שיעור 7
תורת שאנון

7.1 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 מפענח האפשריים.

אנחנו נתייחס לטקסטים גלויים
$$X = \{x_1, x_2, \ldots, x_n\}$$
כמשתנה מקרי (מ"מ) בדיד, אשר ערכו שווה לתוצאה של בחרית טקסט גלוי. כמו כן נתייחס למפתחות
$$K = \{k_1, k_2, \ldots, k_m\}$$
כמשתנה מקרי בדיד אשר ערכו שווה למפתח הנבחר.

נסמן את הפונקציית הסתברות של הטקסט גלוי ב-
$$P_X(x_i) = P(X = x_i) \ .$$
כלומר $P(X = x_i)$ מסמן את ההסתברות לבחור את הטקסט גלוי x מתוך X.
נסמן את הפונקציית הסתברות 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.

הטקסט מוצפן $Y = y$ המתקבל באמצעות הטקסט גלוי $X = x$ הנבחר והמתפח $K = k$ הנבחר הוא גם משתנה מקרי בדיד שמוגדר
$$Y(k) = \left\{ e_k(x) \middle| \ x \in X \right\} \ .$$
ז"א $Y(k)$ מייצג את קבוצת כל הטקסטעם המוצפנים האפשריים המתקבלים על ידי המפתח $k \in K$.
לפיכך, ההסתרות ש- $Y = y$ כאשר y מתקבל על ידי להצפין הטקסט גלוי x באמצעות המפתח k היא
$$P(Y = y) = \sum_{k \in K} P(K = k) P\left(X = d_k(y)\right) \ . \tag{7.1}$$

ההסתברות מותנית $P(Y = y|X = x)$, כלומר ההסתברות לקבל הטקסט מוצפן y בידיעה כי הטקסט גלוי הוא x, היא בדיוק ההסתברות לבחור מפתח מסוים k אשר באמצעותו מקבלים y על ידי להצפין x עם המפתח זה k.
$$P(Y = y|X = x) = \sum_{\substack{k \in K \\ x = d_k(y)}} P(K = k) \ . \tag{7.2}$$

מכאן, לפי נוסחת בייס, $P(X=x|Y=y)=\dfrac{P(Y=y|X=x)P(X=x)}{P(Y=y)}$. נציב את משוואת (7.1) ומשוואות (7.2) ונקבל את הביטוי

$$P(X=x|Y=y)=\frac{P(X=x)\displaystyle\sum_{\substack{k\in K\\ x=d_k(y)}}P(K=k)}{\displaystyle\sum_{k\in K}P(K=k)P\left(X=d_k(y)\right)}\ . \tag{7.3}$$

דוגמה 7.1

נתונה קבוצת טקסט גלוי $X=\{\mathtt{a},\mathtt{b}\}$ עם פונקצית הסתברות

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

נתונה קבוצת מפתחות $K=\{k_1,k_2,k_3\}$ עם פונקצית 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-

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

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

פתרון:

אפשר לייצג את הקריפטו-מערכת כמטריצת הצפנה:

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

נחשב את הפונקצית ההסתברות של Y:

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

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

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

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

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

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

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

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

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

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

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

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

■

הגדרה 7.1 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 ההסתברות כי הטקסט גלוי $X=x$, בידיעה כי הטקסט מוצפן $Y=y$ שווה רק להסתברות כי הטקסט גלוי הוא $X=x$ והבחירה של המפתח שבאמצעותו מתקבל הטקסט מוצפן y לא משפיע על ההסתברות כי הטקסט גלוי $X=x$.

משפט 7.1 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 ההסתברות $P(Y=y)$ באמצעות (7.1). הקבוצת מפתחות בצופן קיסר היא

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

לכן

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

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

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

הכלל מצפין והכלל מפענח של צופן קיסר מוגדרים

$$e_k(x)=x+k \mod 26 \ , \qquad d_k(y)=y-k \mod 26 \ .$$

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

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

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

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

כאשר בשוויון השני השתמשנו בתכונת הנרמול של הפונקצית הסתברות של המ"מ X.

מצד שני, לפי (7.2),

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

האילוץ על הסכום $x=d_k(y)$ אומר ש-

$$x=k-y \mod 26 \qquad \Rightarrow \qquad k=x+y \mod 26 \ .$$

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

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

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

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

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 לפענח בתנאי שמשתמשים במפתח מקרי חדש כל פעם שמצפינים אות אחד של טקסט גלוי.

