קריפטוגרפיה

9-1-25

1) הצפנת האפמן | (המשך)
2) אנטרופיה
3) מידע
4) צופן | פייסטל

<u>דוגמה:</u> (התפלגות מקסימלית, הצפנת האפמן)

נתון | טקסט [illegible] $X = \{a, b, c, d, e\}$

עם פונקצית הסתברות

$$P_X(a) = \frac{1}{13}, \quad P_X(b) = \frac{2}{13}, \quad P_X(c) = \frac{7}{13},$$

$$P_X(e) = \frac{9}{52}, \quad P_X(d) = \frac{3}{52}$$

<u>סעיף א)</u> רשמו את עץ ההצפנה
עבור התפלגות המקסימלית.

<u>סעיף ב)</u> רשמו את עץ ההצפנה עבור

התוחלת המינימלית נמצא את הצפנת הופמן.

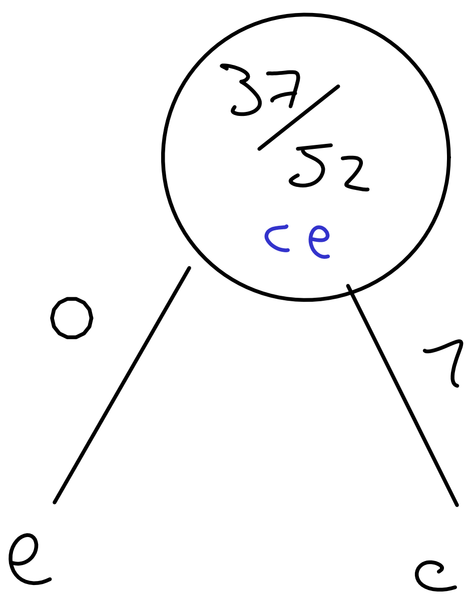
פתרון

רושמים טבלה של ההסתברויות בסדר יורד
של ההסתברויות:

$$P_X(a)=\frac{4}{52},\quad P_X(b)=\frac{8}{52},\quad P_X(c)=\frac{28}{52},\quad P_X(e)=\frac{9}{52},\quad P_X(d)=\frac{3}{52}$$

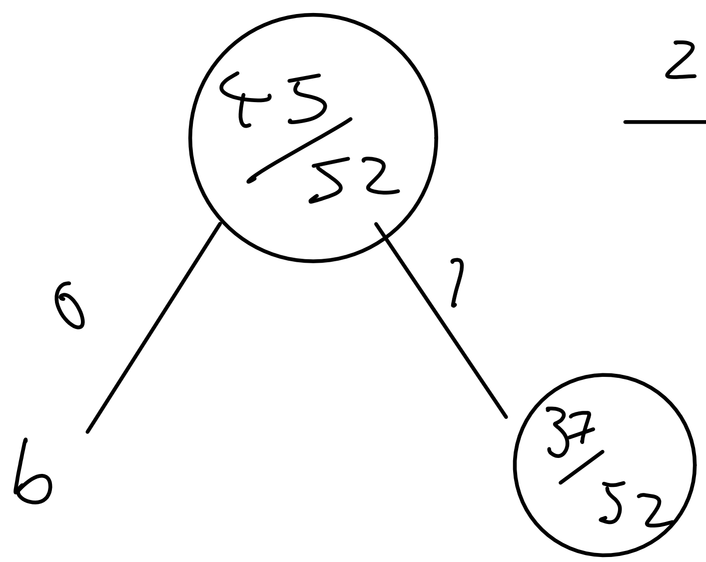
שלב 1

c	e	b	a	d
$\frac{28}{52}$	$\frac{9}{52}$	$\frac{8}{52}$	$\frac{4}{52}$	$\frac{3}{52}$
$\frac{37}{52}$				



