

# שיעור 9

## תורת שאנו

### 1.9. סודיות מושלמת

נתונה קריפטו-מערכת

$$(X, Y, K, E, D)$$

כאשר  $X$  הקבוצה של כל טקסטים גלויים האפשריים,  $Y$  הקבוצה של כל טקסטים מוצפנים האפשריים,  $K$  הקבוצה של כל המפתחות האפשריים,  $E$  הקבוצה של כל כללי מצפין האפשריים ו-  $D$  הקבוצה של כל כללי מפענה האפשריים.

אנחנו נתיחס לטקסטים גלויים

$$X = \{x_1, x_2, \dots, x_n\}$$

כמשתנה מקרי (מ"מ) בדיד, אשר ערכו שווה לתוצאה של בחרית טקסט גלי. כמו כן נתיחס למפתחות

$$K = \{k_1, k_2, \dots, k_m\}$$

כמשתנה מקרי בדיד אשר ערכו שווה למפתח הנבחר.

נסמן את הפונקציית הסתבותות של הטקסט גלי ב-

$$P_X(x_i) = P(X = x_i) .$$

כלומר  $P(X = x_i)$  מסמן את ההסתברות לבחור את הטקסט גלי  $x$  מתוך  $X$ .  
נסמן את הפונקציית הסתבותות של המפתחות ב-

$$P_K(k_i) = P(K = k_i) .$$

כלומר  $P(K = k_i)$  הוא ההסתברות לבחור את המפתח  $k_i$  מתוך  $K$ .

הтекסט מוצפן  $y = Y$  המתקבל באמצעות הטקסט גלי  $x = X$  הנבחר והמתפתח  $K = k$  הנבחר הוא גם משתנה מקרי בדיד שמנדר

$$Y(k) = \{e_k(x) \mid x \in X\} .$$

ז"א  $Y(k)$  מייצג את קבוצת כל הטקסטים המוצפנים האפשריים המתקבלים על ידי המפתח  $k \in K$ .  
לפי כן, ההסתברות ש-  $Y = y$  כאשר  $y$  מתקבל על ידי להצפין הטקסט גלי  $x$  באמצעות המפתח  $k$  היא

$$P(Y = y) = \sum_{k \in K} P(K = k) P(X = d_k(y)) . \quad (9.1)$$

ההסתברות מותנית  $P(Y = y | X = x)$ , כלומר ההסתברות לקבל הטקסט מוצפן  $y$  במידע כי הטקסט גלי  $x$  הוא, היא לבדוק ההסתברות לבחור מפתח מסוים  $k$  אשר באמצעותו מקבלים  $y$  על ידי להצפין  $x$  עם המפתח זה  $k$ .

$$P(Y = y | X = x) = \sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k) . \quad (9.2)$$

מכאן, לפי נוסחת בייס,  $P(X = x|Y = y) = \frac{P(Y = y|X = x)P(X = x)}{P(Y = y)}$ . נציב את המשוואת (9.1) ומשוואות (9.2) ונקבל את הביטוי

$$P(X = x|Y = y) = \frac{P(X = x) \sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k)}{\sum_{k \in K} P(K = k)P(X = d_k(y))}. \quad (9.3)$$

### דוגמה 9.1

נתונה קבוצת טקסט גליי  $X = \{a, b\}$  עם פונקציית הסתברות

$$P(X = a) = \frac{1}{4}, \quad P(X = b) = \frac{3}{4},$$

נתונה קבוצת מפתחות  $K = \{k_1, k_2, k_3\}$  עם פונקציית הסתברות

$$P(K = k_1) = \frac{1}{2}, \quad P(K = k_2) = P(K = k_3) = \frac{1}{4}.$$

ונתונה קבוצת טקסט מוצפן

$$Y = \{1, 2, 3, 4\}.$$

נניח כי הכלל מצפין מוגדר כך ש-

$$e_{k_1}(a) = 1, \quad e_{k_1}(b) = 2, \quad e_{k_2}(a) = 2, \quad e_{k_2}(b) = 3, \quad e_{k_3}(a) = 3, \quad e_{k_3}(b) = 4.$$

מצאו את  $P(X = x|Y = y)$  לכל  $x \in X$  ולכל  $y \in Y$

### פתרונות:

אפשר ליצוג את הкриpto-מערכת כמטריצה הצפנה:

		$X$	a	b
$K$		1	2	
$k_1$		2	3	
$k_2$				
$k_3$		3	4	

נחשב את הפונקציית ההסתברות של  $Y$ :

$$\begin{aligned} P(Y = 1) &= P(K = k_1)P(X = d_{k_1}(1)) + P(K = k_2)P(X = d_{k_2}(1)) + P(K = k_3)P(X = d_{k_3}(1)) \\ &= P(K = k_1)P(X = a) + P(K = k_2)P(X = \emptyset) + P(K = k_3)P(X = \emptyset) \\ &= \frac{1}{2} \cdot \frac{1}{4} + 0 + 0 \\ &= \frac{1}{8}. \end{aligned}$$

$$\begin{aligned}
P(Y=2) &= P(K=k_1)P(X=d_{k_1}(2)) + P(K=k_2)P(X=d_{k_2}(2)) + P(K=k_3)P(X=d_{k_3}(2)) \\
&= P(K=k_1)P(X=b) + P(K=k_2)P(X=a) + P(K=k_3) \cdot P(X=\emptyset) \\
&= \frac{1}{2} \cdot \frac{3}{4} + \frac{1}{4} \cdot \frac{1}{4} \\
&= \frac{7}{16}.
\end{aligned}$$

$$\begin{aligned}
P(Y=3) &= P(K=k_1)P(X=d_{k_1}(3)) + P(K=k_2)P(X=d_{k_2}(3)) + P(K=k_3)P(X=d_{k_3}(3)) \\
&= P(K=k_1) \cdot P(X=\emptyset) + P(K=k_2)P(X=b) + P(K=k_3) \cdot P(X=a) \\
&= \frac{1}{4} \cdot \frac{3}{4} + \frac{1}{4} \cdot \frac{1}{4} \\
&= \frac{1}{4}.
\end{aligned}$$

$$\begin{aligned}
P(Y=4) &= P(K=k_1)P(X=d_{k_1}(4)) + P(K=k_2)P(X=d_{k_2}(4)) + P(K=k_3)P(X=d_{k_3}(4)) \\
&= P(K=k_1) \cdot P(X=\emptyset) + P(K=k_2) \cdot P(X=\emptyset) + P(K=k_3) \cdot P(X=b) \\
&= \frac{1}{4} \cdot \frac{3}{4} \\
&= \frac{3}{16}.
\end{aligned}$$

$$\begin{aligned}
P(X=a|Y=1) &= \frac{P(Y=1|X=a)P(X=a)}{P(Y=1)} \\
&= \frac{P(Y=1|X=a) \left(\frac{1}{4}\right)}{\left(\frac{1}{8}\right)} \\
&= 2 \sum_{\substack{k \in K \\ a=d_k(1)}} P(K=k) \\
&= 2P(K=k_1) \\
&= 1.
\end{aligned}$$

$$\begin{aligned}
P(X=b|Y=1) &= \frac{P(Y=1|X=b)P(X=b)}{P(Y=1)} \\
&= \frac{P(Y=1|X=b) \left(\frac{3}{4}\right)}{\left(\frac{1}{8}\right)} \\
&= 6 \sum_{\substack{k \in K \\ b=d_k(1)}} P(K=k) \\
&= 6 \cdot 0 \\
&= 0.
\end{aligned}$$

$$\begin{aligned}
P(X = \text{a}|Y = 2) &= \frac{P(Y = 2|X = \text{a})P(X = \text{a})}{P(Y = 2)} \\
&= \frac{P(Y = 2|X = \text{a}) \left(\frac{1}{4}\right)}{\left(\frac{7}{16}\right)} \\
&= \frac{4}{7} \sum_{\substack{k \in K \\ \text{a} = d_k(2)}} P(K = k) \\
&= \frac{4}{7} P(K = k_2) \\
&= \frac{1}{7} .
\end{aligned}$$

