# **קווים לפתרון שאלות בממ״ן 15 סמסטר א2010**

**שאלה 1**

מדובר על פונקציה תת-ליניארית. לכן ההנחה היא שהקלט $1^n$ נמצא על סרט קלט לקריאה בלבד, וסיבוכיות המקום מתייחסת למספר התאים שהמכונה משתמשת בהם בסרט העבודה.

להלן מכונת טיורינג מתאימה:

״על קלט $w$ כאשר $w = 1^n$:

1. חשב בסרט העבודה את הייצוג הבינרי של $n$.
2. אתחל משתנה $x$ ל-0. ($x$ יהיה מיוצג בבינרי).
3. $y = x+1$ (בייצוג בינרי).
4. חשב את $y{\cdot}y$ (בייצוג בינרי).
5. בדוק האם $y{\cdot}y > n$ (בייצוגים הבינריים).
   אם כן, החזר את $x$. אם לא, הגדל את $x$ ב-1, ולך ל-3.״

המקום הדרוש לייצוג הבינרי של $n$, ל-$x$, ל-$y$, לחישוב $y{\cdot}y$ ול-$y{\cdot}y$ הוא מסדר גודל של $\log(|w|)$.

**שאלה 2**

א. ההוכחה לאחר השינוי הזה לא טובה.

המכונה $D$ אמורה להיות שונה מכל מכונה $M$ שמכריעה את השפה שלה ב-$o(f(n))$.

אם נבצע סימולציה של $M$ על $<M>$ ולא על $w$, ייתכן ש-$M$ ו-$D$ מתנהגות אותו הדבר על כל קלט. ייתכן ששתיהן דוחות את $<M>$ ומקבלות את $w$, והזמן הדרוש ל-$M$ כדי לדחות את $<M>$ גדול ממה ש-$D$ מרשה כאשר היא רצה על $<M>$.

לכן כאשר $D$ רצה על $<M>$, היא דוחה בגלל חריגה ממגבלת הזמן המותרת.

וכאשר $D$ רצה על $w$, היא מריצה את $M$ על $<M>$. מכיוון ש-$M$ דוחה (את $<M>$), $D$ מקבלת (את $w$).

ב. גם ההוכחה לאחר השינוי הזה לא טובה.

המכונה $D$ אמורה להיות שונה מכל מכונה $M$ שמכריעה את השפה שלה ב-$o(f(n))$.

אם נבצע סימולציה של $M$ על $10^k$ ולא על $w$, ייתכן ש-$M$ ו-$D$ מתנהגות אותו הדבר על כל קלט.

ייתכן ששתיהן דוחות את $10^k$ ומקבלות את $w$, או להפך.

כאשר $D$ רצה על $w$, היא מריצה את $M$ על $10^k$. מכיוון ש-$M$ דוחה (את $10^k$), $D$ מקבלת (את $w$), או להפך.

**שאלה 3**

להלן מכונה מתאימה:

"על קלט $w$ כאשר $w = 1^n$:

1. אתחל בסרט השני משתנה $x$ ל-0. ($x$ יהיה מיוצג בבינרי).
2. עבור על ה-1-ים של מילת הקלט.
3. לכל 1 כזה, הוסף 1 ל-$x$ שבסרט השני."

מעבר על ה-1-ים והגדלת המונה המתאים דורשת רק $O(n)$ צעדים: האורך המקסימלי של המונה הוא $O(\log n)$. בחצי מן ההגדלות מחליפים רק ספרה אחת, ברבע מהן מחליפים שתי ספרות, בשמינית מהן מחליפים שלוש ספרות, וכך הלאה. הסכום של הטור הזה הוא $O(n)$.

**שאלה 4**

א. הקלט: גרף לא מכוון מלא $G = (V, E)$ עם מחירים אי-שליליים על הקשתות; מספר אי-שלילי $m$.
השאלה: האם יש ב-$G$ מעגל המילטון שסכום מחירי הקשתות שלו אינו גדול מ-$m$.

ב. הבעיה שייכת ל-NP: מסמך אישור קצר: רשימה של $n$ קשתות כאשר $n = |V|$.
כדי לוודא את נכונות האישור, בודקים שמספר הקשתות הוא באמת $n$, שהקשתות מהוות מעגל המילטון ב-$G$ (אפשר להניח שהקשתות סדורות לפי סדר המעגל. אז צריך לבדוק שהצד השני של כל קשת הוא הצד הראשון של הקשת הבאה, שהצד השני של הקשת האחרונה הוא הצד הראשון של הקשת הראשונה, ושכל צומת מופיע פעם אחת כצד ראשון של קשת ופעם אחת כצד שני של קשת), ושסכום המחירים שלהן אינו גדול מ-$m$.
כל הבדיקות הללו ניתנות לביצוע בזמן פולינומיאלי.