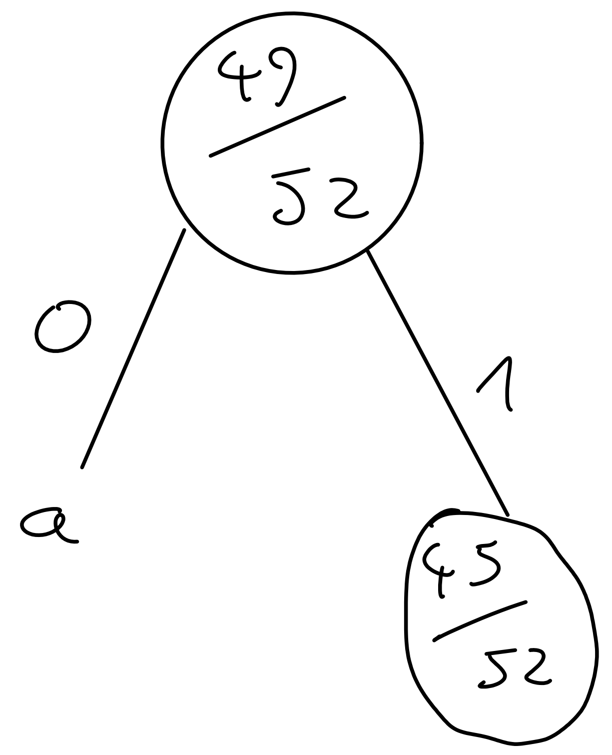
שלב 2

ce	b	a	d
$\frac{37}{52}$	$\frac{8}{52}$	$\frac{4}{52}$	$\frac{3}{52}$
$\frac{45}{52}$		$\frac{4}{52}$	$\frac{3}{52}$