$$\begin{aligned}
P(X = \text{b}|Y = 2) &= \frac{P(Y = 2|X = \text{b})P(X = \text{b})}{P(Y = 2)} \\
&= \frac{P(Y = 2|X = \text{b}) \left(\frac{3}{4}\right)}{\left(\frac{7}{16}\right)} \\
&= \frac{12}{7} \sum_{\substack{k \in K \\ \text{b} = d_k(2)}} P(K = k) \\
&= \frac{12}{7} P(K = k_1) \\
&= \frac{6}{7} .
\end{aligned}$$

$$\begin{aligned}
P(X = \text{a}|Y = 3) &= \frac{P(Y = 3|X = \text{a})P(X = \text{a})}{P(Y = 3)} \\
&= \frac{P(Y = 3|X = \text{a}) \left(\frac{1}{4}\right)}{\left(\frac{1}{4}\right)} \\
&= \sum_{\substack{k \in K \\ \text{a} = d_k(3)}} P(K = k) \\
&= P(K = k_3) \\
&= \frac{1}{4} .
\end{aligned}$$

$$\begin{aligned}
P(X = \text{b}|Y = 3) &= \frac{P(Y = 3|X = \text{b})P(X = \text{b})}{P(Y = 3)} \\
&= \frac{P(Y = 3|X = \text{b}) \left(\frac{3}{4}\right)}{\left(\frac{1}{4}\right)} \\
&= 3 \sum_{\substack{k \in K \\ \text{b} = d_k(3)}} P(K = k) \\
&= 3P(K = k_2) \\
&= \frac{3}{4} .
\end{aligned}$$

$$\begin{aligned}
 P(X = a|Y = 4) &= \frac{P(Y = 4|X = a)P(X = a)}{P(Y = 4)} \\
 &= \frac{P(Y = 4|X = a) \left(\frac{1}{4}\right)}{\left(\frac{3}{16}\right)} \\
 &= \frac{4}{3} \sum_{\substack{k \in K \\ a = d_k(4)}} P(K = k) \\
 &= \frac{4}{3} \cdot 0 \\
 &= 0 .
 \end{aligned}$$

$$\begin{aligned}
 P(X = b|Y = 4) &= \frac{P(Y = 4|X = b)P(X = b)}{P(Y = 4)} \\
 &= \frac{P(Y = 4|X = b) \left(\frac{3}{4}\right)}{\left(\frac{3}{16}\right)} \\
 &= 4 \sum_{\substack{k \in K \\ b = d_k(4)}} P(K = k) \\
 &= 4P(K = k_3) \\
 &= \frac{1}{4} \\
 &= 1 .
 \end{aligned}$$

### הגדרה 9.1 סודיות מושלמת

אומרים כי לקריפטו-מערכת יש סודיות מושלמת אם

$$P(X = x|Y = y) = P(X = x)$$

לכל  $x \in X, y \in Y$ .

ז"א הסתברות כי הטקסט גלי  $x = X$ , בידעה כי הטקסט מוצפן  $y = Y$  שווה רק להסתברות כי הטקסט גלי הוא  $x = X$  והבחירה של המפתח שבאמצעותו מתקבל הטקסט מוצפן  $y$  לא משפייע על הסתברות כי הטקסט גלי  $x = X$ .

### משפט 9.1 תנאי לסודיות מושלמת של צופן קיסר

אם לכל מפתח  $K \in K$  בצופן קיסר יש הסתברות שווה, כלומר

$$P(K = k) = \frac{1}{26} .$$

אז לצופן קיסר יש סודיות מושלמת.

**הוכחה:** תחילה נחשב את הסתברות  $P(Y = y)$  באמצעות (9.1). הקבוצה מפתחות בצופן קיסר היא

$$K = \{0, 1, \dots, 25\} = \mathbb{Z}_{26} .$$

לכן

$$P(Y = y) = \sum_{k \in \mathbb{Z}_{26}} P(K = k) P(X = d_k(y)) .$$

אם ההסתברות של כל מפתח שווה אז ולכן  $P(K = k) = \frac{1}{26}$

$$P(Y = y) = \frac{1}{26} \sum_{k \in \mathbb{Z}_{26}} P(X = d_k(y)) .$$

הכלל מצפין והכלל מפענה של צופן קיסר מוגדרים

$$e_k(x) = x + k \pmod{26}, \quad d_k(y) = y - k \pmod{26} .$$

כאשר  $k \in \mathbb{Z}_{26}$ . לכן  $P(X = d_k(y)) = P(X = y - k \pmod{26})$ . לפיכך

$$P(Y = y) = \frac{1}{26} \sum_{k \in \mathbb{Z}_{26}} P(X = y - k \pmod{26}) .$$

הסכום בצד הימין הוא רק סכום של  $P(X = k)$  מעל כל האיברים  $k \in \mathbb{Z}_{26}$ . לכן

$$P(Y = y) = \frac{1}{26} \sum_{k \in \mathbb{Z}_{26}} P(X = k) = \frac{1}{26} \cdot 1 = \frac{1}{26} .$$

כאשר בשווון השני השתמשנו בתכונת הנרמול של הפונקציה הסתברות של המ"מ  $X$ .

מצד שני, לפי (9.2),

$$P(Y = y|X = x) = \sum_{\substack{k \in \mathbb{Z}_{26} \\ x = d_k(y)}} P(K = k)$$

האילוץ על הסכום  $x = d_k(y)$  אומר ש-

$$x = k - y \pmod{26} \quad \Rightarrow \quad k = x + y \pmod{26} .$$

לכל  $X \in \mathcal{X}$  ולכל  $y \in \mathcal{Y}$  קיים רק מפתח אחד אשר מקיים תנאי זה. ז"א רק איבר אחד של הסכום נשאר ולפיכך

$$P(Y = y|X = x) = \sum_{\substack{k \in \mathbb{Z}_{26} \\ x = d_k(y)}} P(K = k) = P(K = y - x \pmod{26}) .$$

אם ההסתברות של כל מפתח שווה, קלומר אם  $P_K(k) = \frac{1}{26}$ forall  $k \in K$  אז

$$P(Y = y|X = x) = P(K = y - x \pmod{26}) = \frac{1}{26} .$$

לכן

$$P(Y = y) = \frac{1}{26} = P(Y = y|X = x)$$

ז"א לצופן קיסר יש סודיות מושלמת.

במילים פשוטות צופן קיסר אינו ניתן לפענה בתנאי שימושים בפתח מקורי חדש כל פעם שמצפינים אותן אחד של טקסט גלי.

## למה 9.1 תנאי חילופי לסודיות מושלמת

לפי נוסחת בייס אם לקריפטו-מערכת יש סודיות מושלמת אז מתקיים גם

$$P(Y = y | X = x) = P(Y = y). \quad (9.4)$$

## למה 9.2

נתונה קריפטו-מערכת בעלת סודיות מושלמת.

אם  $P(Y = y) > 0$  אז

**1** קיים לפחות מפתח אחד  $k \in K$  כך ש-

$$|K| \geq |Y|. \quad (2)$$

הוכחה:

**1** לפי (9.4)

$$P(Y = y | X = x) = P(Y = y) > 0 \quad (\#1)$$

נציב (9.2) בצד שמאל ונקבל

$$\sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k) = P(Y = y) > 0 \quad (\#2)$$

ז"א

$$\sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k) > 0 \quad (\#3)$$

לכן קיים לפחות מפתח אחד  $k$  עבורו  $x = d_k(y)$

ז"א קיים לפחות מפתח אחד  $k$  עבורו  $y = e_k(x)$

**2** לפי (#1) ו-(#3), לכל  $y \in Y$  קיים לפחות מפתח אחד  $k$  עבורו  $y = e_k(x)$ , לכן בהכרח

$$|K| \geq |Y|. \quad (\#4)$$

## משפט 9.2 משפט שאנו

נתונה קריפטו-מערכת  $(X, Y, K, E, D)$  כך ש-  
למערכת יש סודיות מושלמת אם ורק אם

**1** לכל  $x \in X$  ולכל  $y \in Y$  קיים מפתח  $k$  ייחיד עבורו  $y = e_k(x)$

$$P(K = k) = \frac{1}{|K|} \quad (2)$$

הוכחה:

1) נניח כי  $|K| = |Y|$ . קלומר

$$|\{e_k(x)|x \in X\}| = |K| .$$

ז"א לא קיימים שני מפתחות  $k_1 \neq k_2$  כך ש-  
 $e_{k_1}(x) = y = e_{k_2}(x)$   
 לכן לכל  $x \in X$  ולכל  $y \in Y$  קיים מפתח  $k$  יחיד עבורו  $y$

