Ben-Gurion University of the Negev

SOLUTION

By

Avi Ferdman

שאלה 1

סעיף א:

נגדיר a_{ij} משתנה אינדיקטור לכל $a_i \in (a_1, \dots, a_n)$ באופן הבא: $a_{ij} = 1$ אם $a_i \in s_j$ ו-$a_{ij} = 0$ אם $a_i \notin s_j$

נגדיר X_{s_j} משתנה אינדיקטור לכל $s_j \in (s_1, \dots, s_m)$ באופן הבא: $X_{s_j} = 1$ אם s_j שייכת לכיסוי אחרת $X_{s_j} = 0$.

$$\min \sum_{j=1}^{m} C_{s_j} \cdot X_{s_j}$$

לפי ההוכחה שנלמדה בכיתה האילוץ: לכל $s \in S$: $-X_s \geq -1$ לא נחוץ ולכן האילוצים הם:

לכל: $1 \leq i \leq n$: $\sum_{j=1\dots m} a_{ij} \cdot X_{s_j} \geq 1$

לכל $s \in S$: $X_s \geq 0$

לכל $s \in S$: $X_s \in \{0,1\}$ (האילוץ הזה אינו מתאים לתיאור בעיה לינארית אבל היה דרוש בשאלה אילוץ בשלמים)

הבעיה הדואלית:

$$max \sum_{a_i \epsilon U} 1 \cdot Y_{a_i}$$

$$\sum_{i=1\dots n} a_{ij} \cdot Y_{a_i} \leq C_s \quad \forall s \in S$$

לכל $0 \leq i \leq n$: $0 \leq Y_{a_i}$

סעיף ב:

לכל $1 \leq i \leq n$, $1 \leq j \leq |E|$ נגדיר משתנה a_{ij} המקבל ערך 1 אם הקשת ה-j היא קשת יוצאת מהקוד ה-i אחרת המשתנה הזה מקבל 0, ונגדיר משתנה b_{ij} המקבל ערך 1 אם הקשת ה-j היא קשת נכנסת אל הקוד ה-i ואחרת המשתנה הזה מקבל ערך 0.

$$max \sum_{e \in E} 1 \cdot w(e)$$

לכל $1 \leq i \leq n$: $\sum_{e \in E} a_{ij} w(e) \leq 1$

לכל $1 \leq i \leq n$: $\sum_{e \in E} b_{ij} w(e) \leq 1$

לכל $e \in E$: $w(e) \geq 0$

הבעיה הדואלית:

$$\min\left(\sum_{v \in V} Y_1(v) + \sum_{v \in V} Y_2(v)\right)$$

$\forall e \in E$: $\sum_{v \in V} a_{ij} Y_1(v) + b_{ij} Y_2(v) \geq 1$

לכל $v \in V$: $Y_1(v), Y_2(v) \geq 0$

סעיף ג:

נניח בשלילה שקיים פתרון לבעיה הלינארית מסעיף א1 בעל ערך גדול ממש מ-$|E|$ נסמנו ב-W, לכן המשקל הממוצע של קשת בפתרון זה הוא $\frac{W}{|E|} > 1$ ולכן קיימת e כך שמתקיים: $w(e) \geq \frac{W}{|E|} > 1$ אבל זו סתירה לאילוצים שהגדרנו (כי אז קיימת למשל קשת שיוצאת מקוד' u ומשקלה לכשעצמה גדול מ-1 ולכן דרגת היציאה הממושקלת של u גדולה מ1, בסתירה).

שאלה 2

סעיף א:

נגדיר x_1-מספר השעות בערוץ 1, x_2-מספר השעות ביידיש שפיגל, x_3-מספר השעות בפילוסופיה, x_4-מספר השעות תחת חסותה של מירי מסיקה

$$\min(10x_1 + 16x_2 + 12x_3 + 18x_4)$$

$$0 \cdot x_1 + x_2 + 0 \cdot x_3 + x_4 \geq 50$$

$$x_1 + x_2 + x_3 + x_4 \geq 150$$

$$-x_1 - x_2 - x_3 - x_4 \geq -150$$

$$x_1, x_2, x_3, x_4 \geq 0$$

סעיף ב':

$$\max(50y_1 + 150y_2 - 150y_3)$$

$$y_2 - y_3 \leq 10$$

$$y_1 + y_2 - y_3 \leq 16$$

$$y_1, y_2, y_3 \geq 0$$

סעיף ג':

נציב בבעיה הלינארית המקורית $x_1 = 100$ ו- $x_2 = 50$ וכל שאר המשתנים אפסים, ונקבל פתרון חוקי שערכו הוא 1800.

נציב בבעיה הדואלית $y_1 = 6$ ו- $y_2 = 10$ ו-$y_3 = 0$ ונקבל פתרון חוקי שערכו 1800.