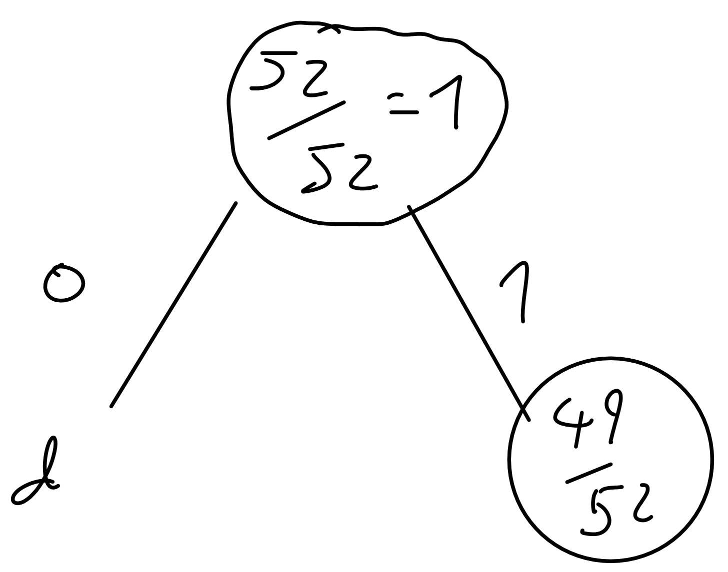
ceb	a	d
45/52	4/52	3/52
49/52		3/52

שלב 3



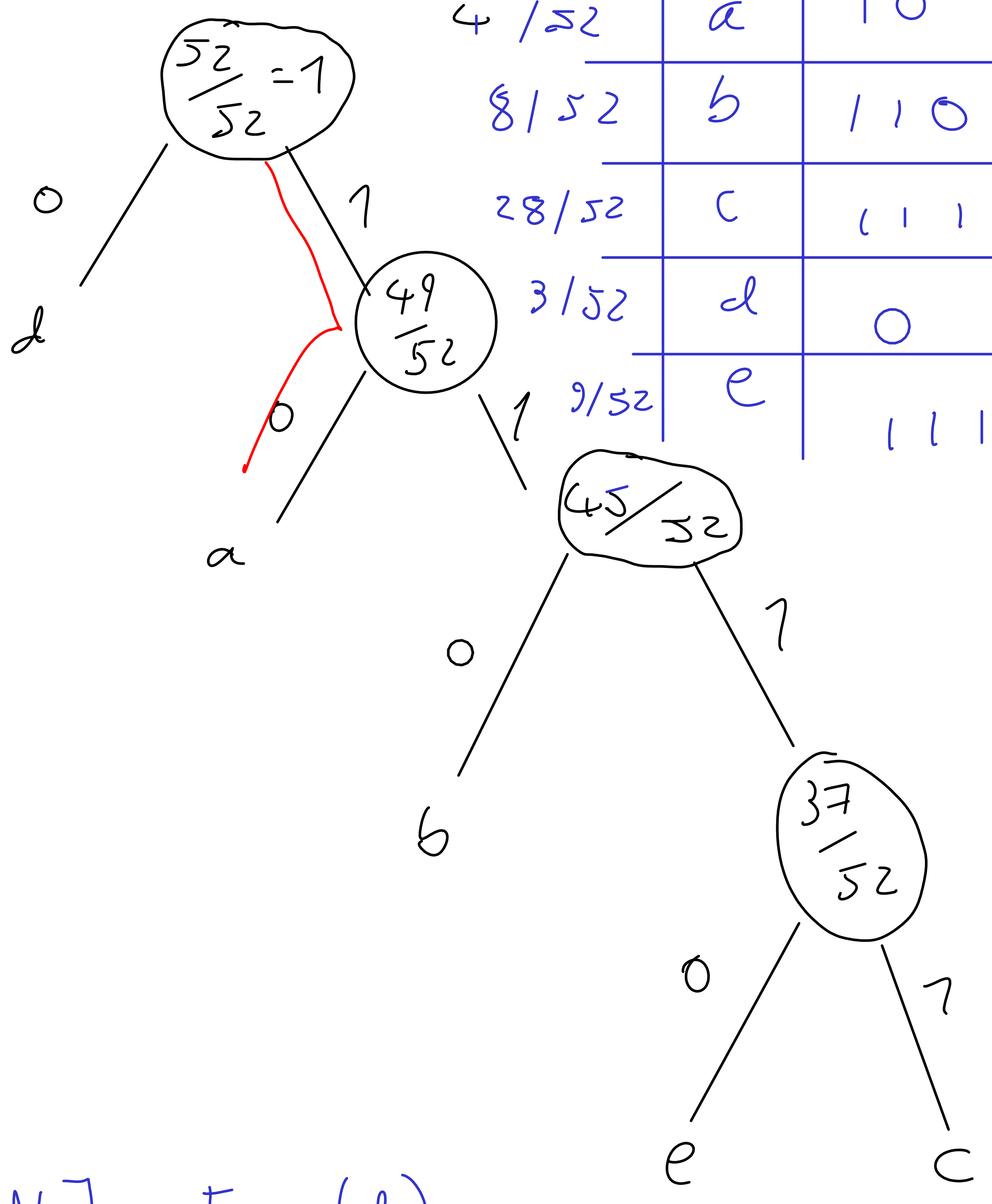
שלב 4

ceba	d
49/52	3/52



שלב 5 מחשבים כל הקודקודים

הסתברות	אות	קידוד
4/52	a	10
8/52	b	110
28/52	c	1111
3/52	d	0
9/52	e	1110



$$E_{max}[N] = E_{max}(l)$$

$$= \underset{2}{l(a)}\,\underset{4/52}{P_X(a)} + l(b)\,P_X(b) + \dots + \overset{4}{l(e)}\,\overset{9/52}{P_X(e)}$$

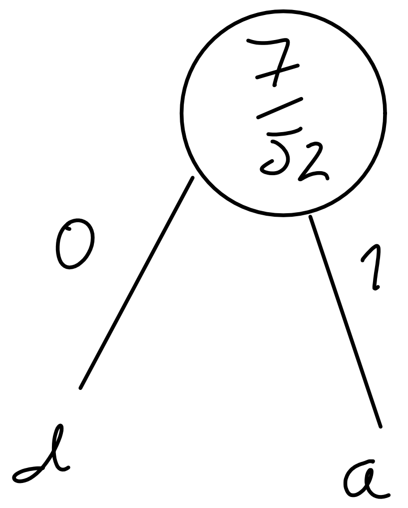
סעיף ב) נחשב עץ ההצפנה שנותן
תוחלת אורך ההצפנה המינימלית
(שלה נקרא הצפנת הופמן).

רושמים את ההסתברויות בסדר עולה:

$P_X(a) = \frac{4}{52}$, $P_X(b) = \frac{8}{52}$, $P_X(c) = \frac{28}{52}$, $P_X(e) = \frac{9}{52}$, $P_X(d) = \frac{3}{52}$