2) נסמן אורך של קבוצת מפתחות ב-  $n = |K|$ . נרשום את הקבוצת טקסטים גלויים כ-

$$X = \{x_i|1 \leq i \leq n\} .$$

נתון  $y \in Y$  קבוע. נמספר את המפתחות  $c - , k_1, k_2, \dots, k_n$  כך ש-  $y = e_{k_i}(x_i)$ . לפי נוסחת בייס

$$\begin{aligned} P(X = x_i|Y = y) &= \frac{P(Y = y|X = x_i)P(X = x_i)}{P(Y = y)} \\ &\stackrel{(9.2)}{=} \frac{P(K = k_i)P(X = x_i)}{P(Y = y)} \end{aligned}$$

אם ל מערכת יש סודיות מושלמת אז ( $P(X = x_i|Y = y) = P(X = x_i)$  לכן

$$P(X = x_i) = \frac{P(K = k_i)P(X = x_i)}{P(Y = y)} \Rightarrow P(K = k_i) = P(Y = y)$$

לכל  $1 \leq i \leq n$ . ז"א לכל מפתח יש הסתברות שווה

$$P(K = k_i) = \frac{1}{|K|} .$$



## 9.2 המושג של מידע

נניח נניח ש-  $X$  משתנה מקרי אשר יכול לקבל אחת מארבע אפשרויות:

$$X \in \{a, b, c, d\} .$$

$X$  ידוע לבוב ( $B$ ) אבל לא ידוע לאלייס ( $A$ ). כל שאלות ידעת הוא ש-  $X$  יכול להיות אחת האותיות  $\{a, b, c, d\}$  בהסתברות שווה. אנחנו אומרים כי לאלייס יש אי-זדאות על הערך של  $X$ . כדי שאלייס תמצא את הערך של  $X$  אליס שואלת סדרת שאלות בינהירות (שאלות כן/לא) לבוב כדי לקבל מידע על המ"מ  $X$  עד שהיא תדע את הערך של  $X$  עם אי-זדאות אפס.

אפשרות אחת לסדרת שאלות היא כך:

$$Q_1: \text{האם } X \in \{a, b\}$$

לפי התשובה אחר כך אליס שואלת

$$Q_2: \text{אם } X = a \text{ האם } X \in \{a, b\}$$

$$Q_3: \text{אחרת אם } X \notin \{a, b\}$$



הסדרה של שאלות בינהריות שמאפשרת לאليس למצוא את  $X$  ללא שופ אי-ודאות מותוארת בעץ-שאלות מעלה.  
מספר השאלות הבינהריות  $N_Q[X]$ , שנדרשות כדי למצוא  $X$  ללא אי-ודאות הוא  $2 = N_Q[X]$ .

כל שאלה היא בינהרית, כלומר התשובה היא כן או לא אנחנו מצפינים תשובה כן עם "1" ותשובה לא עם "0". לפי התשובות אנחנו מצפינים את האותיות כך:

$$a \rightarrow 11, \quad b \rightarrow 10, \quad c \rightarrow 01, \quad d \rightarrow 00.$$

מכיוון ששתי תשובות בינהריות נדרשות כדי למצוא את  $X$ , אנחנו אורמים כי נדרש שני ביטים (bits) של מידע נדרשים כדי למצוא את  $X$ .  
במילים אחרות, שתי ספרות בינהריות  $X = d_1d_2$  נדרשות כדי להצפין את  $X$ , שערכן הן התשובות לשתי שאלות בינהריות,  
לכן המידע המתקבל על מציאת הערך של  $X$  הוא 2 bit.

אליס הייתה יכולה לשנות את הסדרת שאלות שלה כך:

$$?X = a \text{ האם } Q'_1$$

רק אם התשובה היא "לא" אז היא צריכה לשאול שאלה נוספת נוספת:

$$?X = b \text{ האם } Q'_2$$

ורק אם התשובה היא "לא" אז היא צריכה לשאול שאלה נוספת נוספת:

$$?X = c \text{ האם } Q'_3$$

מספר השאלות הבינהריות הנדרשות למצוא את  $X$  תלוי על הערך של  $X$ :  $N_Q(b) = 2$ ,  $N_Q(a) = 1$  ו-  $N_Q(c) = N_Q(d) = 3$ .



$X$  הוא משתנה מקרי בדיד ולכן בהינתן מערכת שאלות, ( $N_Q(X)$ ) הוא פונקציה של משתנה מקרי בדיד, ולכן  $N_Q[X]$  הוא בעצם משתנה מקרי בדיד.

כעת נשאל שאלה. נניח כי אין מעוניינות למצוא מערכת שאלות  $Q$ , אשר נותנת את מספר השאלות המומוצע המינימלי. כלומר, כיצד נמצא מערכת שאלות  $N_Q[X]$  עבורה התוחלת

$$E[N_Q[X]] = \sum_{k \in X} P_X(k) N_Q[k]$$

תהייה מינימלית.

לפנינו שונעה על שאלה זו זאת נתן דוגמה.

נתון המשתנה מקרי  $X = \{a, b, c, d\}$  בעל פונקציית ההסתברות

$$P_X(a) = \frac{1}{2}, \quad P_X(b) = \frac{1}{4}, \quad P_X(c) = P_X(d) = \frac{1}{8}.$$

עבור ההצפנה הראשונה  $Q$ , מספר השאלות הנדרשות כדי למצוא כל ערך של  $X$  הוא 2, אך אז התוחלת תהייה

$$E_Q[N_Q[X]] = \frac{1}{2}(2) + \frac{1}{4}(2) + \frac{1}{8}(2) + \frac{1}{8}(2) = 2,$$

כלומר תוחלת המספר השאלות הוא 2.

עבור ההצפנה השנייה  $Q'$  תוחלת מספר השאלות היא

$$E[N_{Q'}[X]] = \frac{1}{2}(1) + \frac{1}{4}(2) + \frac{1}{8}(3) + \frac{1}{8}(3) = \frac{7}{4}.$$

אשר פחותה מהתוחלת עבור ההצפנה  $Q$ . מכאן אנחנו רואים כי יש קשר בין התוחלת של מספר השאלות הבינאריות לבין מערכת השאלות שאנו שואלים.

אליס שואלת סדרת שאלות ולכל שאלה נשים ערך ביןאיי 0 אם התשובה לא ו- 1 אם התשובה כן. כך אנחנו נשים לכל ערך של  $X$  מספר ביןאיי  $d_1 \dots d_k$  המורכב מספרות ביןאיריות 0, 1. טרנספורמציה כזו בין ערכיים של  $X$  לבין מספרים ביןאירים נקראת הצפנה. שימו לב כי אורך ההצפנה  $[X]_Q[\ell]$  של כל ערך של  $X$  שווה למספר השאלות ביןאיירות הנדרשות כדי למצוא את  $X$  ללא אי-זדאות:

$$\ell_Q[X] = N_Q[X].$$

## משפט 9.3

יהי  $X = \{x_1, x_2, \dots, x_k\}$  משתנה מקרי בדיד כך ש-

$$p_1 \geq p_2 \geq \dots \geq p_k$$

כאשר  $(X = x_i) \ell_Q(x_i) = n_i$ , כלומר  $x_i$  מוצפן על ידי מספר בינארי עם  $n_i$  ספרות בינאריות. התוחלת המינימלית מתקבלת על ידי ההצפנה שמיימת

$$n_1 \leq n_2 \leq \dots \leq n_k .$$

**הוכחה:** נניח בשלילה שקיימת תמורה  $\{p_1, \dots, p_k\}$  של  $\{p_{i_1}, \dots, p_{i_k}\}$ . כך שהתווחלת

$$E = n_1 p_{i_1} + \dots + n_{j-1} p_{i_{j-1}} + n_j p_{i_j} + \dots + n_k p_{i_k} .$$

היא מינימלית. ללא הגבלת הכלליות נניח כי  $p_{i_j} = p_1$ . אז

$$E = n_1 p_{i_1} + \dots + n_{j-1} p_{i_{j-1}} + n_j p_1 + \dots + n_k p_{i_k} .$$

בchnerה  $p_1 \leq p_{i_{j-1}}$ . לכן אם נחליף  $p_1$  עם  $n_{j-1}$  קיבל את התוחלת החדשה

$$E' = n_1 p_{i_1} + \dots + n_{j-1} p_1 + n_j p_{i_{j-1}} + \dots + n_k p_{i_k} .$$

$E' < E$  בסתרה לכך כי  $E$  התוחלת המינימלית המתקבלת עבור התמורה  $(p_{i_1}, \dots, p_{i_k})$ .

