifies the second equality.
For $n = 10^{16}$, we can easily get the following upper bound: $4.8 \cdot 10^{-142}$
Conclusion: *They have similar upper bounds regarding the communication complexity, and the probability of an incorrect answer is practically ZERO for both of them.*