קורס "מבוא לתורת החישוביות והסיבוכיות" (20585)

פתרון הבחינה לדוגמה סמסטר 2014א

שאלה 1

תהי L שפה שיש לה מאמת V.

נבנה מכונת טיורינג לא דטרמיניסטית M שמזהה את L, ובזה נוכיח ש-L מזוהה-טיורינג:

"על קלט w:

1. כתוב על הסרט מימין ל-w מילה כלשהי c באופן לא דטרמיניסטי.
2. שלח את $<w, c>$ למאמת V.
3. אם V קיבל, קבל; אחרת, דחה."

תהי L שפה מזוהה-טיורינג. תהי M מכונת טיורינג שמזהה את L.

נבנה מאמת V לשפה L:

"על קלט $<w, c>$ כאשר w ו-c הן מילים:

1. הרץ את M על w $|c|$ צעדים.
2. אם M קיבלה, קבל; אחרת, דחה."

w שייכת לשפה L אם ורק אם יש מחרוזת c כך ש-V מקבל את $<w, c>$.

שאלה 2

נראה רדוקצית מיפוי של המשלימה של A_{TM}:

"על קלט $<M, w>$ כאשר M היא מכונת טיורינג ו-w היא מחרוזת:

1. בנה את המכונה N הבאה:

   אלפבית הקלט של N יהיה $\{0,1\}$;

   אלפבית הסרט של N יהיה כמו של M בתוספת הסמלים 0 ו-1.

   N = "על קלט v:

   1. אם $v = 001$, דחה.
   2. אחרת, הרץ את M על w.
   3. אם M קיבלה את w, קבל; אחרת, דחה."

2. החזר את $<N>$.

$<M, w>$ שייכת למשלימה של A_{TM} אם ורק אם $<N>$ שייכת ל-T.

שאלה 3

שייכות ל-NP:

מסמך אישור קצר שמוכיח שיש ב-G קבוצה שלטת בגודל k הוא רשימת הצמתים השייכים לקבוצה שלטת כזו.

תחילה עוברים על רשימת הצמתים, ומוודאים שכל אחד מן הצמתים ברשימה שייך ל-V. כמו כן מוודאים שמספר הצמתים ברשימה הוא k.

לאחר מכן עוברים על כל הצמתים של הגרף G, ומוודאים ביחס לכל צומת כי או שהוא שייך לרשימה, או שהוא מחובר בקשת לצומת ששייך לרשימה.

את השלב הראשון אפשר לבצע בזמן פולינומיאלי ב-$|V|$.

את השלב השני אפשר לבצע בזמן פולינומיאלי ב- $|V||E|$.

רדוקציה פולינומיאלית של *VERTEX-COVER*:

תיאור הרדוקציה:

הרדוקציה מקבלת $<G, k>$ - קלט לבעיית *VERTEX-COVER*, ומחזירה $<H, m>$ - קלט לבעיית *DOMINATING-SET*.

הגרף H מכיל את כל הצמתים של הגרף G. בנוסף, לכל קשת (u, v) של G יהיה בגרף H הצומת uv.

הגרף H מכיל את כל הקשתות של הגרף G. בנוסף, לכל קשת (u, v) של G יהיו בגרף H הקשתות (u, uv) ו- (v, uv).

יהי n מספר הצמתים הבודדים ב-G (צמתים שלא קשורים בקשת לאף צומת). אז $m = k + n$.

פולינומיאליות הרדוקציה:

בניית הצמתים של הגרף H ניתנת לביצוע בזמן פולינומיאלי במספר הצמתים והקשתות של הגרף G. כך גם בניית הקשתות של הגרף H. וכך גם חישוב המספר m.

תקפות הרדוקציה:

נניח שיש ב-G כיסוי בצמתים שגודלו k. נוסיף לקבוצת הצמתים השייכים לכיסוי את כל הצמתים הבודדים בגרף G. קיבלנו קבוצת צמתים שגודלה m.

נסמן קבוצה זו ב-U ונראה שהיא קבוצה שלטת ב-H.

יהי w צומת ב-H. אם w הוא צומת בודד, אז הוא שייך ל-U.

אם w איננו בודד, אז או ש-w הוא צומת שנמצא גם ב-G, או ש-w הוא צומת חדש - $w = uv$.

אם w נמצא ב-G והוא איננו בודד, אז w מחובר בקשת לצומת x.

מכיוון ש-U היא כיסוי בצמתים של G, או w או x שייכים ל-U.

בכל מקרה w נשלט על-ידי צומת ב-U.

אם $w = uv$, אז יש ב-G הקשת (u, v).

מכיוון ש-U היא כיסוי בצמתים של G, או u או v שייכים ל-U.

ב-H נמצאות הקשתות (u, uv) ו-(v, uv). לכן w נשלט על-ידי צומת ב-U.

נניח שיש ב-H קבוצה שלטת בגודל m. נקרא לקבוצה הזו U.

U חייבת להכיל את כל הצמתים הבודדים.

כל צומת מהצורה uv ש-U מכילה שולט על עצמו, על u ועל v.

אפשר להחליף אותו ב-u או ב-v ועדיין U תהיה קבוצה שלטת ב-H. (ב-H נמצאות הקשתות (u, uv) ו- (v, uv), ולכן גם u ו-v שולטים על שלושת הצמתים הללו).

