תרגיל:

יהי $X = \{x_1, \dots, x_k\}$ קבוצת אותיות של מקור בדיד ותהי

פונקציית ההסתברות של X:

$$P_X(x_1) = p_1 \quad \dots \quad P_X(x_k) = p_k \qquad 0 \le p_i \le 1.$$

תהי $\ell_Q(x_i)$ המילה הבינארית של x_i לכל $1 \le i \le k$

ויהי n_i אורך המילה של $\ell_Q(x_i)$.

(למשל אם $\ell_Q(x_1) = 001$ אז $n_1 = 3$ (אורך 3)

אם $\ell_Q(x_1) = 00110$ אז $n_1 = 5$ (אורך 5)

הוכיחו: אם

$$p_1 \ge p_2 \ge \dots \ge p_k$$

אז ותוחלת אורך המילה היא מינימלית אם

$$n_1 \le n_2 \le \dots \le n_k.$$

משפט עזר

יהיו $a,b,c,d \in \mathbb{R}$ מספרים ממשיים.

אם $a \geq b$ ו- $c \geq d$ אז $ac + bd \geq ad + bc$.

הוכחה:

$$a \geq b \Rightarrow (a-b) \geq 0$$

$$c \geq d \Rightarrow (c-d) \geq 0$$

לכן

$$(a-b)(c-d) \geq 0 \Rightarrow ac + bd - bc - ad \geq 0$$

$$\Rightarrow ac + bd \geq bc + ad$$

הוכחה:

צריך להוכיח כי התוחלת אורך ההצפנה $E_0 = n_1 p_1 + \dots + n_k p_k$ מינימלית.

נניח בשלילה שקיימת תמורה $\{p_{i_1}, \dots, p_{i_k}\}$

שעבורה התוחלת $E = n_1 p_{i_1} + \dots + n_k p_{i_k}$ מינימלית.

ללא הגבלת הכלליות נניח כי $P_{i_j} = P_1$.

הנחנו כי $P_1 \geq P_2 \geq \cdots \geq P_k$

ז"א $P_{i_{j-1}} \leq P_{i_j} \Longleftarrow P_{i_j} = P_1 = \max(P_1, \dots, P_k)$.

בנוסף, $n_{i_{j-1}} \leq n_{i_j} \Longleftarrow n_1 \leq n_2 \leq \cdots \leq n_k$.

לכן, בהביטוי של E:

$$E = n_1 P_1 + \cdots + n_{i_{j-1}} P_{i_{j-1}} + n_{i_j} P_{i_j} + \cdots + n_k P_k$$

לפי המשפט עזר למעלה:

$$n_{i_{j-1}} P_{i_{j-1}} + n_{i_j} P_{i_j} \geq n_{i_{j-1}} P_{i_j} + n_{i_j} P_{i_{j-1}}$$

לכן

$$E = n_1 P_1 + \cdots + n_{i_{j-1}} P_{i_{j-1}} + n_{i_j} P_{i_j} + \cdots + n_k P_k$$

$$\geq n_1 P_1 + \cdots + n_{i_{j-1}} P_{i_j} + n_{i_j} P_{i_{j-1}} + \cdots + n_k P_k =: E'$$

בסתירה לכך ש-E התוחלת המינימלית.

∎

$$\Sigma = \lambda_1 P_1 + \cdots + \lambda_{i-1} P_{i-1} + \lambda_i P_i + \cdots + \lambda_k P_k$$

$$\Sigma \lambda_1 P_1 + \cdots + \lambda_1 P_{i-1} + \lambda_i P_i + \cdots + \lambda_k P_k =: \Sigma'$$

(مسألة ٣، ص ١٥٥، الفصل ٢) لتكن Σ و Σ' كما أعلاه. أثبت أن

$$\Sigma = \lambda_1 P_1 + \cdots + \lambda_{i-1} P_{i-1} + \lambda_i P_i + \cdots + \lambda_k P_k$$

$$\lambda_{i-1} P_{i-1} + \lambda_i P_i \geq \lambda_{i-1} P_i + \lambda_i P_{i-1}$$

ثم استنتج أن Σ ليست أصغر من Σ' إلا إذا كان $\lambda_{i-1} = \lambda_i$.

٤. (مسألة ٤، ص ١٥٥، الفصل ٢) ليكن P مضلعًا محدبًا في $\mathbb{R}^2$ ذا رؤوس $P_1, \ldots, P_k$ مرتبة عكس عقارب الساعة، وليكن $\Sigma = \lambda_1 P_1 + \cdots + \lambda_k P_k$ تركيبًا محدبًا نقطيًا لها. أثبت أن $\Sigma \in P$ إذا وفقط إذا وُجدت أعداد $\mu_1, \ldots, \mu_k \geq 0$ بحيث $\mu_1 + \cdots + \mu_k = 1$ و

$$\lambda_i = \mu_1 + \cdots + \mu_i \quad \text{لكل } i = 1, \ldots, k$$

ثم برهن أن $\mu_1, \ldots, \mu_k$ وحيدة. ما الشرط الهندسي على P الذي يضمن أن $\mu_i > 0$ لكل i؟