למה 7.1 תנאי חילופי לסודיות מושלמת

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

$$P(Y=y|X=x)=P(Y=y)\ . \tag{7.4}$$

למה 7.2

נתונה קריפטו-מערכת בעלת סודיות מושלמת.

אם $P(Y=y)>0$ אז

1) קיים לפחות מפתח אחד $k\in K$ כך ש- $e_k(x)=y$

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

הוכחה:

1) לפי (7.4),

$$P(Y=y|X=x)=P(Y=y)>0 \tag{\#1}$$

נציב (7.2) בצד שמאל ונקבל

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

ז"א

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

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

$$|K|\geq|Y|\ . \tag{\#4}$$

■

משפט 7.2 משפט שאנון

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

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

2) לכל מפתח יש הסתברות שווה, כלומר $P(K=k)=\dfrac{1}{|K|}$.

הוכחה:

1) נניח כי $|Y|=|K|$. כלומר
$$|\{e_k(x)|x\in X\}|=|K| \ .$$
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 $e_k(x)=y$.

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 כ- $k_1,k_2,\ldots,k_n$ כך ש- $e_{k_i}(x_i)=y$. לפי נוסחת בייס,
$$\begin{aligned}P(X=x_i|Y=y)=&\frac{P(Y=y|X=x_i)P(X=x_i)}{P(Y=y)}\\ \stackrel{\text{לפי (7.2)}}{=}&\frac{P(K=k_i)P(X=x_i)}{P(Y=y)}\end{aligned}$$
אם למערכת יש סודיות מושלמת אז $P(X=x_i|Y=y)=P(X=x_i)$ לכן
$$P(X=x_i)=\frac{P(K=k_i)P(X=x_i)}{P(Y=y)} \quad\Rightarrow\quad P(K=k_i)=P(Y=y)$$
לכל $1\leq i\leq n$. ז"א לכל מפתח יש הסתברות שווה
$$P(K=k_i)=\frac{1}{|K|} \ .$$
■

7.2 המושג של מידע

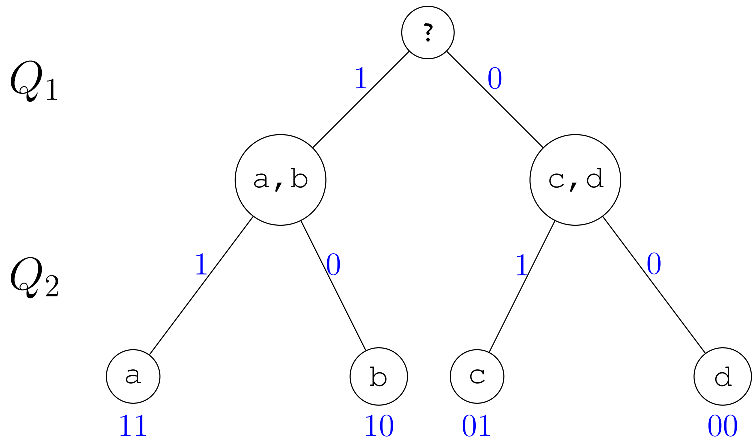
נניח נניח ש- X משתנה מקרי אשר יכול לקבל אחת מארבע אפשריות:
$$X\in\{\mathrm{a},\mathrm{b},\mathrm{c},\mathrm{a}\} \ .$$
X ידוע לבוב (B) אבל לא ידוע לאליס (A). כל שאליס יודעת הוא ש- X יכול להיות אחת האותיות $\{\mathrm{a},\mathrm{b},\mathrm{c},\mathrm{a}\}$ בהסתברות שווה. אנחנו אומרים כי לאליס יש אי-ודאות על הערך של X. כדי שאליס תמצא את הערך של X אליס שואלת סדרת שאלות בינאריות (שאלות כן/לא) לבוב כדי לקבל מידע על המ"מ X עד שהיא תדע את הערך של X עם אי-ודאות אפס.

אפשרות אחת לסדרת שאלות היא כך:

Q_1: האם $X\in\{\mathrm{a},\mathrm{b}\}$?

