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

Authors:
Ben Ayad, Mohamed Ayoub
Kamzon, Noureddine

December 10, 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 $r \neq 0$, this event 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:

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

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:

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

*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.