---

٥. (مسألة ٥، ص ١٥٥، الفصل ٢) ليكن $\Sigma = \lambda_1 P_1 + \cdots + \lambda_k P_k$ تركيبًا محدبًا نقطيًا في $\mathbb{R}^n$، حيث $\lambda_i > 0$ لكل i و $\lambda_1 + \cdots + \lambda_k = 1$. نفترض أن $P_1, \ldots, P_k$ مرتبة بحيث

$$\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_k$$

(أ) أثبت أن Σ تقع على القطعة المستقيمة $[P_1, P_k]$ إذا وفقط إذا كان $\lambda_1 = 1$.

(ب) أثبت أن Σ تقع على حافة P إذا وفقط إذا وُجد $i \in \{1, \ldots, k-1\}$ بحيث $\lambda_1 + \cdots + \lambda_i = 1$.

(ج) أثبت أن Σ تقع في الداخل النسبي لـ P إذا وفقط إذا كان $\lambda_1 < 1$ و $\lambda_k < 1$.

(د) أثبت أن Σ تقع في الداخل النسبي لوجه F من P إذا وفقط إذا كان F هو المجموعة المحدبة لجميع P_i التي تحقق $\lambda_i = 0$.

---

٦. (مسألة ٦، ص ١٥٥، الفصل ٢) ليكن P مضلعًا محدبًا في $\mathbb{R}^2$ ذا رؤوس $P_1, \ldots, P_k$ مرتبة عكس عقارب الساعة، وليكن $\Sigma = \lambda_1 P_1 + \cdots + \lambda_k P_k$ تركيبًا محدبًا نقطيًا لها. أثبت أن $\Sigma \in P$ إذا وفقط إذا وُجدت أعداد $\mu_1, \ldots, \mu_k \geq 0$ بحيث $\mu_1 + \cdots + \mu_k = 1$ و

$$\lambda_i = \mu_1 + \cdots + \mu_i \quad \text{لكل } i = 1, \ldots, k$$

ثم برهن أن $\mu_1, \ldots, \mu_k$ وحيدة. ما الشرط الهندسي على P الذي يضمن أن $\mu_i > 0$ لكل i؟

(א) אליס שולחת לבוב הודעה.
אליס הצפינה את ההודעה באמצעות צופן
תמורה עם המפתח $k=(4\ 2\ 3\ 1)$
הטקסט המוצפן של ההודעה אשר בוב
מקבל הוא $y=$ DOOGKUCL.
חשבו את הטקסט לפני של ההודעה אשר
אליס שלחה.

(ב) יהי $k=(5,23)$. המפתח של צופן אפיני מעל
$\mathbb{Z}_{31}$. יהי $d_k(y)=ay+b$

הכלל המפענח של צופן האפיני הזה
לכל $y\in\mathbb{Z}_{31}$ ו-$a,b\in\mathbb{Z}_{31}$.

חשבו את a ואת b.

פתרון

נשתמש את התמורה הנתונה הבאה:

על בלוקים, והתמורה

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$$

לכן, התמורה ההפוכה היא:

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$$

$Y \in C$	D	O	O	G	K	U	C	L
$y \in \mathbb{Z}_{26}$	3	14	14	6	10	20	2	11
$x = d_\pi(y)$	6	14	14	3	11	20	2	10
$X \in P$	G	O	O	D	L	U	C	K

סעיף ב)

נתון: $k=(5,23)$ מפתח

של צופן אפיני. ז"א

$$e_k(x) = 5x+23 \mod \mathbb{Z}_{31}$$

הכלל מפענח מתקבל ע"י הפונקציית ההופכית של $e_k(x)$ ב-$\mathbb{Z}_{31}$:

$$y = 5x+23 \longrightarrow y-23 = 5x$$

$$\longrightarrow 5^{-1}(y-23) = x$$

לכן

$$d_k(y) = 5^{-1}(y-23) \mod 31$$

נחשב $-23 \mod 31$ ואת $5^{-1} \mod 31$.

$-23 \mod 31 \equiv 8$.

נניח כי $a = 5^{-1} \mod 31$. ז"א

$$= 25(y+8) \bmod 31$$

$$= 25y + 200 \bmod 31$$

$$= 25y + 16 \bmod 31$$

$$d_K(y) = ay + b \bmod 31 \qquad (a, 31) = 1$$

$$a = 25, \quad b = 16$$

$$d_K^{-1}(y) = 5^{-1}(y - 25) \bmod 31$$

$$5^{-1} \bmod 31 \equiv 25$$

$$5 \cdot 25 \equiv 125 \bmod 31 \equiv 1 \bmod 31$$

$$\vdots$$

$$5 \cdot 1 \equiv 5 \bmod 31$$

$$a \cdot 5 \equiv 1 \bmod 31$$