לפי התשובה אחר כך אליס שואלת

Q_2: אם $X\in\{\mathrm{a},\mathrm{b}\}$ האם $X=\mathrm{a}$?
אחרת אם $X\notin\{\mathrm{a},\mathrm{b}\}$ האם $X=\mathrm{c}$?



הסדרה של שאלות בינאריות שמאפשרת לאליס למצוא את X ללא שום אי-ודאות מתוארת בעץ-שאלות למעלה.
מספר השאלות הבינאריות $N_Q[X]$, שנדרשות כדי למצוא X ללא אי-ודאות הוא $N_Q[X]=2$.

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

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

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

אליס הייתה יכולה לשנות את הסדרת שאלות שלה כך:

Q'_1 האם $X=\mathtt{a}$?

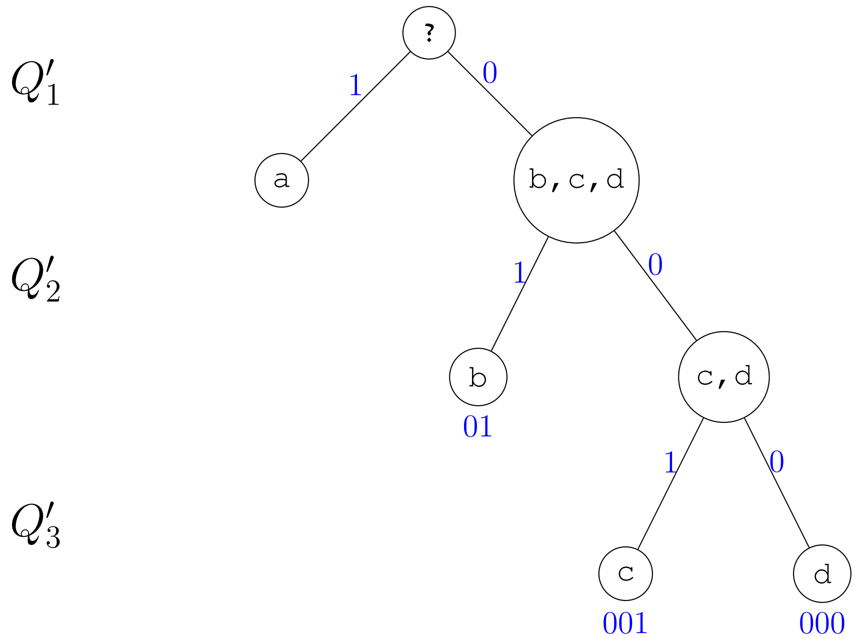
רק אם התשובה היא "לא" אז היא צריכה לשאול שאלה נוספת:

Q'_2 האם $X=\mathtt{b}$?

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

Q'_3 האם $X=\mathtt{c}$?

מספר השאלות הביניאריות הנדרשות למצוא את X תלוי על הערך של X: $N_Q(\mathtt{a})=1$, $N_Q(\mathtt{b})=2$ או $N_Q(\mathtt{c})=N_Q(\mathtt{d})=3$.



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

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

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

תהיה מינימלית.

לפני שנענה על שאלה הזאת נתן דוגמה.

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

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

עבור ההצפנה הראשונה Q, מספר השאלות הנדרשות כדי למצוא כל ערך של X הוא $N_Q[k]=2$, לכן אז התוחלת תהיה

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

כלומר תוחלת המספר השאלות הוא 2.
עבור ההצפנה השנייה Q' תוחלת מספר השאלות היא

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

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

אליס שואלת סדרת שאלות ולכל שאלה נשים ערך בינארי 0 אם התשובה לא ו- 1 אם התשובה כן. כך אנחנו נשים לכל ערך של X מספר בינארי $d_1\ldots d_k$ המורכב מספרות בינאריות $d_i=0,1$. טרנספורמציה כזרת בין ערכים של X לבין מספרים בינארים נקראת הצפנה. שימו לב כי אורך ההצפנה $\ell_Q[X]$ של כל ערך של X שווה למספר השאלות בינאריות הנדרשותת כדי למצוא את X ללא אי-ודאות:

