

## פתרון תרגיל מספר 9 - דאסט

שם: מיכאל גרינבאום, ת"ז: 211747639

24 במאי 2019

1. פתרון:

(א) צ"ל:  $k-1$  אוניברסלית

הוכחה:

יהיו  $\{0, \dots, m-1\}$   $\alpha_1, \dots, \alpha_{k-1}$ , ויהיו  $x_1, \dots, x_k \in U$  נשים לב כי

$$\begin{aligned}\mathbb{P}\left(\bigwedge_{i=1}^{k-1} h(x_i) = \alpha_i\right) &= \sum_{j=0}^{m-1} \mathbb{P}\left(\left(\bigwedge_{i=1}^{k-1} h(x_i) = \alpha_i\right) \mid h(x_k) = j\right) \cdot \mathbb{P}(h(x_k) = j) \\ &\stackrel{*}{=} \sum_{j=0}^{m-1} \mathbb{P}\left(\left(\bigwedge_{i=1}^{k-1} h(x_i) = \alpha_i\right) \wedge (h(x_k) = j)\right) \\ &\leq \sum_{j=0}^{m-1} \frac{1}{m^k} = \frac{m}{m^k} = \frac{1}{m^{k-1}}\end{aligned}$$

כלומר הראנו שלכל  $\alpha_1, \dots, \alpha_{k-1} \in \{0, \dots, m-1\}$  ולכל  $x_1, \dots, x_{k-1} \in U$  מתקיים

$$\mathbb{P}\left(\bigwedge_{i=1}^{k-1} h(x_i) = \alpha_i\right) \leq \frac{1}{m^{k-1}}$$

כלומר  $\mathcal{H}$  היא  $k-1$  אוניברסלית

הערה: \* מתקיים כי המאורעות בלתי תלויים

מ.ש.ל.א. ☺

(ב) צ"ל: הפרך שאם  $\mathcal{H}$  היא 1 אוניברסלית אזי  $\mathcal{H}$  אוניברסלית

הוכחה:

נבחר  $\mathcal{H} = \{h = r\}$ , כאשר  $r$  מוגרל אקראית בין  $0, \dots, m-1$ , לכן

$$\mathbb{P}(h(x) = \alpha) = \frac{1}{m} \leq \frac{1}{m}$$

כלומר  $\mathcal{H}$  היא 1 אוניברסלית, עתה נשים לב כי

$$\mathbb{P}(h(x) = h(y)) = 1 > \frac{1}{m}$$

כלומר  $\mathcal{H}$  היא לא אוניברסלית

מ.ש.ל.ב. ☺

2. צ"ל: הוכיחו ש  $\mathcal{H}$  היא 2-אוניברסלית

הוכחה:

נוכיח באינדוקציה על  $d$  ש  $h_{a,b}$  היא 2-אוניברסלית

בסיס:  $d=1$ , ראינו בתרגול ש  $h_{a,b}$  היא 2-אוניברסלית

**צעד:** נניח ש  $h_{a_d,b}$  היא 2-אוניברסלית לכל  $a_d \in \mathbb{F}_p^d$  ונוכיח ל  $a_{d+1} \in \mathbb{F}_p^{d+1}$ , נשים לב כי מספר האפשרויות להרחיב את הוקטור  $a_d$  ל  $a_{d+1}$  הוא  $p$ , נשים לב כי מספר האפשרויות להרחיב את הוקטור  $a_d$  ל  $a_{d+1}$  כך ש  $h_{a_{d+1},b}(x) = \alpha$  הוא 1, לכן

$$\mathbb{P}(h_{a_{d+1},b}(x) = \alpha) \leq \frac{1}{p} \cdot \mathbb{P}(h_{a_d,b}(x) = \alpha)$$

לכן

$$\begin{aligned} \mathbb{P}(h_{a_{d+1},b}(x) = \alpha \cap h_{a_{d+1},b}(y) = \beta) &\stackrel{*}{=} \mathbb{P}(h_{a_{d+1},b}(x) = \alpha) \cdot \mathbb{P}(h_{a_{d+1},b}(y) = \beta) \\ &\leq \frac{1}{p} \cdot \mathbb{P}(h_{a_d,b}(x) = \alpha) \cdot \frac{1}{p} \cdot \mathbb{P}(h_{a_d,b}(y) = \beta) \\ &\stackrel{\text{induction}}{\leq} \frac{1}{p^2} \cdot \frac{1}{|\mathbb{F}_p^d|^2} = \frac{1}{|\mathbb{F}_p^{d+1}|^2} \end{aligned}$$

