שיעור 7
סודיות מושלמת

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 $X=\{\texttt{a},\texttt{b}\}$ עם פונקצית הסתברות

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

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 טקטס מוצפן

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

נניח כי הכלל מצפין מוגדר כך ש-

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

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:

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

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

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

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

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

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

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

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

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

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

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

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

■

דוגמה 7.2 (משך של דוגמה 7.1)

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

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

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

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),

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

נציב (7.2) בצד שמאל ונקבל

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

ז"א

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

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

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

■

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 $|K|=|Y|$. 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 טקטסים 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,

$$P(X=x_i|Y=y)=\frac{P(Y=y|X=x_i)P(X=x_i)}{P(Y=y)}$$
$$\overset{\text{(7.2) לפי}}{=}\frac{P(K=k_i)P(X=x_i)}{P(Y=y)}$$

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

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

■

הגדרה 7.2 צופן חד פעמי

יהי n שלם ויהי $X = Y = K = (\mathbb{Z}_2)^n$. לכל $k \in (\mathbb{Z}_2)^n$ נגדיר כלל מצפין

$$e_k(x) = (x_1 + k_1, \ldots, x_n + k_n) \mod 2 \ ,$$

ונגדיר כלל מפענח

$$\begin{aligned} d_k(y) &= (y_1 - k_1, \ldots, y_n - k_n) \mod 2 \\ &= (y_1 + k_1, \ldots, y_n + k_n) \mod 2 \ . \end{aligned}$$

דוגמה 7.3

נתון הקבוצת מפתחות $K = \{0, 1, 1, 0, 0\}$ של צופן חד-פעמי ונתון הטקסט גלוי $x = 1110100010$.

(1 מצאו את הטקסט מוצפן.

(2 וודאו כי הכלל מפענח מחזירה הטקסט גלוי המקורי.

פתרון:

(1

$$\begin{aligned} e_k(x) =& \{1+0 \ , \ 1+1 \ , \ 1+1 \ , \ 0+0 \ , \ 1+1 \ , \ 0+0 \ , \ 0+1 \ , \ 0+1 \ , \ 1+0 \ , \ 0+1\} \mod 2 \\ =& \{1, 0, 0, 0, 0, 0, 1, 1, 1, 1\} \ . \end{aligned}$$

(2

$$\begin{aligned} d_k(y) =& \{1+0 \ , \ 0+1 \ , \ 0+1 \ , \ 0+0 \ , \ 0+1 \ , \ 0+0 \ , \ 1+1 \ , \ 1+1 \ , \ 1+0 \ , \ 1+1\} \mod 2 \\ =& \{1, 1, 1, 0, 1, 0, 0, 0, 1, 0\} \ . \end{aligned}$$

■

נשים לב כי בצופן חד-פעמי

$$|X| = |Y| = |K| = \mathbb{Z}_2^n$$

לפיכך לפי משפט שאנון לצופן חד-פעמי יש סודיות מושלמת.

7.2 תכונות של אנטרופיה

הגדרה 7.3 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 7.3 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

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

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 7.4

יהי

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

משתנה מקרי בדיד בעל פונקצית הסתברות

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

$0 < p_i \leq 1$ 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 $p_i = \dfrac{1}{n}$ לכל $1 \leq i \leq n$. ■

משפט 7.5

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

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

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

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

$0 < q_i \leq 1$ 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 הפונקצית הסתברות שולית של X היא

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

והפונקצית 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 7.4 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 7.6

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

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 7.7

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

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

הוכחה: (*להעשרה בלבד)

לפי משפט 7.5, $H(X,Y)\leq H(X)+H(Y)$. נציב משפט 7.6 ונקבל

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

בנוסף לפי משפט 7.5, $H(X,Y) = H(X) + H(Y)$ אם ורק אם X, Y משתנים בלתי תלויים, לכן
$$H(X|Y) = H(X)$$
אם ורק אם X, Y משתנים בלתי תלויים.