■

במשפט הבא אנחנו נוכיח כי אפשר לגוזר ביטוי בשביל התוחלת המינימלית באמצעות הפונקציית הסתברות של המשתנה מקרי  $X$  בלבד. נסמן

$$p_x = P_X(X = x) .$$

אנחנו ראיינו לעלה כי אורך ההצפנה של  $x = X$  בהצפנה אופטימלית  $Q^*$  הוא פונקציה של הסתברות  $p_x$ , כלומר

$$\ell_{Q^*}(x) = f(p_x) . \quad (\#)$$

## משפט 9.4 אנטרופיה של שאנו

נתון משתנה מקרי  $X$  בעל פונקציית הסתברות  $P_X(x)$ . התוחלת המינימלית של אורך ההצפנה של  $X$  מסומן ב-  $H[X]$  ונתונה על ידי הנוסחה

$$H[X] = - \sum_{x \in X} P_X(x) \log_2 P_X(x) .$$

נקרא **האנטרופיה** של  $X$ .

**הוכחה:** נניח כי  $Z = Y \cap X$ , כאשר  $Y, Z$  משתנים מקרים בלתי תלויים. לפי משועאה (#):

$$\ell_Q(x) = f(p_x) .$$

$$H[X] = \sum p_x \ell_Q(x) = \sum p_x f(p_x) .$$

תהיינה  $P_Z(z)$  ו-  $P_Y(y)$  פונקציות הסתברות של  $Z$  ושל  $Y$  בהתאם. נסמן  $p_z = P_Z(z)$  ו-  $p_y = P_Y(y)$ .

מכיוון ש-  $Y$  ו-  $Z$  משתנים בלתי תלויים אז

$$P(X = Y \cap Z) = P_Y(y)P_Z(z) = p_y p_z .$$

נשים לב שידיעה של  $Y$  לא נותנת שום מידע על הערך של  $Z$ , לכן

$$\ell_Q[Y \cap Z] = \ell_Q[Y] + \ell_Q[Z] .$$

לפיכך

$$H[X] = \sum p_x \ell_Q(x) = \sum p_y p_z [\ell_Q(y) + \ell_Q(z)]$$

מכאן

$$H[X] = \sum p_y p_z f(p_y p_z) = \sum p_y p_z [f(p_y) + f(p_z)]$$

$$f(p_y p_z) = f(p_y) + f(p_z) .$$

$$f(p) = C \log(p)$$

כעת נניח כי יש לנו משתנה מקרי  $X = \{a, b\}$  בעל פונקציית ההסתברות  $P_X(a) = \frac{1}{2}, P_X(b) = \frac{1}{2}$ . ההצפנה של  $X$  צריכה ספרה אחת, לכן  $f(\frac{1}{2}) = 1$  ונקבל  $f(Q^*(a)) = f(Q^*(b)) = 1$ .

■

## 9.3 הגדרה של מידע

### הגדרה 9.2 מידע של מאורע (שאנו)

נתון משתנה מקרי  $X$ . המידע של ערך מסוים של  $X$  מסומן  $I_X(x)$  ומוגדר להיות

$$I(X = x) = \log_2 \left( \frac{1}{P_X(x)} \right) = -\log_2(P_X(x))$$

כאשר  $P_X(x)$  פונקציית ההסתברות של המשתנה מקרי  $X$ .

### דוגמה 9.2 המידע המתקיים על קבלת תוצאה של הטלת מטבע

נטיל מטבע הוגנת ונגידר משתנה מקרי  $X$  להיות התוצאה.  $X$  מקבל את הערכים

$$X = \{H, T\} .$$

מצאו את המידע של המאורע  $X = H$

**פתרון:**

$$P(X = H) = \frac{1}{2} .$$

$$I(X = H) = -\log_2 \left( \frac{1}{2} \right) = 1 .$$

כלומר על קבלת התוצאה "H" אנחנו מקבלים ביט אחד של מידע.

**הסביר:**

במקום הסימנים " $H$ " ו- " $T$ " בשביל המ"מ  $X$  ניתן להצפין את הערכים האפשריים בספרות בינהיות "0" או "1".  
כלומר

ערך של $X$	הצפנה בספרות בינהיות
0	$H$
1	$T$

ז"א כדי להצפין את הערכים של  $X$  אנחנו צריכים ספרה בינהיות אחת:

$$d_1 \in \{0, 1\}.$$

אשר יכול להציג את הערכים 0 או 1.  
■ ספרה בינהיות אחת נדרשת להצפין את הערך של  $X$  שכן המידע של ערך כלשהו של  $X$  הוא 1 (בית אחד).

### דוגמה 9.3 שליפת קלף מחבילת קלפים תיינית

בניסוי שליפת קלף אחד מחבילת קלפים תיינית. נגדיר משתנה מקרי  $X$  להיות הסוג של הקלף (תלון, עלה, לב או יהלום). חשבו את את המידע של המאורע שללפנו קלף מסווג לב.

**פתרון:**

הסתברות שלוף קלף של הסוג לב מחבילת קלפים סטנדרטית היא

$$P(X = \heartsuit) = \frac{13}{52} = \frac{1}{4}.$$

לכן

$$I(X = \heartsuit) = -\log_2 \left( \frac{1}{4} \right) = 2 \text{ bits}$$

**הסבר:**

יש 4 ערכים אפשריים של  $X$ :

$$X = \{\spadesuit, \clubsuit, \heartsuit, \diamondsuit\}$$

כל ספרה בינהיות מחזיקה 2 ערכים אפשריים: 0 או 1 שכן ידרש שתי ספרות בינהיות כדי להצפין את ה-4 ערכים האפשריים של  $X$ :

$$d_1 d_2, \quad d_1, d_2 \in \{0, 1\}.$$

ההצפנה עצמה מתוארת בטבלה למטה:

ערך של $X$	הצפנה בספרות בינהיות
00	$\spadesuit$
01	$\clubsuit$
10	$\heartsuit$
11	$\diamondsuit$

אורך המספר  $d_1 d_2$  הוא 2 שכן המידע של המשתנה מקרי  $X$  הוא 2 bits (שני ביטים).  
■

## דוגמה 9.4 שליפת קלף מחבילת קלפים תיינית



בניסוי שליפת קלף אחד מחבילת קלפים תיינית. מצאו את המידע המתkeletal אם הקלף נשלף.

תמונה	מספרים	צורה
		עליה
		תלון
		לב
		ילהום

**פתרון:**

יהי  $X$  המ"מ שמסמן את הקלף הנשלף. ההסתברות לשלוフ הקלף שלוש מסוג לב מחבילת קלפים סטנדרטית היא

$$P\left(X = \begin{array}{|c|} \hline 3 \\ \hline \spadesuit \\ \hline \end{array}\right) = \frac{1}{52}.$$

לכן

$$I\left(X = \begin{array}{|c|} \hline 3 \\ \hline \spadesuit \\ \hline \end{array}\right) = -\log_2\left(\frac{1}{52}\right) = 5.7 \text{ bits}$$

**הסביר:**

כדי להציג את כל הערכים האפשריים של  $X$  כמספר בינארי, נדרש רצף סיביות אשר מקבל לפחות 52 ערכים שונים. מספר בעל 5 סיביות לא מספיק מסיבה שיש לו רק  $2^5 = 32$  ערכים שונים. אבל מספר בעל 6 סיביות נותן  $2^6 = 64$  ערכים שונים, שמספיק להציג את כל הערכים האפשריים של  $X$ .

$$d_1 d_2 d_3 d_4 d_5 d_6$$

האורך של מספר זה הוא 6 ולכן הוא מחייב 6 bits של מידע. לכל סיבית יש 2 ערכים אפשריים ולכן 64 ערכים שונים בסה"כ.

נשים לב שרק 52 מתוך ה-64 צירופים נדרשים כדי להציג את הערכים האפשריים של  $X$  וכך אפשר להוריד את ■ החלק של הערכים המיוטרים. הקבוצת המספריים הנשארת מכילה 5.7 bits של מידע.