כעת ממשפט הדואליות החלשה נובע שלא נוכל למצוא ערך לבעיה הדואלית שהוא גדול יותר מ1800 (כי אז הוא בהכרח יהיה גדול יותר מהפתרון החוקי של בעיית המינימום וזו סתירה למשפט) באופן דומה לא יכול להיות פתרון לבעיה המקורית קטן יותר מ1800 ולכן ערך הפתרון האופטימלי הוא 1800.

שאלה 3

סעיף א:

פתרון דטרמיניסטי: אליס תשלח את שרשור ההודעות כך שהריישא ה-n-ית של ההודעה תהיה המחרוזת A והסייפא ה-n-ית תהיה המחרוזת B. בוב ישווה את המחרוזת C שלו לרישא ה-n-ית של ההודעה שנשלחה ואת המחרוזת D שלו לסייפא ה-n-ית של ההודעה שנשלחה ויחזיר אמת לאליס אמ"מ $A = C$ וגם $B \neq D$ אחרת, יחזיר שקר. סך הכל אורך ההודעה של אליס תהיה $2n$ ביטים.

סעיף ב:

תיאור האלגוריתם:

בוב יחזיק שני ערכים בוליאניםb_1, b_2, אחד תשובה אם המחרוזות A, C לדעתו שוות והשני תשובה אם המחרוזות B, D לדעתו שונות. בוב יחזיר לאליס את התשובה $b_1 \& b_2$.

עבור השוואת המחרוזות A, C אליס ובוב ישתמשו באלגוריתם רבין קארפ ללא שינוי ובוב יזין ל-b_1 את התשובה. ועבור המחרוזות B, D בוב יבדוק האם על פי הפרוטוקול של רבין קארפ הוא אמור לענות אמת, אם כן כלומר שהמחרוזות לדעתו שוות אז במקרה שלנו הוא יציב $\boldsymbol{b_2 = false}$, אחרת, אם לפי הפרוטוקול של רבין קארפ בוב אמור לענות שקר, כלומר המחרוזות לדעתו שונות אז במקרה שלנו הוא יציב $\boldsymbol{b_2 = true}$. אליס תגריל שני מספריים ראשוניים באופן בלתי תלוי, תחשב את $z_1 = A \; mod q_1$ תחשב את $z_2 = B \; mod q_2$ ותשלח לבוב את $z_1 \circ q_1 \circ z_2 \circ q_2$

סיבוכיות תקשורת:

אליס שולחת $n^2 > z_1, q_1$ עבור A, וגם שולחת $n^2 > z_2, q_2$ עבור B. ולכן $\log n^2 = 2 \log n$ ביטים לכל מספר, וסה"כ $8 \log n$ ביטים.

בוב עונה לאליס בחזרה בסך הכל ביט אחד.

לכן סה"כ סיבוכיות התקשורת היא: $\boldsymbol{O(\log n)}$

הוכחת הסתברות שגיאה:

האלגוריתם נכשל בשני מקרים (אם לפחות אחד מהם מתקיים):

1) אם $A \neq C$ ואליס הגרילה q_1 כך ש- $(A - C) mod q = 0$. (מסמל את המשתה שתיארנו b_1)
2) אם $B \neq D$ ואליס הגרילה q_2 כך ש-$(B - D) mod q = 0$. (מסמל את המשתה שתיארנו b_2)

נחשב את ההסתברות למקרה הראשון, וההסתברות הזו תהיה זהה משיקולי סימטרי למקרה השני.

נסתמך על 2 עובדות מתורת המספרים:

1) יהי $w < 2^n$ $w \in N$ אזי, מספר הראשוניים השונים שמחלקים את w קטן מ-n
2) לכל t מספר הראשוניים שקטנים מ-t הוא לפחות $\frac{t}{\log t}$.

$$P(fail\ in\ th\ case\ where\ A \neq C) = P(Alice\ picked\ q \leq n\ and\ (A - C) mod q = 0) \leq$$

$$\leq \frac{number\ of\ q's\ divided\ (A - C)}{number\ of\ primes < n^2} \leq \frac{n}{\frac{n^2}{\log n^2}} = \frac{2 \log n}{n} \leq \frac{1}{8}$$

החל מ-n מסויים אי השיוויון הנ"ל מתקיים. משיקולי סימטריה הסיכוי לשגיאה במקרה השני הוא זהה החל מאותו n.

ולכן בגלל שהמאורעות זרים, ההסתברות לשגיאה היא:

$$p(mistake) = p(mistake\ in\ first\ case) + p(mistake\ in\ second\ case) \leq \frac{1}{8} + \frac{1}{8} = \frac{1}{4}$$