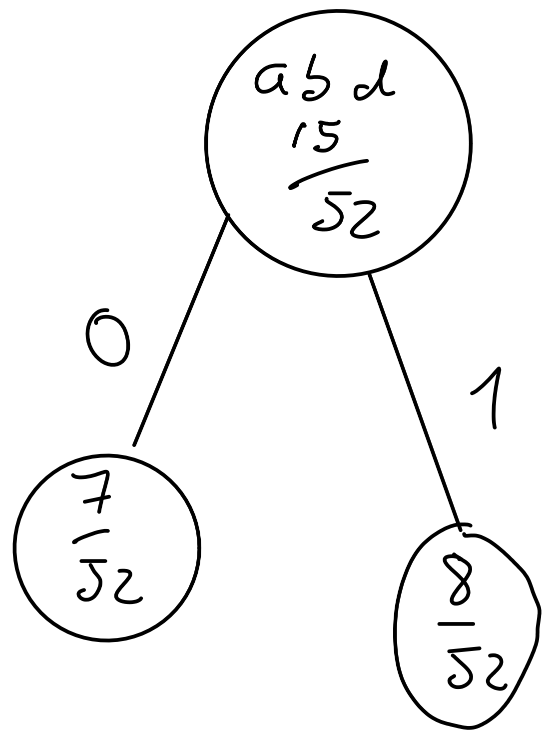
שלב 1:

d	a	b	e	c
$\frac{3}{52}$	$\frac{4}{52}$	$\frac{8}{52}$	$\frac{9}{52}$	$\frac{28}{52}$
$\frac{7}{52}$				



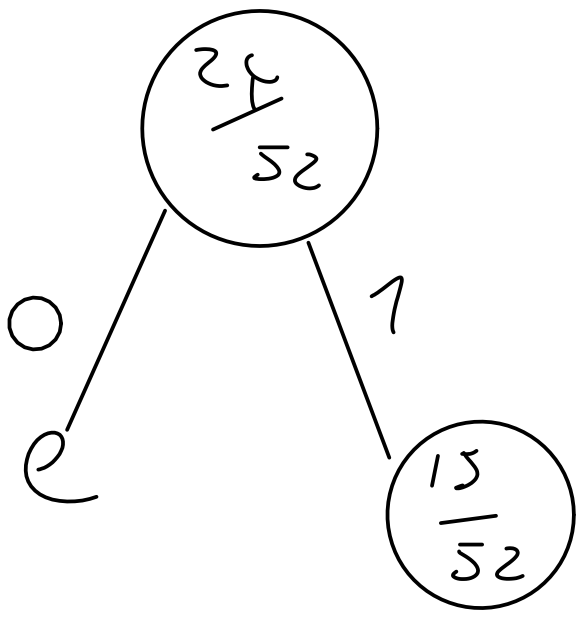
שלב 2:

ad	b	e	c
$\frac{7}{52}$	$\frac{8}{52}$	$\frac{9}{52}$	$\frac{28}{52}$
$15/52$		$\frac{9}{52}$	$28/52$



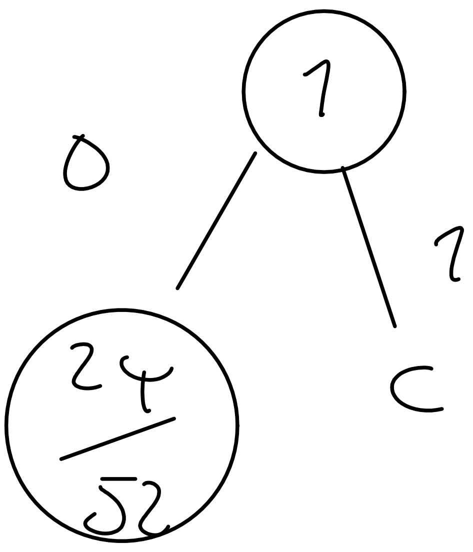
שלב 3:

e	adb	c
$\frac{9}{52}$	$\frac{15}{52}$	$\frac{28}{52}$
$\frac{24}{52}$		$\frac{28}{52}$