ככל שההסתברות של מאורע יותר קטנה אז המידע המתkeletal יותר גבוהה.

כלומר, ככל שהמידע של מאורע יותר גבוהה אז ההסתברות שלו יותר קטנה

**דוגמה 9.5 (המשך של דוגמה 9.1)**

$$\begin{aligned}
 H(X) &= -P(X = a) \log_2 P(X = a) - P(X = b) \log_2 P(X = b) \\
 &= -\frac{1}{4} \log_2 \left(\frac{1}{4}\right) - \frac{3}{4} \log_2 \left(\frac{3}{4}\right) \\
 &= -\frac{1}{4}(-2) - \frac{3}{4} (\log_2 3 - \log_2 4) \\
 &= \frac{1}{2} - \frac{3}{4} \log_2 3 + \frac{6}{4} \\
 &= 2 - \frac{3}{4} \log_2 3 \\
 &\approx 0.81 .
 \end{aligned}$$

$$\begin{aligned}
 H(K) &= -P(K = k_1) \log_2 P(K = k_1) - P(K = k_2) \log_2 P(K = k_2) - P(K = k_3) \log_2 P(K = k_3) \\
 &= -\frac{1}{2} \log_2 \left(\frac{1}{2}\right) - \frac{1}{4} \log_2 \left(\frac{1}{4}\right) - \frac{1}{4} \log_2 \left(\frac{1}{4}\right) \\
 &= -\frac{1}{2}(-1) - \frac{1}{4}(-2) - \frac{1}{4}(-2) \\
 &= 1 + \frac{1}{2} + \frac{1}{2} \\
 &= \frac{3}{2} .
 \end{aligned}$$

$$\begin{aligned}
 H(Y) &= -P(Y = 1) \log_2 P(Y = 1) - P(Y = 2) \log_2 P(Y = 2) - P(Y = 3) \log_2 P(Y = 3) \\
 &\quad - P(Y = 4) \log_2 P(Y = 4) \\
 &= -\frac{1}{8} \log_2 \left(\frac{1}{8}\right) - \frac{7}{16} \log_2 \left(\frac{7}{16}\right) - \frac{1}{4} \log_2 \left(\frac{1}{4}\right) - \frac{3}{16} \log_2 \left(\frac{3}{16}\right) \\
 &= \frac{27}{8} - \frac{7}{16} \log_2 7 - \frac{3}{16} \log_2 3 \\
 &\approx 1.85 .
 \end{aligned}$$

■

במקרה שההתברות של כל תוצאה שווה, כלומר

$$P(X = x_i) = \frac{1}{|X|} = \frac{1}{N}$$

אז

$$H(X) = -\sum_{i=1}^N \frac{1}{N} \log_2 \left(\frac{1}{N}\right) = \frac{1}{N} \sum_{i=1}^N \log_2 N = \log_2 N .$$

לכן

$$N = 2^{H(X)} .$$

ניתן להוכיח ש-  $\log_2 N$  הוא הערך המקסימלי האפשרי של  $H(X)$ .

## משפט 9.5

נתון מ"מ בדיד  $X$  אשר מקבל  $N$  ערכים שונים

$$X = \{x_1, \dots, x_N\}$$

בנסיבות שווה, קלומר

$$P(X = x_i) = \frac{1}{N}$$

از האנתרופיה מקבלת ערך מקסימלי שנייה על ידי

$$H_{\max}(X) = \log_2 N .$$

ערך זה הוא הערך המקסימלי האפשרי של האנתרופיה.

## דוגמה 9.6 אנתרופיה בהטלת מטבע

נניח כי נטיל מטבע עם הסתברות  $p \leq 1$  (0) לקבל "H". יהיו  $X$  משתה מקרי ששויה לתוצאה הניסוי. מצאו את האנתרופיה של המ"מ מקרי  $X$ .

**פתרון:**

נסמן  $\{0, 1\}$  כאשר  $0 = X$  מסמן תוצאה  $H$  ו-  $1 = X$  מסמן תוצאה  $T$ . פונקציית ההסתברות היא

$$P_X(0) = p , \quad P_X(1) = 1 - p .$$

לכן המידע של המאורע לקבל תוצאה  $H$  הוא

$$I(X = 0) = -\log_2(P_X(0)) = -\log_2(p)$$

והמידע של המאורע לקבל תוצאה  $H$  הוא

$$I(X = 1) = -\log_2(P_X(1)) = -\log_2(1 - p)$$

נשים לב שגם המטבע הוגנת או  $p = \frac{1}{2}$  ו-  $I(X = 0) = I(X = 1) = 1$  ו-  $p = \frac{1}{2}$ -cut נחשב את האנתרופיה של  $X$ :

$$H(X) = -P_X(0) \log_2 P_X(0) - P_X(1) \log_2 P_X(1) = -p \log_2 p - (1 - p) \log_2(1 - p) .$$

נרשום את האנתרופיה כפונקציה של ההסתברות  $p$ :

$$H(X) = -p \log_2 p - (1 - p) \log_2(1 - p) =: h(p).$$

ל-  $p = \frac{1}{2}$  יש נקודת מקסימום ב-

$$h'(p) = -\frac{1}{\ln 2} - \log_2 p + \frac{1}{\ln 2} + \log_2(1 - p) = -\log_2 p + \log_2(1 - p) = \log_2 \left(\frac{1}{p} - 1\right) \stackrel{!}{=} 0 \Rightarrow p = \frac{1}{2} .$$

ז"א הערך המקסימלי של האנתרופיה מתקיים כאשר לכל הערכים של  $X$  יש הסתברות שווה, ואכן

$$h(p = \frac{1}{2}) = -\frac{1}{2} \log_2 \frac{1}{2} - \frac{1}{2} \log_2 \frac{1}{2} = \log_2 2 = 1 .$$



**דוגמה 9.7**

בניסוי הטלת מטבח לא מאוזנת, ההסתברות לקבל תוצאה  $H$  היא  $\frac{1}{1024} = p$ . מצאו את האנטרופיה של  $X$ .

**פתרון:**

נסמן  $T$  כאשר  $X = 0$  מסמן תוצאה  $H$  ו-  $X = 1$  מסמן תוצאה  $T$ .

$$I(X = 0) = -\log_2 \frac{1}{1024} = 10 \text{ bits}, \quad I(X = 1) = -\log_2 (1 - p) = -\log_2 \frac{1023}{1024} = 0.00141 \text{ bits}.$$

לפי זה

$$H(X) = -p \log_2 p - (1 - p) \log_2 (1 - p) = -\frac{1}{1024} \log_2 \frac{1}{1024} - \frac{1023}{1024} \log_2 \frac{1023}{1024} = 0.0112 \text{ bits}.$$

המשמעות של התשובה לדוגמה הקודמת היא כך. נניח שנטיל אותה מטבח ללא מאוזנת 100,000 פעמים. בכדי להציג את כל התוצאות נדרש מספר בינארי עם 100,000 סיביות, כאשר כל ספרה נותנת התוצאה של ניסוי אחד. זו א"א  $10^5$  bits של מידע נדרש כדי להציג את כל התוצאות.

מצד שני מצאנו כי התוחלת של המידע המתkeletal לניסוי (כמוות מידע פר ניסוי) הוא 0.0112 bit פר ניסוי. במילימט לאחרות, ב-  $10^5$  ניסויים רק 1120 bit של מידע נדרש בממוצע כדי להציג את כל התוצאות של רצף ההצלחות.

**9.4 הצפנה האפמן**

סביר הצפנה האפמן בעזרת הדוגמה הבאה. נתון הטקסט גלי

$$X = \{a, b, c, d\}$$

ונניח כי פונקציית ההסתברות של  $X$  נתונה בטבלה הבאה:

$I(X = x_i) = -\log_2(p_i)$	$p_i = P_X(x_i)$	בחירה אותן של $X$
1.58 bit	$\frac{1}{3}$	a
1 bit	$\frac{1}{2}$	b
3.58 bit	$\frac{1}{12}$	c
3.58 bit	$\frac{1}{12}$	d

נשאל את השאלה: כמה ביטים של מידע נדרש כדי להציג (בסיביות) רצף של 1000 אותיות של טקסט גלי  $X$ ?

