Randomised Algorithms
Winter term 2022/2023, Exercise Sheet No. 8

Authors:
Ben Ayad, Mohamed Ayoub
Kamzon, Noureddine

December 11, 2022

Exercise 1.
(a) *The algorithm described briefly as follows, has a* ***cubic*** *runtime.*

for $1 \leq i \leq n, 1 \leq j \leq n$ ***do***
    $\alpha_{i,j} \leftarrow sum([A_{i,k}B_{k,j} : k \in \{1, \dots, n\}])$
    $\alpha_{i,j} \leftarrow \alpha_{i,j} - c_{i,j}$
    if $\alpha_{i,j} \neq 0$ ***then***
        return 0
    end if
end for
return 1

(b) *Computing x, y, and z requires $\mathcal{O}(n^2)$ each, and computing $t = y - z$ requires $\mathcal{O}(n)$, hence, the asymptotic runtime of this RA is $\mathcal{O}(n^2)$.*

(c) *If $r \neq 0$, the event $\mathcal{E}$ implies the following:*

- $r \in Ker(D)$
- *r is orthogonal to all rows of D*
- *Since $D \neq 0$, there exists at least one row $d_i \neq 0$ s.t: $d_i^\top r = 0$*

We have:

$$\begin{aligned} \mathbb{P}[\mathcal{E}] &= \mathbb{P}[Dr = 0 | r = 0]\mathbb{P}[r = 0] + \mathbb{P}[Dr = 0 | r \neq 0]\mathbb{P}[r \neq 0] \\ &= \frac{1}{3^n} + \mathbb{P}[Dr = 0 | r \neq 0](1 - \frac{1}{3^n}) \qquad \textbf{\textit{[1]}} \end{aligned}$$

For some $k \leq n$, we let, $d_1, \dots, d_k$ be the rows of D that are not equal to 0. We have:

$$\begin{aligned} \mathbb{P}[Dr = 0 | r \neq 0] &= \mathbb{P}[d_1^\top r = 0, \dots, d_k^\top r = 0 | r \neq 0] \\ &\leq \mathbb{P}[d_1^\top r = 0 | r \neq 0] \qquad \textbf{\textit{[2]}} \end{aligned}$$

Let $d_{1,j}$ be the last element of d_1 not equal to 0, we have: $d_1^\top r = 0$ ***if and only if*** *after $j-1$ picks of $r_1, \dots, r_{j-1}$, the j^{th} pick (i.e., r_j) is chosen s.t: $-d_{1,j}r_j = \sum_{i=1}^{j-1} d_{1,i}r_i$.*

And hence, knowing the values $r_1, \dots, r_{j-1}$, we conclude the following:

$$\mathbb{P}[d_1^\top r = 0 | r \neq 0] = \mathbb{P}\left[r_j = \sum_{i=1}^{j-1} \frac{-d_{1,i}}{d_{1,j}} r_i | r \neq 0 \right] \leq \frac{1}{3}$$

*Using **[2]**, we get $\mathbb{P}[Dr = 0 | r \neq 0] \leq \frac{1}{3}$, anf from **[1]**, we conclude that:*

$$\mathbb{P}[\mathcal{E}] \leq \frac{1}{3^n} + \frac{1}{3}(1 - \frac{1}{3^n}) \leq \frac{1}{3}$$

(d) *We can reduce the probability by amplification.*

Exercise 2.

(a) *We condider the following Algorithm T_k, we choose $k = [\sqrt{2n}] + 1$.*

We generate k images, as follows: $e_1 = h(1), \dots, e_k = h(k)$
if *A collision happens* ***then***
  return $s = n$
end if
return $s = n^2$

(b) *We will refer to the probability of T_k being correct as $\mathbb{P}[T]$, we have:*

$$\begin{aligned}
\mathbb{P}[T] &= \mathbb{P}[s = n]\mathbb{P}[T | s = n] + \mathbb{P}[s = n^2]\mathbb{P}[T | s = n^2] \\
&= \frac{1}{2}(\mathbb{P}[T | s = n] + \mathbb{P}[T | s = n^2]) \\
&= \frac{1}{2}(\mathbb{P}[\textit{A collision happening in } T_k | s = n] + \mathbb{P}[\textit{No collisions happening in } T_k | s = n^2])
\end{aligned}$$