כלומר קיבלנו כי לכל  $x, y, \alpha, \beta$  מתקיים לכל  $d$

$$\mathbb{P}(h_{a_d,b}(x) = \alpha \cap h_{a_d,b}(y) = \beta) \leq \frac{1}{|\mathbb{F}_p^{d+1}|^2}$$

כלומר  $\mathcal{H}$  היא 2-אוניברסלית  
**הערה:** \* מתקיים כי המאורעות בלתי תלויים

מ.ש.ל.  $\odot$

3. **צ"ל:** סיכוי לשרוד את ת'אנוס אולי אפילו פעמיים!!!!  
**הוכחה:**  
נשים לב כי

$$\mathbb{P}(\text{survived}) = \mathbb{P}(\text{survived} \mid 2 \text{ thanoses}) \cdot \mathbb{P}(2 \text{ thanoses}) + \mathbb{P}(\text{survived} \mid 1 \text{ thanos}) \cdot \mathbb{P}(1 \text{ thanos})$$

נשים לב כי מהיות ההתפלגות אחידה מתקיים

$$\mathbb{P}(1 \text{ thanos}) = \mathbb{P}(2 \text{ thanoses}) = \mathbb{P}(\text{survived} \mid 1 \text{ thanos}) = \frac{1}{2}$$

וגם

$$\mathbb{P}(\text{survived} \mid 2 \text{ thanoses}) = \frac{1}{2^2} = \frac{1}{4}$$

נציב ונקבל

$$\boxed{\mathbb{P}(\text{survived}) = \frac{1}{2} \cdot \frac{1}{4} + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{8}}$$

**הערה:** זה סיכוי יותר טוב מלא לקבל ספוילרים ל  $\text{end game}$   $\odot$

מ.ש.ל.  $\odot$

4. **צ"ל:** אלגוריתם ל  $O(n)$  בממוצע  
**הוכחה:**

הצעה לאלגוריתם: נעבור איבר איבר במערך שנשמנו ב  $a$ , ונבדוק האם  $k - a$  מוכל ב  $hash$ ,

• אם  $k - a$  מוכל, נחזיר  $true$ ,

• אחרת, נכניס את  $a$  ל- $hash$ , ונעבור לאיבר הבא.

אם עברנו על כל האיברים, נחזיר  $false$ , נשים לב שעבור כל איבר, אנחנו שואלים האם  $k - a$  שייך או מכניסים אותו, שלוקח  $O(1)$  בממוצע, לכן לעבור על כל האיברים במקרה הגרוע הוא  $O(n) = n \cdot O(1)$  בממוצע.

מ.ש.ל. ☺

5. צ"ל:  $\mathcal{H}$  היא אוניברסלית

הוכחה:

יהיו  $x, y$  שונים, נשים לב כי יש  $m^N$  פונקציות והן נבחרות באופן אחיד לכן אם נגדיר  $N$  שמחזיר את מספר הפונקציות שמקיימות תנאי נקבל כי

$$\mathbb{P}(h(x) = h(y)) = \frac{N(h(x) = h(y))}{m^N}$$

עתה נרצה לחשב את  $N(h(x) = h(y))$ , בשביל ש  $h(x) = h(y)$ , נבחר את הערך  $h(x)$ , לכך יש  $m$  אפשרויות, לאחר מכן נצטרך לבחור את הערכים לכל  $t \neq x, y$  שיש לו  $m$  אפשרויות, ויש  $N - 2$ ,  $t$  כאלה לכן

$$N(h(x) = h(y)) = m \cdot m^{N-2} = m^{N-1}$$

לכן

$$\mathbb{P}(h(x) = h(y)) = \frac{N(h(x) = h(y))}{m^N} = \frac{m^{N-1}}{m^N} = \frac{1}{m} \leq \frac{1}{m}$$

כלומר  $\mathcal{H}$  היא אוניברסלית כי היא מקיימת את התנאי הנדרש לאוניברסליות

מ.ש.ל. ☺