יש 4 אותיות ב-  $X$ , כולן 4 ערכים אפשריים של המ"מ בדיד  $X$ . לפיכך נדרש רצף של 2 סיביות כדי להציג טקסט גלי של TWO אחד בהצפנה סיביות קבועה. דוגמה:

בחירה אות של $X$	הצפנה
00	a
01	b
10	c
11	d

וזא להצפיןתו אחד של הטקסט גלי  $X$  נדרש bit 2. לכן להצפין רצף אותיות של טקסט גלי נדרש  $2 \times 1000 = 2000$  bit, כולל 2000 סיביות.

האנטרופיה של  $X$  היא

$$H(X) = -p_1 \log_2(p_1) - p_2 \log_2(p_2) - p_3 \log_2(p_3) - p_4 \log_2(p_4) = 1.62581 \text{ bit} .$$

וזא לכל ניסוי המידע המומוצע הנדרש כדי להצפיןתו אחד של טקסט גלי הוא bit 1.62581. לכן המידע המומוצע הנדרש כדי להצפין רצף אותיות של טקסט גלי הוא

$$1000 \times 1.62581 = 1625.81 \text{ bit} .$$

לכן, רצף סיביות של אורך 1626 ב ממוצע יהיה מספיק כדי להעביר את ההודעה.

כעת נבנה הצפנה של הטקסט גלי על ידי האלגוריתם של האפמן.

### שלב 1)

	c	d	a	b
	1	1	4	6

### שלב 2)

	c	d	a	b
	1	1	4	6
	0	1		
	2	4	6	



### שלב 3)

	cd	a	b
	2	4	6
	0	1	
	6	6	



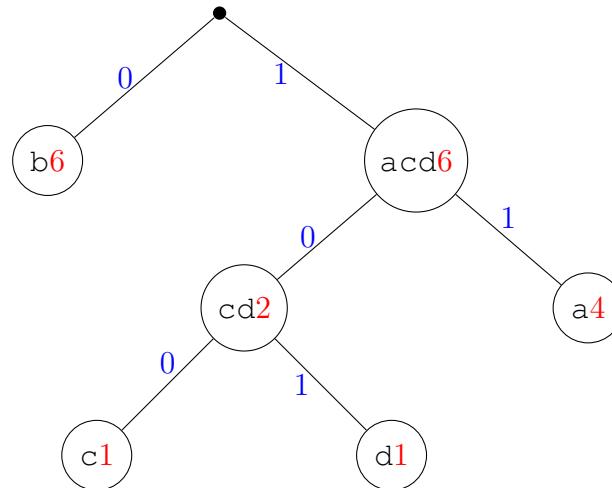
שלב 4)

שלב 5)

	acd	b
6		6
0		1
	12	



שלב 6)



בסוף של התהליך האותיות של הטקסט גלי יהיו בעלים של העץ והחצפנה ניתנת על ידי הריצף סיביות על הענפים במסלול מהנקודות הראשית של העץ עד העלה בו רשום האות בשאלת.

בחירה אות של $x_i \in X$	הצפנת האפסן
11	a
100	b
110	c
101	d

**דוגמה 9.8**

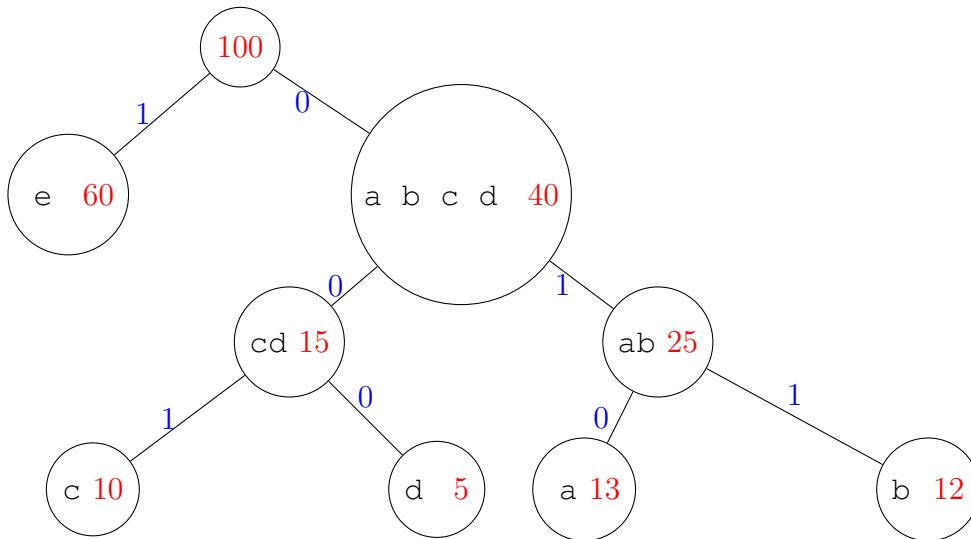
נתון הטקסט גליי הבא

$$X = \{a, b, c, d, e\}$$

והפונקציית הסתברות

$$P(X = a) = \frac{13}{100} = 0.13, \quad P(X = b) = \frac{3}{25} = \frac{12}{100} = 0.12, \quad P(X = c) = \frac{1}{10} = \frac{10}{100} = 0.1,$$

$$P(X = d) = \frac{1}{20} = \frac{5}{100} = 0.05, \quad P(X = e) = \frac{3}{5} = \frac{60}{100} = 0.6.$$

מצאו את העץ הצפנה וההצפנה האפמן של כל תו של  $X$ .**פתרונות:**

בחירה האפמן $x_i \in X$	בחירה אוטומטית
010	a
011	b
001	c
000	d
1	e

פורמלי הבחירה האפמן מוגדרת לפי ההגדרה הבאה:

**הגדרה 9.3 הבחירה האפמן**נתון משתנה מקרי  $X$ . נגידר הבחירה האפמן של  $X$  להיות הפונקציה (כלל מיפוי)

$$f : X \rightarrow \{0, 1\}^*$$

כasher  $\{0, 1\}^*$  קבוצת רצפים של סיביות סופיים.

נתון רצף מאורעות  $x_1, \dots, x_n$ . נגיד

$$f(x_1 \dots x_n) = f(x_1) || \dots || f(x_n)$$

כאשר " $||$ " מסמן שרשור (concatenation).

#### הגדלה 9.4 תוחלת האורך של הצפנת האפמן

נתונה הצפנת האפמן  $f$ . תוחלת האורך של ההצפנה מוגדרת

$$l(f) = \sum_{x \in X} P(X = x) |f(x)| .$$

#### משפט 9.6 אי-שוויון האפמן

נתון קבוצת אובייקטים של טקסט גליי  $X$  והצפנת האפמן  $f$ . נניח כי  $l(f)$  תוחלת האורך של ההצפנה ו-  $H(X)$  האנטרופיה של הטקסט גליי. מתקיים

$$H(X) \leq l(f) \leq H(X) + 1 .$$

#### דוגמה 9.9 (המשך דוגמה 9.8)

נתון הטקסט גליי הבא

$$X = \{a, b, c, d, e\}$$

והפונקציית הסתברות

$$P(X = a) = \frac{13}{100} = 0.13 , \quad P(X = b) = \frac{3}{25} = 0.12 , \quad P(X = c) = \frac{1}{10} = 0.1 , \quad P(X = d) = \frac{1}{20} = 0.05 ,$$

$$P(X = e) = \frac{3}{5} = 0.6 .$$

1) מצאו את תוחלת האורך של ההצפנת האפמן.

2) מצאו את האנטרופיה.

3) הוכחו כי אי-שוויון האפמן של ההצפנה שמצאתם בדוגמה 9.8 לעלה מותקיים.

**פתרונות:**

**סעיף 1)**

$$\begin{aligned} l(f) &= \frac{5}{100} \cdot 3 + \frac{10}{100} \cdot 3 + \frac{12}{100} \cdot 3 + \frac{13}{100} \cdot 3 + \frac{60}{100} \cdot 1 \\ &= \frac{15 + 30 + 36 + 30 + 60}{100} \\ &= \frac{180}{100} \\ &= 1.8 \end{aligned}$$

**סעיף 2**

$$\begin{aligned}
 H(X) &= -P(X=a)\log_2 P(X=a) - P(X=b)\log_2 P(X=b) - P(X=c)\log_2 P(X=c) \\
 &\quad - P(X=d)\log_2 P(X=d) - P(X=e)\log_2 P(X=e) \\
 &= 1.74018 .
 \end{aligned}$$

**סעיף 3**  $H(X) + 1 = 1.84018$ ,  $H(X) = 1.74018$  לכן  $l(f) = 1.8$ .

$$H(X) \leq l(f) \leq H(X) + 1$$

מתקיים.