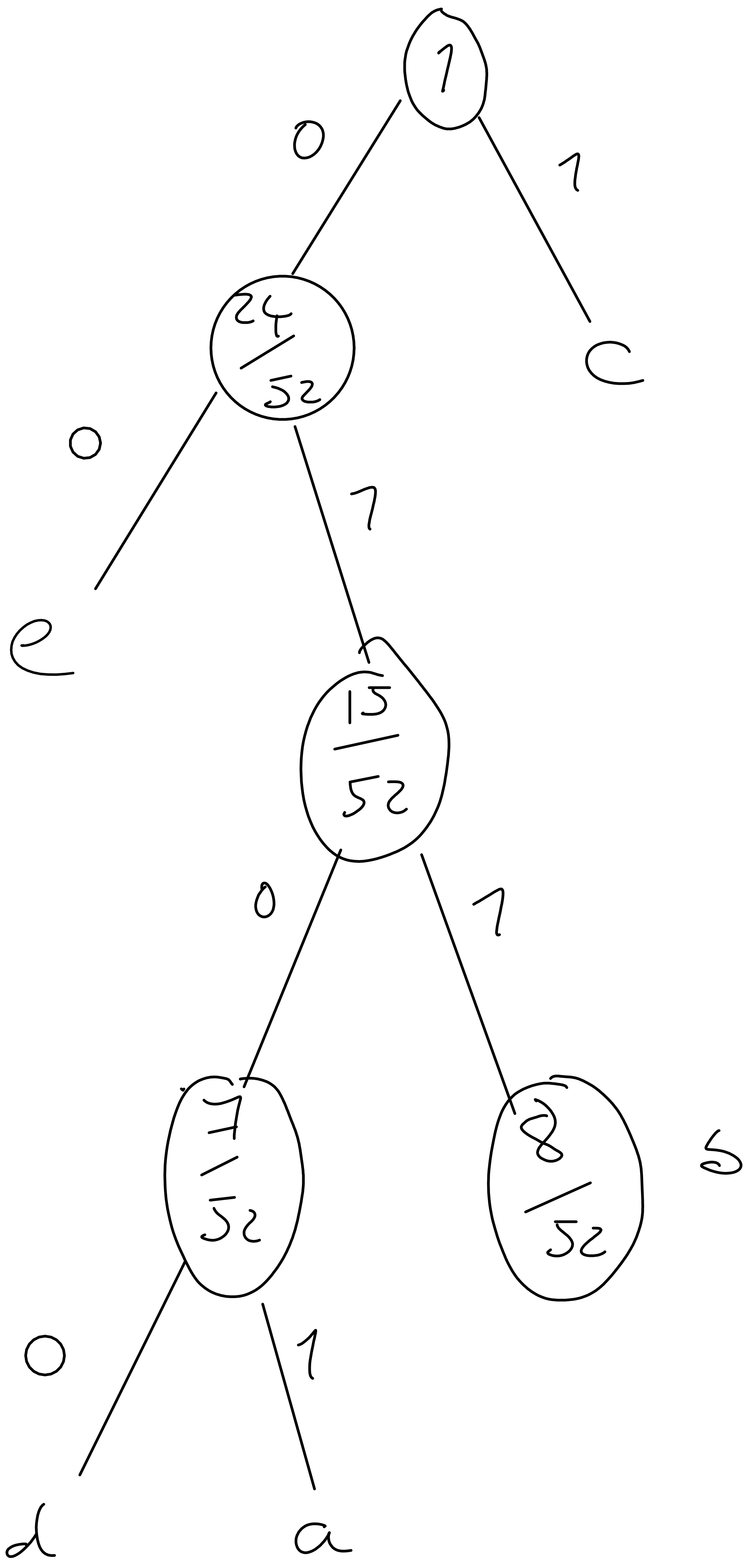


שלב 4:

eadb	c
$\frac{24}{52}$	$\frac{28}{52}$
$52/52$	



5 ide



		P_X
a	0101	4/52
b	011	8/52
c	1	28/52
d	0100	3/52
e	00	9/52

$$E_{min}[N] = E_{min}(\ell)$$

$$= P_X(a)\,\ell(a) + P_X(b)\,\ell(b) + \dots + P_X(e)\,\ell(e)$$

$P_X(a) = 4/52$, $\ell(a) = 4$, $P_X(e) = 9/52$, $\ell(e) = 2$

אנטרופיה

תזכורת:

נתון מ״מ בדיד X עם פונקציית התפלגות $P_X(k)$.

האנטרופיה מוגדרת להיות:

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

משפט האנטרופיה

נתון מ״מ X. האנטרופיה $H[X]$ היא חסם תחתון של תוחלת אורך ההצפנה האופטימלי.

בשפה פורמלית:

נסמן $|f(k)|$ אורך ההצפנה של $X=k$.