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

משפט 7.3

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

$$p_1 \geq p_2 \geq \cdots \geq p_k$$

כאשר $p_i = P\left(X=x_i\right)$. תהי $\ell_Q[X]$ הצפנה כך ש- $\ell_Q(x_i)=n_i$, כלומר x_i מוצפן על ידי מספר בינארי עם n_i ספרות ביניאריות. התוחלת המינימלית מתקבלת על ידי ההצפנה שמקיימת

$$n_1 \leq n_2 \leq \ldots \leq n_k \ .$$

הוכחה: נניח בשלילה שקיימת תמורה $\{p_{i_1},\ldots,p_{i_k}\}$ של $\{p_1,\ldots,p_k\}$. כך שהתוחלת

$$E=n_1p_{i_1}+\ldots+n_{j-1}p_{i_{j-1}}+n_jp_{i_j}+\ldots+n_kp_{i_k} \ .$$

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

$$E=n_1p_{i_1}+\ldots+n_{j-1}p_{i_{j-1}}+n_jp_1+\ldots+n_kp_{i_k} \ .$$

$p_1=\max(p_1,\ldots,p_n)$ אז בהכרח $p_{i_{j-1}} \leq 1$. לכן אם נחליף p_1 עם שכנו נקבל את התוחלת החדשה

$$E'=n_1p_{i_1}+\ldots+n_{j-1}p_1+n_jp_{i_{j-1}}+\ldots+n_kp_{i_k} \ .$$

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

■

במשפט הבא אנחנו נוכיח כי אפשר לגזור ביטוי בשביל התוחלת המינימלית באמצעות הפונקצית ההסתברות של המשתנה מקרי X בלבד. נסמן

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

אנחנו ראינו למעלה כי אורך ההצפנה של $X=x$ בהצפנה אופטימלית Q^* הוא פונקציה של ההסתברות p_x, כלומר

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

משפט 7.4 אנטרופיה של שאנון

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

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

$H[X]$ נקרא **האנטרופיה** של X.

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

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

$$H[X]=\sum p_x\ell_Q(x)=\sum p_xf\left(p_x\right) \ .$$

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

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

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

מכאן

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

לכל p_y ו- p_z. לכן

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

ז"א $f(p)=C\log(p)$.

כעת נניח כי יש לנו משתנה מקרי $X=\{a,b\}$ בעל פונקצית ההסתברות $P_X(b)=\frac{1}{2},\ P_X(a)=\frac{1}{2}$. ההצפנה של X צריכה ספרה אחת, לכן $\ell_{Q^*}(a)=\ell_{Q^*}(b)=1$. לכן נשים $f\left(\frac{1}{2}\right)=1$ ונקבל $f(p)=-\log_2(p)$.

■

7.3 הגדרה של מידע

הגדרה 7.2 מידע של מאורע (שאנון)

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

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

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

דוגמה 7.2 המידע המתקבל על קבלת תוצאה של הטלת מטבע

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

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

מצאו את המידע של המאורע $X=H$.

פתרון:

$P(X=H)=\frac{1}{2}$. לכן

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

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

הסבר:

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

ערך של X	הצפנה בספרות בינאריות
H	0
T	1

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

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

אשר יכול להחזיק את הערכים 0 או 1.
ספרה ביניארית אחת נדרשת להצפין את הערך של X לכן המידע של ערך כלשהו של X הוא 1 bit (ביט אחד). ■

דוגמה 7.3 שליפת קלף מחבילת קלפים תיקנית

בניסוי שליפת קלף אחד מחבילת קלפים תיקנית. נגדיר משתנה מקרי X להיות הסוג של הקלף (תלתן, עלה, לב או יהלום). חשבו את את המידע של המאורע ששלפנו קלף מסוג לב.

פתרון:
ההסתברות לשלוף 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 בינארית מחזיקה 2 ערכים אפשריים: 0 או 1 לכן ידרש שתי ספרות בינאריות כדי להצפין את ה-4 ערכים האפשריים של X:

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

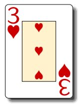
ההצפנה עצמה מתוארת בטבלא למטה:

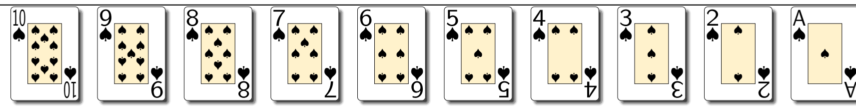
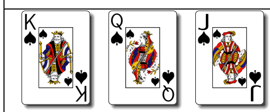
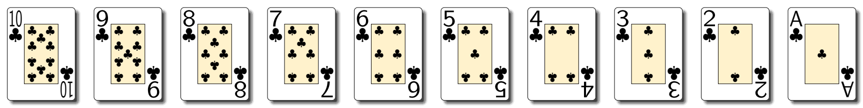
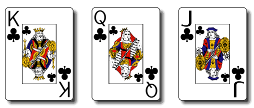
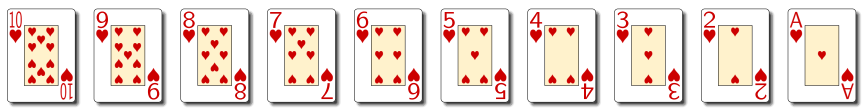
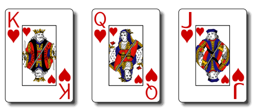
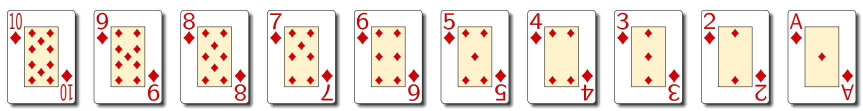
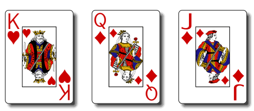
ערך של X	הצפנה בספרות בינאריות
$\spadesuit$	00
$\clubsuit$	01
$\heartsuit$	10
$\diamondsuit$	11

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

■

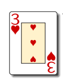
דוגמה 7.4 שליפת קלף מחבילת קלפים תיקנית

בניסוי שליפת קלף אחד מחבילת קלפים תיקנית. מצאו את המידע המתקבל אם הקלף  נשלף.

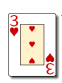
צורה	מספרים	תמונות
עלה		
תלתן		
לב		
יהלום		

פתרון:

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

$$P\left(X = \right.$$

$$\left.\right) = \frac{1}{52} \ .$$

לכן

$$I\left(X = \right.$$

$$\left.\right) = -\log_2\left(\frac{1}{52}\right) = 5.7 \text{ bits}$$

הסבר:

כדי להצפין 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 להצפין 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 מחזיק 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 להצפין את הערכים האפשריים של X לכן אפשר להוריד את החלק של הערכים המיותרים. הקבוצת המספרים הנשארת מכילה 5.7 bits של מידע. ■

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

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

דוגמה 7.5 (המשך של דוגמה 7.1)

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

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

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

■

במקרה שההסתברות 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 7.5

נתון מ"מ בדיד X אשר מקבל N ערכים שונים

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

בהסתברות שווה, כלומר

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

אז האנטרופיה מקבלת ערך מקסימלי שניתנת על ידי

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

ערך זה הוא הערך המקסימלי האפשרי של האנטרופיה.

דוגמה 7.6 אנטרופיה בהטלת מטבע

נניח כי נטיל מטבע עם הסתברות p ($0 \leq p \leq 1$) לקבל "H". יהי X משתה מקרי ששווה לתוצאת הניסוי. מצאו את האנטרופיה של המ"מ מקרי X.

פתרון:

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

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

לכן המידע של המאורע לקבל תוצאת H הוא

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

והמידע של המאורע לקבל תוצאת H הוא

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

נשים לב שאם המטבע הוגנת אז $p = \frac{1}{2}$ ו- $I(X = 0) = I(X = 1) = 1$.
כעת נחשב את האנטרופיה 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 האנטרופיה כפונקציה של ההסתברות p:

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

ל- $h(p)$ יש נקודת מקסימום ב- $p = \frac{1}{2}$:

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

ז"א הערך המקסימלי של האנטרופיה מתקבל כאשר לכל הערכים של X יש הסתברות שווה, $P_X(0) = P_X(1) = \frac{1}{2}$.
אכן

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

■

דוגמה 7.7

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

פתרון:
נסמן $X=\{0,1\}$, כאשר $X=0$ מסמן תוצאת H ו- $X=1$ מסמן תוצאת T.

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

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 מטבע הלא מאוזנת $100,000$ פעמים. בכדי להצפין את כל התוצאות נדרש מספר בינארי עם $100,000$ סיביות, כאשר כל ספרה נותנת התוצאה של ניסוי אחד. ז"א 10^5 bits של מידע נדרש כדי להצפין את כל התוצאות.