## 9.5 תכונות של אנטרופיה

### הגדרה 9.5 פונקציה קעורה

פונקציה ממשית  $f(x)$  נקראת **פונקציה קעורה** בתחום  $I$  אם

$$f\left(\frac{x_1+x_2}{2}\right) \geq \frac{f(x_1)+f(x_2)}{2}$$

לכל  $x_1, x_2 \in I$

פונקציה ממשית  $f(x)$  נקראת **פונקציה קעורה ממש** בתחום  $I$  אם

$$f\left(\frac{x_1+x_2}{2}\right) > \frac{f(x_1)+f(x_2)}{2}$$

לכל  $x_1, x_2 \in I$

### משפט 9.7 אי-שוויון ינסן

נניח כי  $f$  פונקציה רציפה וקעורה ממש בקטע  $I$ . נתון מספרים ממשיים  $a_1, \dots, a_n > 0$  כך ש-  $\sum_{i=1}^n a_i = 1$ .

$$\sum_{i=1}^n a_i f(x_i) \leq f\left(\sum_{i=1}^n a_i x_i\right)$$

אם  $x_1 = \dots = x_n$  ורק אם  $\sum_{i=1}^n a_i f(x_i) = f\left(\sum_{i=1}^n a_i x_i\right)$   $x \in I$ .

### משפט 9.8

יהי

$$X = \{x_1, \dots, x_n\}$$

משתנה מקרי בדיד בעל פונקציית הסתברות

$$P_X(x_1) = p_1, \dots, P_X(x_n) = p_n,$$

$1 \leq i \leq n$  לכל  $0 < p_i \leq 1$

$$H(X) \leq \log_2 n$$

אם ורק אם

$$p_i = \frac{1}{n}$$

לכל  $n$

**הוכחה:** לפי אי-שוויון ינסן:

$$\begin{aligned} H(X) &= -\sum_{i=1}^n p_i \log_2 p_i \\ &= \sum_{i=1}^n p_i \log_2 \left( \frac{1}{p_i} \right) \\ &\leq \log_2 \left( \sum_{i=1}^n p_i \cdot \frac{1}{p_i} \right) \\ &= \log_2 \left( \sum_{i=1}^n 1 \right) \\ &= \log_2 n. \end{aligned}$$

בנוסח  $n$  אם ורק אם  $H(X) = \log_2 n$

## משפט 9.9

יהי  $X = \{x_1, \dots, x_m\}$  משתנה מקרי בדיד בעל פונקציית הסתברות

$$P_X(x_1) = p_1, \dots, P_X(x_m) = p_m,$$

יהי  $Y = \{y_1, \dots, y_n\}$  משתנה מקרי בדיד בעל פונקציית הסתברות

$$P_Y(y_1) = q_1, \dots, P_Y(y_n) = q_n,$$

$1 \leq i \leq n$  לכל  $0 < q_i \leq 1$

$$H(X, Y) \leq H(X) + H(Y)$$

אם ורק אם  $X$  ו- $Y$  בלתי תלויים.

**הוכחה: (\*להעשרה בלבד)**

פונקציית הסתברות של  $X$  היא  $P_X(x_i) = p_i$  ופונקציית הסתברות של  $X$  היא  $P_Y(y_i) = q_i$ . נגידר הפוקנציית הסתברות של המשתנה מקרי דו-ממדי:

$$r_{ij} = P(X = x_i, Y = y_j).$$

אז הפונקציית הסתבותות שולית של  $X$  היא

$$p_i = \sum_{j=1}^n r_{ij} , \quad \forall 1 \leq i \leq m$$

והפונקציית הסתבותות שולית של  $Y$  היא

$$q_j = \sum_{i=1}^m r_{ij} , \quad \forall 1 \leq j \leq n .$$

מכאן

$$\begin{aligned} H(X) + H(Y) &= - \sum_{i=1}^m p_i \log_2 p_i - \sum_{j=1}^n q_j \log_2 q_j \\ &= - \sum_{i=1}^m \left( \sum_{j=1}^n r_{ij} \right) \log_2 p_i - \sum_{j=1}^n \left( \sum_{i=1}^m r_{ij} \right) \log_2 q_j \\ &= - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 p_i - \sum_{j=1}^n \sum_{i=1}^m r_{ij} \log_2 q_j \\ &= - \sum_{i=1}^m \sum_{j=1}^n r_{ij} (\log_2 p_i + \log_2 q_j) \\ &= - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 (p_i q_j) . \end{aligned}$$

מצד שני:

$$H(X, Y) = - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 r_{ij} = \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 \frac{1}{r_{ij}} .$$

לכן

$$\begin{aligned} H(X, Y) - H(X) - H(Y) &= \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 \frac{1}{r_{ij}} + \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 (p_i q_j) \\ &= \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 \left( \frac{p_i q_j}{r_{ij}} \right) \\ &\leq \log_2 \left( \sum_{i=1}^m \sum_{j=1}^n p_i q_j \right) \quad \text{(אי-שוויון ינסן)} \\ &= \log_2 1 \\ &= 0 . \end{aligned}$$

לכן

$$H(X, Y) - H(X) - H(Y) \leq 0 \quad \Rightarrow \quad H(X, Y) \leq H(X) + H(Y) .$$



## הגדלה 9.6 אנטרופיה מותנית

יהיו  $X, Y$  משתנים מקריים בדים. נגיד

$$H(X|Y = y) = - \sum_{x \in X} P(X = x|Y = y) \log_2 P(X = x|Y = y) .$$

**האנטרופיה מותנית** תסומן  $H(X|y)$  ותוגדר הממוצע המשוקל של  $H(X|Y = y)$  ביחס להסתירות  $P(Y = y)$

$$H(X|Y) = - \sum_{y \in Y} \sum_{x \in X} P(Y = y) P(X = x|Y = y) \log_2 P(X = x|Y = y) .$$

האנטרופיה המותנית  $H(X|Y)$  מכמתת המידע הממוצע של המ"מ  $X$  המועברת אשר לא מוגלה באמצעות  $Y$ .

## משפט 9.10

$$H(X, Y) = H(Y) + H(X|Y) .$$

הוכחה: (\*להעשרה בלבד)

$$\begin{aligned} H(X|Y) &= - \sum_{i=1}^m \sum_{j=1}^n P(Y = y_j) P(X = x_i|Y = y_j) \log_2 P(X = x_i|Y = y_j) \\ &= - \sum_{i=1}^m \sum_{j=1}^n P(X = x_i \cap Y = y_j) \log_2 \frac{P(X = x_i \cap Y = y_j)}{P(Y = y_j)} \\ &= - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 \frac{r_{ij}}{q_j} . \end{aligned}$$

מצד שני

$$H(Y) = - \sum_{j=1}^n q_j \log_2 q_j = - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 q_j$$

$$H(X, Y) = - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 r_{ij} .$$

-1

לכן

$$\begin{aligned}
 H(Y) + H(X|Y) &= -\sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 \frac{r_{ij}}{q_j} - \sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 q_j \\
 &= -\sum_{i=1}^m \sum_{j=1}^n r_{ij} \left( \log_2 \frac{r_{ij}}{q_j} + \log_2 q_j \right) \\
 &= -\sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 \left( \frac{r_{ij}}{q_j} \cdot q_j \right) \\
 &= -\sum_{i=1}^m \sum_{j=1}^n r_{ij} \log_2 r_{ij} \\
 &= H(X, Y) .
 \end{aligned}$$

**משפט 9.11**

$$H(X|Y) \leq H(X)$$

אם ורק אם  $X$  ו-  $Y$  משתנים מקיימים בלתי-תלויים.

**הוכחה: (\*להעשרה בלבד)**

לפי משפט 9.9,  $H(X, Y) \leq H(X) + H(Y)$ . נציב משפט 9.10 ונקבל

$$H(Y) + H(X|Y) \leq H(X) + H(Y) \Rightarrow H(X|Y) \leq H(X) .$$

בנוסף לפי משפט 9.9,  $H(X, Y) = H(X) + H(Y)$ , לכן

$$H(X|Y) = H(X)$$

אם ורק אם  $X, Y$  משתנים בלתי-תלויים.

