

# Negyedik házfeladat

## Bonyolultság elmélet gyakorlat

Toffalini Leonardo

### Feladat 1

Adj egy  $\tilde{O}(n^2)$  idejű randomizált algoritmust, ami edlönti az  $A, B, C$   $n \times n$ -es egész mátrixokról, hogy  $A \cdot B = C$  igaz-e. Melyik osztályba van ez az algoritmus **RP**, **co-RP**, és **BPP** közül?

### Lemma 0.1

Schwartz–Zippel

Legyen  $P \in \mathbb{Z}[x_1, \dots, x_n]$  egy nem azonosan nulla polinom, aminek a foka legalább  $d \geq 0$ .  
Legyen  $S$  egy véges halmaz és  $r_1, \dots, r_n \in S$  véletlen elemek. Ekkor

$$\mathbb{P}(P(r_1, \dots, r_n) = 0) \leq \frac{d}{|S|}.$$

### Megoldás

$$A \cdot B = C \iff AB - C = 0$$

Ha  $AB - C = 0$ , akkor  $(AB - C)x = 0$  minden  $x \in \mathbb{R}^n$ -re. Nyilván  $AB - C$  is egy  $n \times n$ -es egész mátrix.

Figyeljük meg, hogy egy  $c \cdot x$  skaláris szorzat érthető úgy mint egy  $c$  együtthatókkal rendelkező  $n$  változós elsőrendű polinomba behelyettesítés:

$$x_1 c_1 + x_2 c_2 + \dots + x_n c_n.$$

Ha  $AB - C$  sorait a  $c_i$  vektorok jelölik, akkor  $(AB - C)x = 0$  ekvivalens azzal, hogy  $x$  gyöke a  $c_i$  együtthatós elsőfokú  $n$  változós polinomoknak.

Tehát az algoritmus csak annyit fog csinálni, hogy kiválaszt véletlenül egy  $n$  hosszú  $x$  vektort egy kellően nagy halmazból és leteszteli, hogy  $(AB - C)x \stackrel{?}{=} 0$ .

Ha van olyan koordináta ami nem 0, akkor fixen  $AB \neq C$ , ha viszont a csupa nulla vektort kapjuk eredményül, akkor csak kis eséllyel tévedünk.

Amikor a nem választ mindig eltaláljuk és az igenlő válasznál mindig legfeljebb  $\frac{1}{2}$  eséllyel tévedünk az a **co-RP** definíciója. Tehát ez a feladat **co-RP**-ben van. Mivel **co-RP**  $\subseteq$  **BPP**, ezért **BPP**-ben is benne van ez a feladat.

Ennek az algoritmusnak a futásideje valóban négyzetes (logaritmusoktól eltekintve), mivel sosem szoroztunk össze mátrixokat, csak mátrix-vektor szorzatot számoltunk, ami négyzetes időben könnyen kiszámolható. Újra zárójellezve látjuk, hogy

$$(AB - C)x = A(Bx) - Cx,$$

ahonnan valóban csak három mátrix-vektor szorzatot és egy vektor-vektor kivonást kell elvégeznünk RAM-gépen, amit meg tudunk csinálni  $\tilde{O}(n^2)$  időben.