מצד שני מצאנו כי התוחלת של המידע המתקבל לניסוי (כמות מידע פר ניסוי) הוא 0.0112 bit פר ניסוי. במילים אחרות, ב- 10^5 ניסוים רק 1120 bit של מידע נדרש בממוצע כדי להצפין את כל התוצאות של רצף ההטלות.

7.4 הצפנת האפמן

נסביר הצפנת האפמן בעזרת הדוגמה הבאה. נתון הטקסט גלוי

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

ונניח כי פונקצית ההסתברות של X נתונה בטבלא הבאה:

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

נשאל את השאלה: כמה ביטים של מידע נדרשים כדי להצפין (בסיביות) רצף של 1000 אותיות של טקסט גלוי X?

יש 4 אותיות ב- X, כלומר 4 ערכים אפשריים של המ"מ בדיד X. לפיכך נדרש רצף של 2 סיביות כדי להצפין טקסט גלוי של תו אחד בהצפנת סיביות קבועה. לדוגמה:

בחירת אות של $x_i \in X$	הצפנה
a	00
b	01
c	10
d	11

ז"א להצפין תו אחד של הטקסט גלוי X נדרש 2 bit. לכן להצפין רצף אותיות של טקטסט גלוי נדרש $2 \times 1000 =$ 2000 bit, כלומר 2000 סיביות.

האנטרופיה של X היא

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

ז"א לכל ניסוי המידע הממוצע הנדרש כדי להצפין תו אחד של טקסט גלוי הוא 1.62581 bit. לכן המידע הממוצע הנדרש כדי להצפין רצף אותיות של טקסט גלוי הוא

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

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

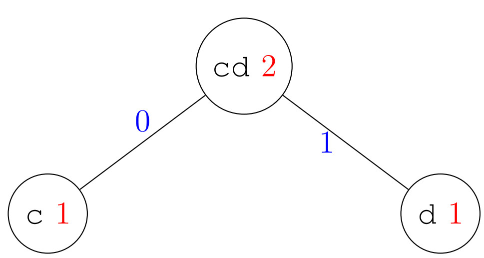
כעת נבנה הצפנה של הטקסט גלוי על ידי האלגוריתם של האפמן.

שלב 1)

	c	d	a	b
	1	1	4	6

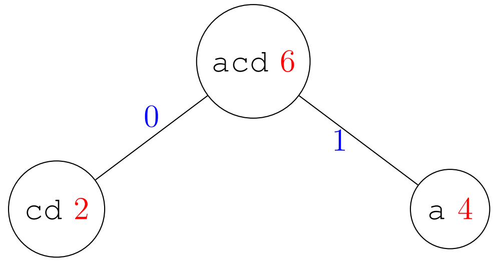
שלב 2)

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



שלב 3)

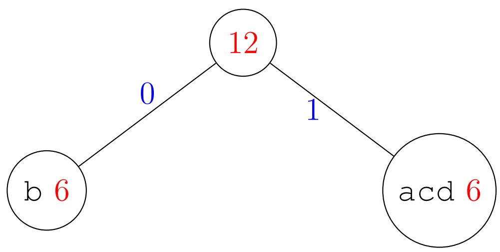
	cd	a	b
	2	4	6
	0	1	
	6		6



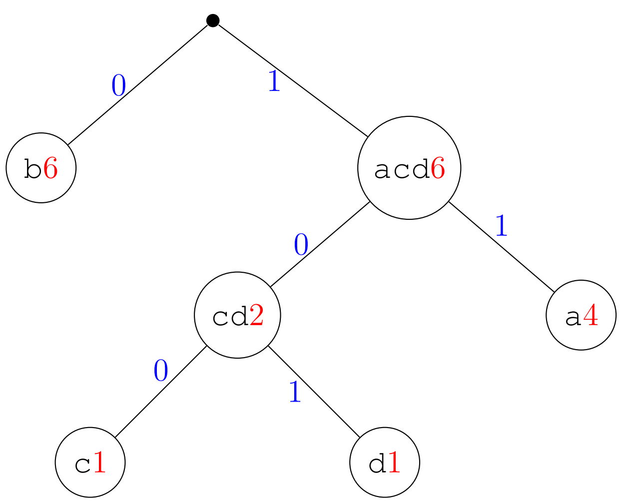
שלב 4)

שלב 5)

	acd	b
	6	6
	0	1
	12	



שלב 6)



בסוף של התהליך האותיות של הטקסט גלוי יהיו בעלים של העץ וההצפנה ניתנת על ידי הרצף סיביות על הענפים במסלול מהנקודת התחלתית של העץ עד העלה בו רשום האות בשאלה.