From the lecture notes, we have, $\mathbb{P}[\textit{A collision happening in } T_k | s = n] > \frac{1}{2}$, also:

$$\begin{aligned}
\mathbb{P}[\textit{No collisions happening in } T_k | s = n^2]) &= \prod_{i=2}^{k} (1 - \frac{i-1}{n^2}) \\
&\geq (1 - \frac{k-1}{n^2})^k \qquad \textit{(using the Bernoulli Inequality)} \\
&\geq 1 - \frac{k(k-1)}{n^2} \\
&> \frac{1}{2} \qquad (\textit{as } \frac{n}{2} > k)
\end{aligned}$$

Exercise 3.
(a) *We have:*

$$\begin{aligned}
\sum_{i\geq 1}\mathbb{P}[X\geq i] &= \sum_{i\geq 1}\sum_{j=i}^{\infty}\mathbb{P}[X=j]\\
&= \sum_{j\geq 1}\sum_{i=1}^{j}\mathbb{P}[X=j]\\
&= \sum_{j\geq 1}\mathbb{P}[X=j]\sum_{i=1}^{j}1\\
&= \sum_{j\geq 1}j\mathbb{P}[X=j]=\mathbb{E}[X]
\end{aligned}$$

If X can only take negative values, then:

$$\begin{aligned}
\mathbb{E}[X] &= -\mathbb{E}[-X]\\
&= -\sum_{j\geq 1}\mathbb{P}[-X\geq j]\\
&= -\sum_{j\geq 1}\mathbb{P}[X\leq -j]
\end{aligned}$$

(b) *Let $\mathbb{P}[X\geq 0]=p_X$, and $\mathbb{P}[Y\geq 0]=p_Y$, we have: $p_X\leq p_Y$, we suppose that $0<p_X<1$ and $0<p_Y<1$:*

$$\begin{aligned}
\mathbb{E}[Y]-\mathbb{E}[X] &= p_Y\mathbb{E}[Y|Y>0]+(1-p_Y)\mathbb{E}[Y|Y<0]-p_X\mathbb{E}[X|X>0]-(1-p_X)\mathbb{E}[X|X<0]\\
&= p_Y\mathbb{E}[Y|Y>0]-p_X\mathbb{E}[X|X>0]+(1-p_Y)\mathbb{E}[Y|Y<0]-(1-p_X)\mathbb{E}[X|X<0] \qquad \textbf{\textit{Eq.}}\ \#42
\end{aligned}$$

We have:
for $i\geq 1$:

$$\begin{aligned}
\mathbb{P}[X\geq i]\leq\mathbb{P}[Y\geq 1] &\implies \sum_{k\geq 1}\mathbb{P}[X\geq k]\leq\sum_{k\geq 1}\mathbb{P}[Y\geq k]\\
&\implies \sum_{k\geq 1}\frac{\mathbb{P}[X\geq k]}{p_Y}\leq\sum_{k\geq 1}\frac{\mathbb{P}[Y\geq k]}{p_Y}\\
&\implies p_X\sum_{k\geq 1}\frac{\mathbb{P}[X\geq k]}{p_X}\leq p_Y\sum_{k\geq 1}\frac{\mathbb{P}[Y\geq k]}{p_Y} \qquad \textit{(as } p_X\leq p_Y\textit{)}\\
&\implies p_X\mathbb{E}[X|X>0]\leq p_Y\mathbb{E}[Y|Y>0] \quad \textit{[1]} \quad \textit{(using the result of the past question)}
\end{aligned}$$

On the other side, we have:

$$\mathbb{E}[X|X<0]=-\sum_{i\geq 1}\frac{\mathbb{P}[X\leq -i]}{1-p_X}\implies(1-p_X)\mathbb{E}[X|X<0]=-\sum_{i\geq 1}\mathbb{P}[X\leq -i]$$

Similarily:

$$(1-p_Y)\mathbb{E}[Y|Y<0] = -\sum_{i\geq 1}\mathbb{P}[Y\leq -i]$$

Hence,

$$\begin{aligned}(1-p_Y)\mathbb{E}[Y|Y<0]-(1-p_X)\mathbb{E}[X|X<0] &= \sum_{i\geq 1}\mathbb{P}[X\leq -i]-P[Y\leq -i]\\ &= \sum_{i\geq 1}\mathbb{P}[Y\geq i]-P[X\geq i]\\ &\geq 0 \qquad \textit{[2]}\end{aligned}$$

*By using the results in **[1]** and **[2]** in **Eq.** #42, we conclude that* $\mathbb{E}[X]\leq\mathbb{E}[Y]$.