נסמן תוחלת של אורך ההצפנות ב-

$$\ell(f) = \sum_{k\in X} P_X(k)\,|f(k)|$$

אזי:

אנטרופיה

$$H[X] \le \ell(f) \le H[X]+1$$

תוחלת אורך ההצפנות.

דוגמה: נתון מ״מ

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

$$P_X(a) = \frac{13}{100},\quad P_X(b) = \frac{12}{100},\quad P_X(c) = \frac{10}{100}$$

$$P_X(d) = \frac{5}{100}\qquad P_X(e) = \frac{60}{100}$$

א) בנו את ההצפנה האופטימלית
(הצפנה אופטימלית = הצפנה הפוכה
ותוחלת מינימלית).

ב) חשבו את $\ell(f)$ (תוחלת אורך לגבי ההצפנות)

ג) חשבו את $H[X]$ (האנטרופיה)

3) הוכיחו את משפט האנטרופיה.

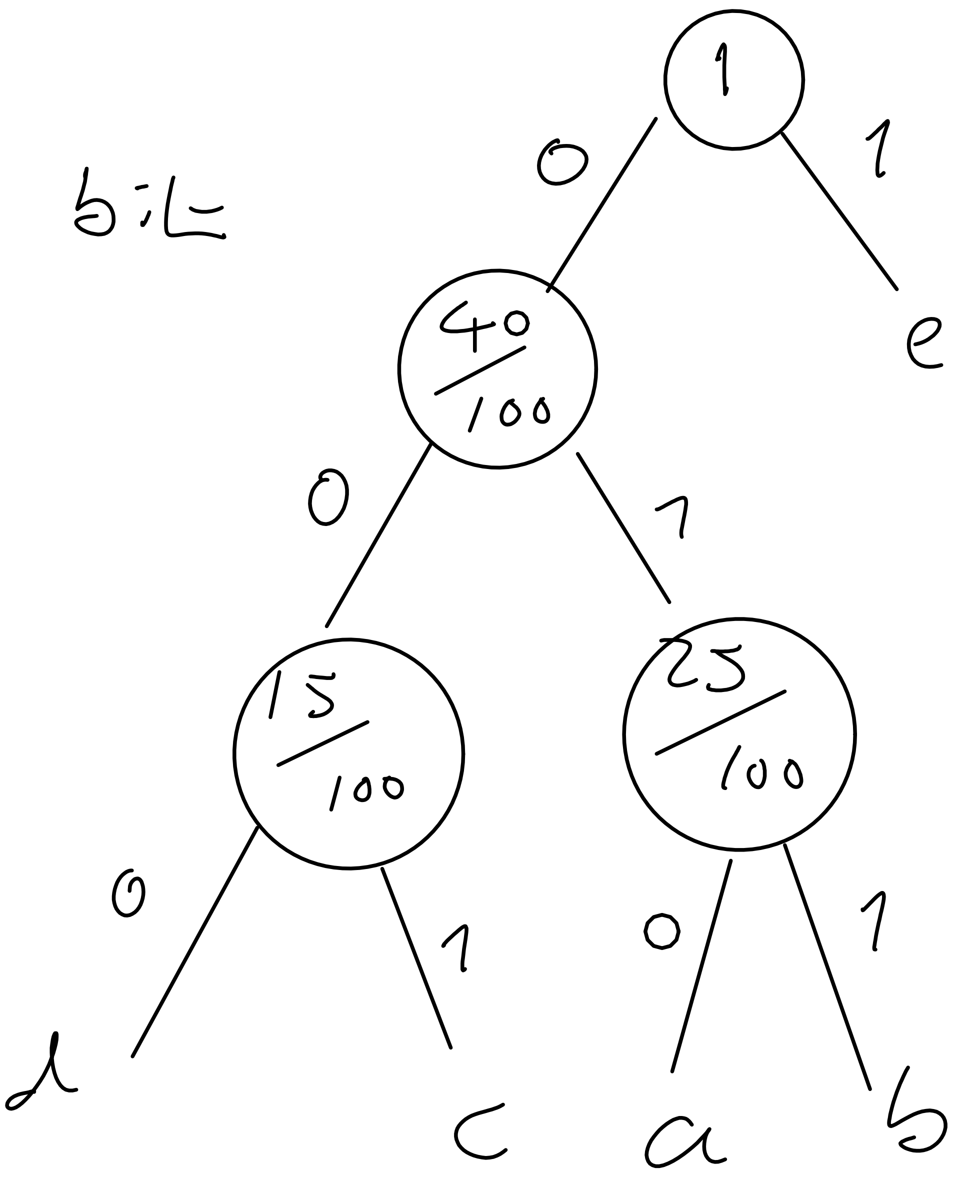
$$H[X] \le \ell(f) < H[X]+1$$

<u>פתרון</u> <u>סעיף א)</u>

לפי הצפנת ה[illegible]/ (תרגיל בית)
(חשוב למבחן)