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

דוגמה 7.8

נתון הטקסט גלוי הבא

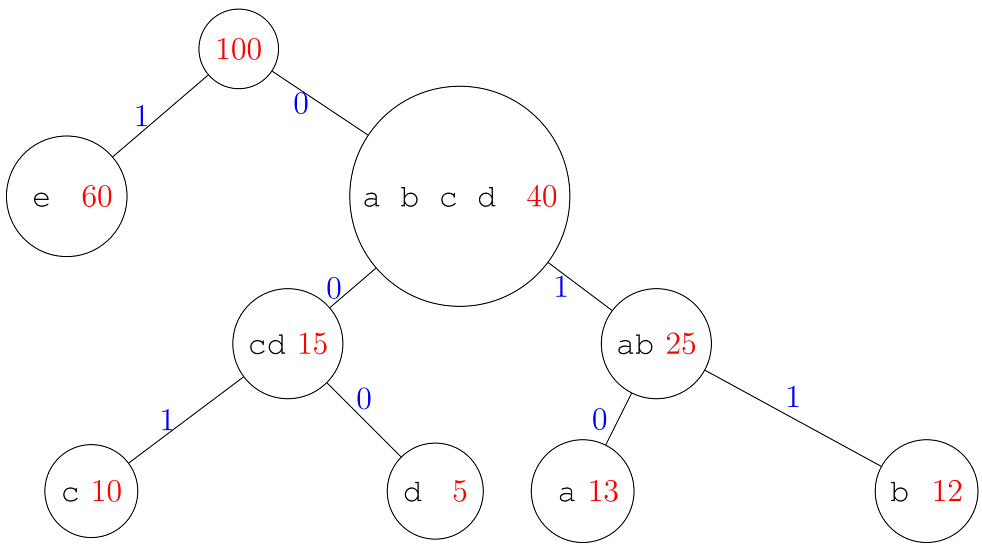
$$X = \{\mathtt{a}, \mathtt{b}, \mathtt{c}, \mathtt{d}, \mathtt{e}\}$$

והפונקצית הסתברות

$$P(X = \mathtt{a}) = \frac{13}{100} = 0.13 \ , \quad P(X = \mathtt{b}) = \frac{3}{25} = \frac{12}{100} = 0.12 \ , \quad P(X = \mathtt{c}) = \frac{1}{10} = \frac{10}{100} = 0.1 \ ,$$
$$P(X = \mathtt{d}) = \frac{1}{20} = \frac{5}{100} = 0.05 \ , \quad P(X = \mathtt{e}) = \frac{3}{5} = \frac{60}{100} = 0.6 \ .$$

מצאו את העץ הצפנה וההצפנת האפמן של כל תו של X.

פתרון:



הצפנת האפמן	בחירת אות של $x_i \in X$
010	a
011	b
001	c
000	d
1	e

■

פורמלי הצפנת האפמן מוגדרת לפי ההגדרה הבאה:

הגדרה 7.3 הצפנת האפמן

נתון משתנה מקרי X. נגדיר הצפנת האפמן של X להיות הפונקציה (כלל מצפין)

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

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

נתון רצף מאורעות $x_1,\ldots,x_n$. נגדיר

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

כאשר "||" מסמן שרשור (concatenation).

הגדרה 7.4 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 7.6 אי שוויון האפמן

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

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

דוגמה 7.9 (המשך של דוגמה 7.8)

נתון הטקסט גלוי הבא

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

והפונקצית הסתברות

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

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

(1 מצאו את תוחלת האורך של ההצפנת האפמן.

(2 מצאו את האנטרופיה.

(3 הוכיחו כי אי-שוויון האפמן של ההצפנה שמצאתם בדוגמה 7.8 למעלה מתקיים.

פתרון:

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)

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

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

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

מתקיים.

■

7.5 תכונות של אנטרופיה

הגדרה 7.5 פונקציה קעורה

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

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

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 7.7 אי-שוויון ינסן

נניח כי f פונקציה רציפה וקעורה ממש בקטע I. נתון מספרים ממשיים $a_i>0$, $i=1,\ldots,n$ כך ש- $\sum\limits_{i=1}^n a_i = 1$. אז

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

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

משפט 7.8

יהי

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

משתנה מקרי בדיד בעל פונקצית הסתברות

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

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

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

אם ורק אם

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

לכל $1 \leq i \leq n$.