## 9.6 משפט האנתרופיה לקריפטו-מערכת

**משפט 9.12 משפט האנתרופיה לקריפטו-מערכת**

תהי  $(P, C, K, E, D)$  קריפטו-מערכת. אז

$$H(K|C) = H(K) + H(P) - H(C) .$$

**הוכחה: (\*להעשרה בלבד)**

לפי משפט 9.10,

$$H(K, P, C) = H(K, P) + H(C|K, P) .$$

בגלל שהכל מציין  $y = e_k(x)$  הוא פונקציה חד-חד-ערכית, אז המפתח והטקסט גלי קבועים את הטקסט מוצפן בדרך ייחודית. ז"א

$$H(C|K, P) = 0 .$$

לכן

$$H(K, P, C) = H(K, P) . \quad (*1)$$

המשתנים מקרים  $K$  ו-  $P$  בלתי-תלויים. לכן לפי משפט 9.9  $H(K, P) = H(K) + H(P)$  ולפיכך נקבל

$$H(K, P, C) = H(K) + H(P) . \quad (*2)$$

באותה מידת, לפי משפט 9.10,

$$H(K, P, C) = H(K, C) + H(P|K, C) . \quad (*3)$$

מכיוון שהכל מפענה  $x = d_k(y)$  פונקציה חד-חד ערכית, אז המפתח והטקסט מוצפן קובעים את הטקסט גלו' בדרך ייחודית. לכן

$$H(P|K, C) = 0 .$$

ומכאן

$$H(K, P, C) = H(K, C) . \quad (*4)$$

לפי משפט 9.10.  $H(K, C) = H(C) + H(K|C)$

$$\begin{aligned} H(K|C) &= H(K, C) - H(C) \\ &= H(K, P, C) - H(C) \quad (\text{לפי } *4) \\ &= H(K) + H(P) - H(C) \quad (\text{לפי } *2) \end{aligned} \quad (9.5)$$

כנדרש.



### דוגמה 9.10 (המשך של דוגמה 9.1 והמשך של דוגמה 9.5)

עבור דוגמה 9.1 מצאו את  $H(K|C)$  ובדקו כי הערך המתתקבל תואם עם  $H(C)$ .

**פתרונות:**

בדוגמה 9.5 מצאנו כי  $H(C) = 1.85$  ו-  $H(K) = 1.5$ ,  $H(P) = 0.81$   
 $H(K|C) = H(K) + H(P) - H(C) = 0.46$

כעת נחשב את  $H(K|C)$  בעזרת התוצאות של דוגמה 9.1:

$$P(K = k_1|C = 1) = \frac{P(C = 1|K = k_1) P(K = k_1)}{P(C = 1)} = \frac{\left(\frac{1}{4}\right) \left(\frac{1}{2}\right)}{\left(\frac{1}{8}\right)} = 1 ,$$

$$P(K = k_2|C = 1) = \frac{P(C = 1|K = k_2) P(K = k_2)}{P(C = 1)} = \frac{0 \left(\frac{1}{4}\right)}{\left(\frac{1}{8}\right)} = 0 ,$$

$$P(K = k_3|C = 1) = \frac{P(C = 1|K = k_3) P(K = k_3)}{P(C = 1)} = \frac{0 \left(\frac{1}{4}\right)}{\left(\frac{1}{8}\right)} = 0 ,$$

$$P(K = k_1|C = 2) = \frac{P(C = 2|K = k_1) P(K = k_1)}{P(C = 2)} = \frac{\left(\frac{3}{4}\right) \left(\frac{1}{2}\right)}{\left(\frac{7}{16}\right)} = \frac{6}{7} ,$$

$$P(K = k_2|C = 2) = \frac{P(C = 2|K = k_2) P(K = k_2)}{P(C = 2)} = \frac{\left(\frac{1}{4}\right) \left(\frac{1}{4}\right)}{\left(\frac{7}{16}\right)} = \frac{1}{7} ,$$

$$P(K = k_3|C = 2) = \frac{P(C = 2|K = k_3) P(K = k_3)}{P(C = 2)} = \frac{0 \left(\frac{1}{4}\right)}{\left(\frac{7}{16}\right)} = 0 ,$$

$$P(K = k_1|C = 3) = \frac{P(C = 3|K = k_1) P(K = k_1)}{P(C = 3)} = \frac{(0) \left(\frac{1}{2}\right)}{\left(\frac{1}{4}\right)} = 0 ,$$

$$P(K = k_2|C = 3) = \frac{P(C = 3|K = k_2) P(K = k_2)}{P(C = 3)} = \frac{\left(\frac{3}{4}\right) \left(\frac{1}{4}\right)}{\left(\frac{1}{4}\right)} = \frac{3}{4} ,$$

$$P(K = k_3|C = 3) = \frac{P(C = 3|K = k_3) P(K = k_3)}{P(C = 3)} = \frac{\left(\frac{1}{4}\right) \left(\frac{1}{4}\right)}{\left(\frac{1}{4}\right)} = \frac{1}{4} ,$$

$$P(K = k_1|C = 4) = \frac{P(C = 4|K = k_1) P(K = k_1)}{P(C = 4)} = \frac{(0) \left(\frac{1}{2}\right)}{\left(\frac{3}{16}\right)} = 0 ,$$

$$P(K = k_2|C = 4) = \frac{P(C = 4|K = k_2) P(K = k_2)}{P(C = 4)} = \frac{0 \left(\frac{1}{4}\right)}{\left(\frac{3}{16}\right)} = 0 ,$$

$$P(K = k_3|C = 4) = \frac{P(C = 4|K = k_3) P(K = k_3)}{P(C = 4)} = \frac{\left(\frac{3}{4}\right) \left(\frac{1}{4}\right)}{\left(\frac{3}{16}\right)} = 1 .$$

מבחן

$$\begin{aligned}
 H(K|C) &= - \sum_{y=1}^4 \sum_{k \in \{k_1, k_2, k_3, k_4\}} P(C=y)P(K=k|C=y) \log_2 P(K=k|C=y) \\
 &= - P_C(1)P_{K|C}(k_1|1) \log_2 P_{K|C}(k_1|1) - P_C(2)P_{K|C}(k_1|2) \log_2 P_{K|C}(k_1|2) \\
 &\quad - P_C(3)P_{K|C}(k_1|3) \log_2 P_{K|C}(k_1|3) - P_C(4)P_{K|C}(k_1|4) \log_2 P_{K|C}(k_1|4) \\
 &\quad - P_C(1)P_{K|C}(k_2|1) \log_2 P_{K|C}(k_2|1) - P_C(2)P_{K|C}(k_2|2) \log_2 P_{K|C}(k_2|2) \\
 &\quad - P_C(3)P_{K|C}(k_2|3) \log_2 P_{K|C}(k_2|3) - P_C(4)P_{K|C}(k_2|4) \log_2 P_{K|C}(k_2|4) \\
 &\quad - P_C(1)P_{K|C}(k_3|1) \log_2 P_{K|C}(k_3|1) - P_C(2)P_{K|C}(k_3|2) \log_2 P_{K|C}(k_3|2) \\
 &\quad - P_C(3)P_{K|C}(k_3|3) \log_2 P_{K|C}(k_3|3) - P_C(4)P_{K|C}(k_3|4) \log_2 P_{K|C}(k_3|4) \\
 &= - \frac{1}{8} \log_2 1 - \frac{7}{16} \cdot \frac{6}{7} \log_2 \frac{6}{7} - \frac{1}{4} \cdot 0 \log_2 0 - \frac{3}{16} \cdot 0 \log_2 0 \\
 &\quad - \frac{1}{8} 0 \cdot \log_2 0 - \frac{7}{16} \cdot \frac{1}{7} \log_2 \frac{1}{7} - \frac{1}{4} \cdot \frac{3}{4} \log_2 \frac{3}{4} - \frac{3}{16} \cdot 0 \log_2 0 \\
 &\quad - \frac{1}{8} \cdot 0 \log_2 0 - \frac{7}{16} \cdot 0 \log_2 0 - \frac{1}{4} \cdot \frac{1}{4} \log_2 \frac{1}{4} - \frac{3}{16} \cdot 1 \cdot \log_2 1 \\
 &= 0.461676 .
 \end{aligned}$$

הרי

$$H(K|C) = 0.46 = H(K) + H(P) - H(C)$$

כנדרש.