רדוקציה של *UHAMCIRCUIT*: בהיתן קלט לבעיית *UHAMCIRCUIT* - גרף לא מכוון $G$, נבנה קלט לבעיית הסוכן הנוסע המטרית: נשלים את הקשתות החסרות ב-$G$ כך שנקבל גרף מלא. נקבע מחיר 1 לקשתות המקוריות של $G$ ומחיר 2 לקשתות החדשות שהוספנו. נקבע את $m$ להיות מספר הצמתים של $G$.
הרדוקציה תקפה: יש מעגל המילטון בגרף המקורי אם ורק אם יש בגרף החדש מעגל המילטון שמחירו כמספר הצמתים. (אם משתמשים בקשתות החדשות שהוספנו, מחיר המעגל יהיה גדול ממספר הצמתים, כי מחיר כל קשת חדשה הוא 2).
הרדוקציה ניתנת לחישוב בזמן פולינומיאלי: השלמת הקשתות החסרות וקביעת המחירים לקשתות ניתנת לביצוע בזמן פולינומיאלי. כך גם קביעת $m$ כמספר הצמתים של הגרף.

ג. תהי $T$ בעיית סוכן נוסע לא מטרית. נסמן על-ידי $max$ את מחיר הקשת היקרה ביותר בבעיה. נוסיף לכל הקשתות את $max$.
הבנייה הזו ניתנת לביצוע בזמן פולינומיאלי. נראה שהבעיה החדשה מקיימת את הדרישות.
מכיוון שהוספנו לכל הקשתות גודל קבוע, ומכיוון שבכל מעגל המילטון יש בדיוק $n$ קשתות (כאשר $n$ הוא מספר הצמתים בגרף), הוספנו למחיר של כל מעגל המילטון אותו גודל ($n \cdot max$).

לכן $P$ הוא מסלול אופטימלי בבעיה המקורית אם ורק אם $P$ מסלול אופטימלי בבעיה החדשה. כעת נראה שהבעיה החדשה היא מטרית. נסתכל על שלוש קשתות שיוצרות משולש. נניח שמחיריהן בבעיה המקורית הם $c_1$, $c_2$ ו-$c_3$. אז המחירים בבעיה החדשה הם $c_1+max$, $c_2+max$ ו-$c_3+max$. מכיוון ש- $max \geq c_i$ ל- $i = 1, 2, 3$, אז $c_1+max + c_2+max \geq c_3+max$.

ד. אין סתירה בין שתי התוצאות.

כאשר נעבור לבעיה המטרית בצורה שהצענו בסעיף הקודם, נוכל להפעיל עליה אלגוריתם קירוב, ולקבל מעגל המילטון שמחירו לכל היותר כפול ממחיר המעגל האופטימלי **בבעיה המטרית**. אבל צריך לזכור שלכל מעגל המילטון בבעיה החדשה נוסף גודל קבוע של $n{\cdot}max$.

נניח לדוגמה ש-$C$ הוא מעגל אופטימלי שמחירו $c$ בבעיה המקורית.

אז $C$ הוא מעגל אופטימלי גם בבעיה המטרית. מחירו בבעיה המטרית הוא $c+n{\cdot}max$.

אלגוריתם הקירוב ימצא מעגל $C'$ שמחירו אינו גדול מ-$2(c+n{\cdot}max)$.

בבעיה המקורית מחירו של $C'$ הוא לא יותר מאשר $2c+n{\cdot}max$.

אבל כל מעגל המילטון בבעיה המקורית הוא בעל מחיר שאינו גדול מ-$n{\cdot}max$. (להזכירכם, $max$ הוא מחיר הקשת היקרה ביותר בבעיה המקורית).

לכן $C'$ בגרף המקורי לא מהווה קירוב טוב ל-$C$ של הגרף המקורי.

**שאלה 5**

להלן האלגוריתם לבעיית האופטימיזציה:

"על קלט $\langle G\rangle$ כאשר $G$ הוא גרף לא מכוון:

1. אתחל משתנה $x$ ל-0.
2. בדוק, בעזרת האלגוריתם לבעיית ההכרעה, האם יש ב-$G$ חתך שגודלו לפחות $x$.
3. אם כן, $x = x+1$; לך ל-2.
4. אם לא, קבע את $k$ להיות $x–1$. ($k$ הוא גודל החתך המקסימלי).
5. אם יש קשתות שעדיין לא נבחרו, בחר קשת $e = (v, u)$ שעדיין לא נבחרה, מחק את $e$ מהגרף, ובדוק בעזרת אלגוריתם ההכרעה, האם עדיין יש חתך שגודלו $k$.
6. אם כן, אל תחזיר את $e$ לגרף, ציין ש-$v$ ו-$u$ שייכים לאותה תת-קבוצה, לך ל-5.
7. אם לא, החזר את $e$ לגרף, סמן שהיא נבחרה, ציין ש-$v$ ו-$u$ שייכים לקבוצות שונות, לך ל-5.
8. כאשר אין קשתות שלא נבחרו, יישארו $k$ קשתות שמהוות חתך בעל גודל מקסימלי ב-$G$. הצמתים של הגרף יחולקו לשתי קבוצות, כך שכל קשת מ-$k$ הקשתות מחברת צומת של אחת הקבוצות עם צומת של הקבוצה השנייה."