ההצפנה את

k	f(k)	|f(k)| bit
a	010	3
b	011	3
c	001	3
d	000	3
e	1	1



$f(a) = 010 \quad f(b) = 011 \quad f(c) = 001$

$f(d) = 000 \quad f(e) = 1$

$f(k)$ מסמנת את ההצפנה עצמה של k.

<u>סעיף ב)</u> תוחלת אורך ההצפנה מסומנת $\ell(f)$.

$$\ell(f) = \sum_{k \in X} P_X(k) \cdot |f(k)|$$

$$= \underset{13/100}{P_X(a)}\,\underset{(3)}{|f(a)|} + \underset{3/25}{P_X(b)}\,\underset{(3)}{|f(b)|} + \underset{10/100}{P_X(c)}\,\underset{3}{|f(c)|}$$

$$+ \underset{5/100}{P_X(d)}\,\underset{(3)}{|f(d)|} + \underset{60/100}{P_X(e)}\,\underset{(1)}{|f(e)|}$$

$$= 1.8 \text{ (bit)}$$

סעיף ג)

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

$$= -P_X(a)\log_2 P_X(a) - P_X(b)\log_2 P_X(b) - P_X(c)\log_2 P_X(c) - P_X(d)\log_2 P_X(d) - P_X(e)\log_2 P_X(e)$$

(above the terms: $\frac{13}{100}$, $\frac{12}{100}$, $\frac{10}{100}$, $\frac{5}{100}$, $\frac{60}{100}$)

$$= 1.74018.$$

סעיף ד)

$$H[X] \le \ell(f) \le H[X]+1$$

$$1.74 \le 1.8 \le 2.74.$$

מתקיים.

הגדרות: **מידע**

נתון טקסטים X.

נגדיר את המידע של האות "X=k" לפי:

$$I(X=k) = -\log_2 P_X(k).$$

הערה: משמעות: אנטרופיה היא תוחלת המידע:

$$H[X] = \sum_{k \in X} P_X(k) \left(-\log_2 P_X(k) \right)$$

$$= \sum_{k \in X} P_X(k)\, I(X=k)$$

כלומר, $H[X]$ היא התוחלת של המידע של X.

דוגמה: נתון | משתנה מקרי

$X = \{H, T\}$

X מסמן את התוצאה של הטלת מטבע הוגן. ז"א $P_X(H)=\frac{1}{2}$, $P_X(T)=\frac{1}{2}$

חשבו את המידע של כל תוצאה.

פתרון

$$I_X(H) = -\log_2 P_X(H)$$
$$= -\log_2\left(\frac{1}{2}\right) = -\log_2\left(2^{-1}\right)$$
$$= -(-1)$$
$$= 1 \quad (bit)$$

$$I_X(T) = -\log_2 P_X(T) = -\log_2\left(\tfrac{1}{2}\right) = 1$$

משמעות: הצפנת האפמן של $X=\{H,T\}$ היא

$f(H) = 0$

$f(T) = 1$.

$\Leftarrow$ לקידוד | "H" אנו צריכים ספרה אחת $f(H)=\alpha$, $\alpha \in \{0,1\}$

ז"א הצפנה של "H" דורשת 1 bit של מידע.

דוגמה: נתון 60/76

כאל ... הוגנת (וסימטרית)

$$P_X(k) = \frac{1}{4} \quad \forall k \in X.$$

חשבו את המידע של כל $k \in X$.

