

נושאים בתורת המידע – 89-641-01

מרצה: פרופ' טומי קליין
 סמסטר א' מועד א'
 תאריך הבחינה: 30.1.2019
 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 .

הג הגללה 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 ו B רוצה להחליף 3. דאגי לכך שלא ניתן לרמות, ז"א שחקן חייב להחליט איזה קלפים להחזיר לפני שהוא רואה את הקלפים המחליפים. מותר להניח שהקלפים המוחזרים אינם מצורפים לקבוצת הקלפים שמתוכה נבחרים המחליפים.

[2] Source $\langle n_1, \dots, n_k \rangle$ הוא צורה קומפקטית לתיאור עץ Huffman קנוני, כאשר n_i הוא מספר העלים ברמה i בעץ ו k הוא עומק העץ. נתון ה source $\langle 0, 0, 2, 5, 8, 11, 0, 0, 8 \rangle$.

1. איך בודקים שזו אכן סדרה שמתארת source (שהרי לא כל סדרת מספרים מתאימה)?
2. מה מספר הקדקודים בעץ השלד (skeleton tree) המתאים לעץ הקנוני של ה source הזה?
3. מה מספר הקדקודים בעץ ה 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] נתון הקוד האינסופי C, הדומה לקוד פיבונצ'י, אך בו כל מילת קוד מסתיימת ב-111 והתבנית 111 אינה מופיעה במקום אחר באף מילת קוד. התחלת הקוד הוא

$$C = \left\{ 111, 0111, 00111, 10111, 000111, 100111, 010111, 110111, 0000111, \dots \right. \\ \left. 1000111, \dots, 0110111, 00000111, 10000111, \dots \right\}$$

מספר מילות הקוד באורך 3, 4, 5, וכו' הוא 1, 1, 2, 4, 7, 13, וכו'. אם נסמן את מספר מילות הקוד באורך n ע"י T_n , הראה/י ש $n \geq 3$, $T_n = T_{n-1} + T_{n-2} + T_{n-3}$

$$T_3 = 1, T_4 = 1, T_5 = 2, T_n = T_{n-1} + T_{n-2} + T_{n-3} \quad n > 5$$

הראה/י שהקוד C הוא שלם ע"י שימוש בשוויון McMillan כך שתראה/י ש- $\sum_{j=1}^{\infty} 2^{-l_j} = 1$, כאשר

l_j אורך מילת הקוד ה- j -ית. השתמש/י בזהות $\sum_{j=1}^{\infty} 2^{-l_j} = \sum_{i=3}^{\infty} T_i 2^{-i}$ ובנוסחה הרקורסיבית ל T_n .

רמז: סמן / את הסכום $\sum_{j=1}^{\infty} 2^{-l_j}$ ב S , צור/י משוואה ל S והסק/י את ערכו של S .

[4] השתמש/י במשפט ש $-\sum p_i \log p_i \leq -\sum p_i \log q_i$ עבור התפלגויות $\{p_i\}_1^n$ ו- $\{q_i\}_1^n$, עם שוויון אם ורק אם $p_i = q_i$ לכל i , כדי להוכיח את אי-השוויון הידוע בין ממוצע גיאומטרי לממוצע אריתמטי, דהיינו:

יהיו x_1, \dots, x_n מספרים חיוביים כלשהם ויהיו a_1, \dots, a_n מספרים חיוביים כך ש- $\sum_{i=1}^n a_i = 1$, אז

$x_1^{a_1} x_2^{a_2} \dots x_n^{a_n} \leq a_1 x_1 + a_2 x_2 + \dots + a_n x_n$ ובפרט $\sqrt[n]{\prod_{i=1}^n x_i} \leq \frac{1}{n} \sum_{i=1}^n x_i$ עם שוויון אם ורק אם כל ה- x_i שווים.

רמז: הגדר $p_i = a_i$ ו $q_i = \frac{a_i x_i}{\sum_{j=1}^n a_j x_j}$

בהצלחה !!!