מכיוון שקוראים לאלגוריתם ההכרעה מספר פעמים שאיננו גדול מפעמיים מספר הקשתות של הגרף, ובכל קריאה כזו גודל הגרף איננו גדול מגודלו של הגרף המקורי $G$, זמן הריצה של האלגוריתם לבעיית האופטימיזציה פולינומיאלי אם זמן הריצה של האלגוריתם לבעיית ההכרעה פולינומיאלי.

**שאלה 6**

אם $t$ לא זר ל-$p$, אז גם כל חזקה של $t$ לא זרה ל-$p$. לכן האלגוריתם ידחה בשלב 4:

לא ייתכן ש- $t^{p-1}$ יהיה 1 מודולו $p$, משום שאז $t^{p-1} = kp+1$ ל-$k$ טבעי כלשהו.

נעביר אגפים ונקבל $t^{p-1} - kp = 1$.

צד ימין מתחלק במחלק המשותף של $t$ ו-$p$. לכן גם צד שמאל צריך להתחלק בו. לכן המחלק המשותף הזה חייב להיות 1, בסתירה לכך שיש ל-$t$ ול-$p$ מחלק משותף גדול מ-1.

**שאלה 7**

$\mathrm{RP} \cap \mathrm{coRP} \subseteq \mathrm{ZPP}$:

אם $A$ שייכת ל- $\mathrm{RP} \cap \mathrm{coRP}$, אז יש מכונה $M_1$ מסוג RP ל-$A$ ומכונה $M_2$ מסוג RP למשלימה של $A$.

נבנה מכונה מסוג ZPP ל-$A$:

"על קלט $w$:

1. הרץ פעמיים את $M_1$ על $w$. אם היא קיבלה לפחות באחת הפעמים, קבל.
2. הרץ פעמיים את $M_2$ על $w$. אם היא קיבלה לפחות באחת הפעמים, דחה.
3. החזר ?."

אם $w$ שייכת ל-$A$, אז ההסתברות שבשלב 1 היא לא תתקבל בשתי הפעמים איננה גדולה מ- $\frac{1}{4}$.

לכן ההסתברות שהיא תתקבל לפחות פעם אחת היא לפחות $\frac{3}{4}$.

אם היא התקבלה אפילו פעם אחת, היא שייכת בוודאות ל-$A$.

כמו כן, אם $w$ לא שייכת ל-$A$, היא בוודאות לא תתקבל בשתי הפעמים של שלב 2.

באופן סימטרי, אם $w$ לא שייכת ל-$A$, היא בוודאות לא תתקבל בשלב 1, וההסתברות שהיא תתקבל לפחות פעם אחת בשלב 2 היא לפחות $\frac{3}{4}$.

אם היא התקבלה אפילו פעם אחת בשלב 2, היא בוודאות שייכת למשלימה של $A$.

זמן הריצה של המכונה שבנינו פולינומיאלי.

$\mathrm{ZPP} \subseteq \mathrm{RP} \cap \mathrm{coRP}$:

אם $A$ שייכת ל-ZPP, אז יש מכונה מסוג ZPP ל-$A$. נניח שהפולינום המתאים למכונה הוא $p(x)$.

נבנה מכונה מסוג RP ל-$A$:

"על קלט $w$:

1. הרץ את המכונה של $A$ על $w$ $2p(|w|)$ צעדים.
2. אם היא קיבלה, קבל. אם היא דחתה, או החזירה ?, או לא סיימה, דחה."

אם $w$ לא שייכת ל-$A$, אז מכונת ZPP לא תקבל אותה. לכן במקרה זה $w$ תידחה בהסתברות 1.

אם $w$ שייכת ל-$A$, אז זמן הריצה הממוצע של מכונת ZPP על $w$ חסום על-ידי $p(|w|)$. לפי משפטים בהסתברות, זמן ריצה מעל $2p(|w|)$ יכול להיות רק למיעוט של ענפי החישוב. לכן ההסתברות

לקבלה גדולה מקבוע.

(אפשר גם לוותר על משפטים מתורת ההסתברות, ולהניח מראש שהפולינום $p(x)$ איננו זמן הריצה הממוצע אלא פולינום גדול יותר שמבטיח שרוב (גדול) של ענפי החישוב יסתיימו בתוך $p(|w|)$ צעדים).

זמן הריצה של המכונה שבנינו פולינומיאלי.

באופן סימטרי אפשר לבנות מכונת RP למשלימה של $A$.