

## נושאים בתורת המידע – 89-641-01

מרצה: פרופ' טומי קליין  
 סמסטר א' מועד ב'  
 תאריך הבחינה: 22.2.2019  
 משך הבחינה: שעתיים

ללא חומר עזר.  
 ענה/י על כל השאלות. כל תשובה צריכה להיות מנומקת היטב. כל השאלות שוות משקל.

### [1] ראינו את הפרוטוקול כדי לשחק mental poker.

1. A מקודד את הקלפים 1, ..., 52 ושולח את  $E_A(1), \dots, E_A(52)$  ל B.
2. B בוחר אקראית 5 קלפים  $E(a_1), \dots, E(a_5)$  ומחזיר אותם ל A שמוריד את ההצפנה שלו  $D_A E_A(a_j) = a_j$ .
3. B בוחר עוד 5 קלפים  $E(b_1), \dots, E(b_5)$  בשביל עצמו, ושולח ל A את  $E_B E_A(b_j)$ .
4. A מוריד את ההצפנה שלו ומחזיר ל B את  $D_A E_B E_A(b_j) = E_B(b_j)$ .
5. B מוריד את ההצפנה שלו ומקבל  $b_1, \dots, b_5$ .

הגז הכללה של הפרוטוקול שמתאים לחוקים של משחק הפוקר: אחרי שכל שחקן קיבל את קלפיו וראה אותם, מותר לו להחזיר כמה מהם לפי בחירתו ולקבל קלפים אחרים במקומם. הסברי את המשך הפרוטוקול אם A רוצה להחליף 2 קלפים ב B רוצה להחליף 3. דאגי לכך שלא ניתן לרמות, ז"א שחקן חייב להחליט איזה קלפים להחזיר לפני שהוא רואה את הקלפים המחליפים. צריך להניח שהקלפים המוחזרים חייבים להיות מצורפים לקבוצת הקלפים שמתוכה נבחרים המחליפים (ז"א אין וודאות שלא לקבל שוב חלק מהקלפים המוחזרים).

### [2] תן/י דוגמה לסדרה של $n$ משקלים שעבורם ההפרש בין מספר הקדקודים בעץ Huffman לבין מספר הקדקודים בעץ השלד המתאים (skeleton tree) הוא קטן ביותר.

מה יהיה אז ההפרש בין מספר הקדקודים ב skeleton tree לבין מספר הקדקודים בעץ reduced skeleton tree?

תזכורת: כל עלה ב skeleton tree מתאים לשורש של תת-עץ מלא בעץ הקנוני המקורי. עץ מלא הוא עץ שכל עליו באותה רמה. כל עלה ב reduced skeleton tree מתאים לשורש של תת-עץ בעץ הקנוני המקורי שעליו ברמות שכינות; אם אין תת-עץ כזה, לוקחים תת-עץ מלא.

### [3] אפשר להגיע להגדרת האנטרופיה גם ע"י אילוצים על פונקציית כמות המידע $h$ ולא על $H$ . נתונה פונקציית $h(p)$ עבור $0 < p \leq 1$ שמקיימת:

$$h(pq) = h(p) + h(q) \quad (1)$$

$$h(p) \text{ רציפה ויורדת מונוטונית.} \quad (2)$$

ניתן אז להראות שהפונקציה היחידה שמקיימת תנאים אלה היא  $h(p) = -C \log_a p$  עבור קבועים  $a > 1$  ו  $C > 0$  מסוימים. ההוכחה שוב בכמה שלבים, דומים למה שראינו עבור  $H$ , ומוכיחים את הטענה לפי הסדר:

- (1) עבור  $p = 1/n$  כאשר  $n$  מספר טבעי.
- (2) עבור  $p = r/s$  כאשר  $r$  ו  $s$  טבעיים, ז"א  $p$  רציונלי.
- (3) לכל  $p$ , גם אי-רציונלי.

הניחו נכונות של (1) והוכיחו (2). (3) אז נובע ע"י רציפות.

רמז: התחילו מהשוויון הבא:  $\frac{1}{s} = \frac{r}{s} \cdot \frac{1}{r}$ , הפעילו את  $h$  על שני האגפים והשתמשו בתכונות הידועות כבר של  $h$ .

**[4]** נתון הקוד  $\{01, 000, 110, 0111, 1011, 10101, 111101\}$  עבור הא"ב  $\{x_1, \dots, x_7\}$

- (א) הראה/י שהקוד אינו UD.
- (ב) יהי  $l_i$  האורך בסיביות של מילת הקוד עבור  $x_i$  איך מסתדרת התשובה ב-א) עם העובדה ש

$$\sum_{i=1}^7 2^{l_i} < 1 ?$$

**בהצלחה !!!**