פתרון

$$I_X(k) = -\log_2 P_X(k)$$

$$= -\log_2\left(\frac{1}{4}\right) = -\log_2\left(2^{-2}\right)$$

$$= 2\,\text{bit}, \quad \forall k \in X$$

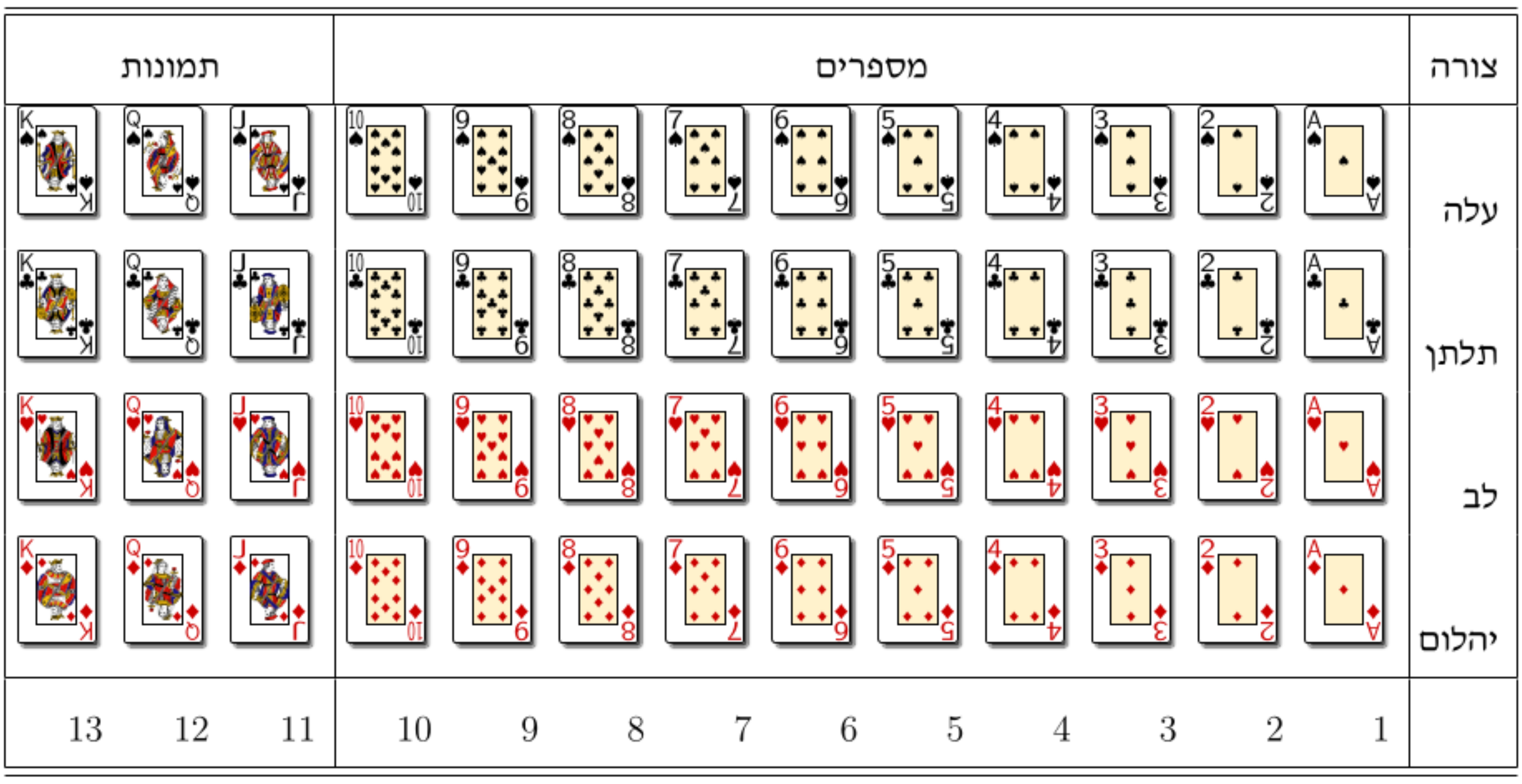
דוגמה:

$$X = \{\text{קלפי משחק}\}$$

נניח שלכל קלף יש הסתברות שווה.

$$P_X(k) = \frac{1}{52}$$

$k =$



$$I_X(k = 10\heartsuit) = -\log_2 P_X(k = 10\heartsuit)$$

$$= -\log_2\left(\frac{1}{52}\right)$$

$$= 5.7\,\text{bit}$$

בגלל שההסתברות של כל קלף שווה,

$$I_X(\text{כל קלף}) = 5.7\,\text{bit}$$ כ"ל