הוכחה: לפי אי-שוויון ינסן:

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

בנוסף $H(X) = \log_2 n$ אם ורק אם $p_i = \frac{1}{n}$ לכל $1 \leq i \leq n$. ■

משפט 7.9

יהי $X = \{x_1, \cdots, x_m\}$ משתנה מקרי בדיד בעל פונקצית הסתברות

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

$1 \leq p_i < 0$ לכל $1 \leq i \leq m$, ויהי $Y = \{y_1, \cdots, y_n\}$ משתנה מקרי בדיד בעל פונקצית הסתברות

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

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

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

ו- $H(X,Y) = H(X) + H(Y)$ אם ורק אם X ו- Y בלתי תלויים.

הוכחה: (*להעשרה בלבד)

פונקצית הסתברות של X היא $P_X(x_i) = p_i$ ופונקצית הסתברות של X היא $P_Y(y_i) = q_i$. נגדיר הפוקנצית הסתברות של המשתנה מקרי דו-ממדי:

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

אז הפונקציית הסתברות שולית של X היא

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

והפונקציית הסתברות שולית של Y היא

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

מכאן

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

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

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

לכן

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

■

הגדרה 7.6 אנטרופיה מותנית

יהיו X,Y משתנים מקריים בדידים. נגדיר

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

האנטרופיה מותנית תסומן $H(X|y)$ ותוגדר הממוצע המשוקלל של $H(X|Y=y)$ ביחס להתברויות $P(Y=y)$, כלומר התוחלת של $H(X|Y=y)$:

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

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

משפט 7.10

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

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

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

ו-

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

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 7.11

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

ו- $H(X|Y)=H(X)$ אם ורק אם X ו- Y משתנים מקיים בלתי-תלויים.

הוכחה: (*להעשרה בלבד)
לפי משפט 7.9, $H(X,Y)\leq H(X)+H(Y)$. נציב משפט 7.10 ונקבל

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

בנוסף לפי משפט 7.9, $H(X,Y)=H(X)+H(Y)$ אם ורק אם X,Y משתנים בלתי תלויים, לכן

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

אם ורק אם X,Y משתנים בלתי תלויים.

■

7.6 משפט האנטרופיה לקריפטו-מערכת

משפט 7.12 משפט האנטרופיה 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 7.10,

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

בגלל שהכלל מצפין $y=e_k(x)$ הוא פונקציה חד-חד-ערכית, אז המפתח והטקסט גלוי קובעים את הטקסט מוצפן בדרך יחידה. ז"א

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

לכן

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

המשתנים מקריים K ו- P בלתי-תלויים. לכן לפי משפט 7.9, $H(K,P) = H(K) + H(P)$ ולפיכך נקבל

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

באותה מידה, לפי משפט 7.10,

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

מכיוון שהכלל מפענח $x = d_k(y)$ פונקציה חד-חד ערכית, אז המפתח והטקסט מוצפן קובעים את הטקסט גלוי בדרך יחידה. לכן

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

ומכאן

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

לפי משפט 7.10, $H(K,C) = H(C) + H(K|C)$. לכן

$$\begin{aligned} H(K|C) =& H(K,C) - H(C) \\ =& H(K,P,C) - H(C) && \text{(לפי 4*)} \\ =& H(K) + H(P) - H(C) && \text{(לפי 2*)} \qquad (7.5) \end{aligned}$$

כנדרש.

■

דוגמה 7.10 (המשך של דוגמה 7.1 והמשך של דוגמה 7.5)

עבור דוגמה 7.1 מצאו את $H(K|C)$ ובדקו כי הערך המתקבל תואם עם $H(K|C) = H(K) + H(P) - H(C)$.

פתרון:
בדוגמה 7.5 מצאנו כי $H(P) = 0.81$, $H(K) = 1.5$ ו- $H(C) = 1.85$. ז"א $H(K|C) = H(K) + H(P) - H(C) = 0.46$.

כעת נחשב את $H(K|C)$ בעזרת התוצאות של דוגמה 7.1:

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

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

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

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

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

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

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

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

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

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

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

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

מכאן

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

הרי

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

כנדרש. ■