■

7.3 צופן מרוכב

הגדרה 7.5 צופן מרוכב

נתון קריפטו-מערכת
$$S_1 = (P, P, K_1, E_1, D_1)$$
וקריפטו-מערכת שניה
$$S_2 = (P, P, K_2, E_2, D_2)$$
הקריפטו-מערכת המורכבת מ- S_1 ו- S_2 מסומנת $S_1 \times S_2$ ומוגדרת להיות הקריפטו-מערכת
$$(P, P, K_1 \times K_2, E, D)$$
מפתח של הקריפטו-מערכת המורכבת $k \in K$,
$$k = (k_1, k_2)$$
כאשר $k_1 \in K_1$ ו- $k_2 \in K_2$. הכלל מצפין של $S_1 \times S_2$ הוא
$$e_{(k_1,k_2)}(x) = e_{k_2}\left(e_{k_1}(x)\right)$$
והכלל מפענח של $S_1 \times S_2$ הוא
$$d_{(k_1,k_2)}(y) = d_{k_1}\left(d_{k_2}(y)\right)$$
כלומר, ראשית מצפינים x עם $e_{k_1}(x)$ ואז חוזרים ומצפינים שוב עם e_{k_2}. מבצעים פענוח בסדר הפוך, כלומר
$$\begin{aligned} d_{k_1,k_2}\left(e_{(k_1,k_2)}(x)\right) =& d_{k_1,k_2}\left(e_{k_2}\left(e_{k_1}(x)\right)\right) \\ =& d_{k_1}\left(d_{k_2}\left(e_{k_2}\left(e_{k_1}(x)\right)\right)\right) \\ =& d_{k_1}\left(\left(e_{k_1}(x)\right)\right) \\ =& x \ . \end{aligned}$$

לכל קריפטו-מערכת יש פונקצית הסתברות של הקבוצת מפתחות. נגדיר את הפונקצית הסתברות של המפתח של הצופן המורכב כך:
$$P\left(k_1, k_2\right) = P(k_1)P(k_2)$$
ז"א הבחירות של המפתחות k_1 ו- k_2 הם מאורעות בלתי-תלויים.

הגדרה 7.6 צופן הרכבה

יהיו $P = C = \mathbb{Z}_{26}$ ונגדיר קבוצת מפתחות
$$K = \{a \in \mathbb{Z}_{26} \mid \gcd(a.26) = 1\} \ .$$
לכל $a \in K$ נגדיר כלל מצפין
$$e_a(x) = ax \mod 26 \ ,$$

לכל $x \in \mathbb{Z}_{26}$, ונגדיר כלל מפענח
$$d_a(y) = a^{-1}y \mod 26 ,$$
לכל $y \in \mathbb{Z}_{26}$.

דוגמה 7.4

יהי S צופן הזזה עם מפתח $k \in \mathbb{Z}_{26}$ ויהי M צופן מכפלה עם מפתח $a \in \mathbb{Z}_{26}$. הוכיחו כי הקריפטו-מערכת המורכבת $M \times S$ היא צופן איפיני.

פתרון:

$$e_{a,k}(x) = e_a(x+k) = ax + ak .$$

מכיוון ש- $\gcd(a,26)=1$ לכן $ak \mod 26 = k$ ולכן

$$e_{a,k}(x) = e_a(x+k) = ax + k .$$

ז"א $e_{a,k}(x)$ זהה לכלל מצפין של צופן אפיני. נשאר להוכיח כי הפונקצית הסתברות של המפתח (a,k) של $M \times S$ שווה להסתברות של המפתח של צופן האפיני, דהיינו $\frac{1}{312}$: עבור צופן הזזה:

$$P_S(k) = \frac{1}{26}$$

עבור צופן הרכבה:

$$P_M(a) = \frac{1}{12}$$

לכן

$$P_{M\times S} = P_M(a)P_S(k) = \frac{1}{12}\cdot\frac{1}{26} = \frac{1}{312} .$$

■

דוגמה 7.5

יהי S צופן הזזה עם מפתח $k \in \mathbb{Z}_{26}$ ויהי M צופן מכפלה עם מפתח $a \in \mathbb{Z}_{26}$. הוכיחו כי הקריפטו-מערכת המורכבת $S \times M$ היא צופן איפיני.

פתרון:

$$e_{k,a}(x) = e_k(ax) = ax + k .$$

לכן $e_{k,a}(x)$ זהה לכלל מצפין של צופן אפיני.

$$P_{S\times M} = P_S(k)P_M(a) = \frac{1}{26}\cdot\frac{1}{12} = \frac{1}{312} .$$

■

7.4 משפט האנטרופיה לקריפטו-מערכת

משפט 7.8 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 7.6,

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

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 7.5, $H(K,P)=H(K)+H(P)$ ולפיכך נקבל

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

באותה מידה, לפי משפט 7.6,

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

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 7.6, $H(K,C)=H(C)+H(K|C)$. 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 7.6 (המשך של דוגמה 7.1 והמשך של דוגמה 7.2)

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 7.2 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:

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

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

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

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

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

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

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

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

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

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

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

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

מכאן

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

הרי

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

כנדרש. ■