מסקנה: אפשר להניח ש-U מכילה את n הצמתים הבודדים ועוד k צמתים של G.

נקרא לקבוצה של k הצמתים הללו W. נראה ש-W היא כיסוי בצמתים ב-G.

תהי (u, v) קשת ב-G. הצומת uv ב-H יכול להישלט או על-ידי u או על-ידי v.

לכן או u או v (או שניהם) שייכים ל-W. לכן הקשת (u, v) מכוסה על-ידי צומת מ-W.

שאלה 4

נניח שיש שפה L שהיא NP-שלמה והיא שייכת ל-coNP. נראה ש- NP = coNP:

תהי A שפה ב-NP. כדי להראות ש-A שייכת ל- coNP, נראה ש- $\overline{A}$ שייכת ל-NP.

יש רדוקציה פולינומיאלית של A ל-L (כי A שייכת ל-NP, ו-L NP-שלמה).

לכן יש רדוקציה פולינומיאלית של $\overline{A}$ ל- $\overline{L}$.

L שייכת ל- coNP. לכן $\overline{L}$ שייכת ל-NP.

כלומר, יש רדוקציה פולינומיאלית של $\overline{A}$ לשפה ב-NP. לכן $\overline{A}$ שייכת ל-NP.

תהי B שפה ב- coNP. נראה ש-B שייכת ל-NP.

מכיוון ש-B שייכת ל- coNP, $\overline{B}$ שייכת ל-NP.

לכן יש רדוקציה פולינומיאלית של $\overline{B}$ ל-L.

לכן יש רדוקציה פולינומיאלית של B ל- $\overline{L}$.

מכיוון ש- $\overline{L}$ שייכת ל-NP (שהרי L שייכת ל- coNP), גם B שייכת ל-NP.

שאלה 5

נוכיח ש- $\overline{EQ_{\mathrm{DFA}}}$ שייכת ל-NL. מזה נקבל ש- $\overline{EQ_{\mathrm{DFA}}}$ שייכת ל- SPACE($\log^2 n$). ומזה נקבל ש- EQ_{DFA} שייכת ל- SPACE($\log^2 n$).

יהיו A ו-B שני האוטומטים הדטרמיניסטיים שהם הקלט לבעיה $\overline{EQ_{\mathrm{DFA}}}$.

נסמן על-ידי m את מספר המצבים של A ועל-ידי k את מספר המצבים של B.

אם נבנה את אוטומט המכפלה של שני האוטומטים הללו, נקבל אוטומט דטרמיניסטי שמספר מצביו אינו גדול מ-mk. אפשר להגדיר את המצבים של אוטומט המכפלה באופן שהוא יקבל את השפה $(L(A) - L(B)) \cup (L(B) - L(A))$.

השפות של שני האוטומטים שונות זו מזו, אם ורק אם השפה של אוטומט המכפלה הזה לא ריקה.

אם השפה שלו איננה ריקה, אז יש בה מילה באורך שאינו גדול מ-mk (מילה שמביאה מן המצב ההתחלתי למצב מקבל ללא שום לולאות בדרך).

לפי דרך הבנייה של אוטומט המכפלה הזה, מילה זו שייכת לשפה שמזהה אחד מהאוטומטים A ו-B, והיא לא שייכת לשפה שמזהה האוטומט השני.

מסקנה: אם שתי השפות של האוטומטים המקוריים שונות זו מזו, אז יש מילה שאורכה אינו גדול מ-mk ששייכת לשפה של אחד האוטומטים ואיננה שייכת לשפה של האוטומט השני.

המכונה הלא דטרמיניסטית תנסה למצוא מילה ששייכת לשפה של אחד האוטומטים ולא שייכת לשפה של האוטומט השני.

לשם כך היא תשמור את האות הבאה במילה הזו, את המצב שבו נמצא האוטומט A ואת המצב שבו נמצא האוטומט B. בנוסף היא תשמור מונה שיספור את האותיות של המילה עד עתה.

בכל שלב רושמים באופן לא דטרמיניסטי את האות הבאה של המילה (במקום האות שכתובה), מעדכנים את המצב שבו נמצאים באוטומט A ואת המצב שבו נמצאים באוטומט B, ומגדילים את המונה ב-1.

אם בשלב כלשהו מגיעים למצב מקבל באחד האוטומטים ולמצב לא מקבל באוטומט השני, עוצרים ומקבלים.

אם המונה הגיע ל-mk, עוצרים ודוחים.

המכונה שתיארנו פועלת במקום לוגריתמי והיא מכריעה את השפה $\overline{EQ_{\text{DFA}}}$.

שאלה 6

RP חלקית ל-NP: לכל שפה A ששייכת ל-RP, יש מכונת טיורינג הסתברותית ופולינומיאלית שמקבלת כל מילה ששייכת ל-A ולא מקבלת אף מילה שלא שייכת ל-A. אפשר לבנות מן המכונה הזו מכונה לא דטרמיניסטית שמקבלת את A בזמן פולינומיאלי לא דטרמיניסטי.

נוכיח שאם SAT שייכת ל-RP, אז NP חלקית ל-RP:

נזכיר ש-SAT היא NP-שלמה.

תהי B שפה ב-NP. נראה ש-B שייכת ל-RP:

יש רדוקציה פולינומיאלית של B ל-SAT.

נפעיל את הרדוקציה ונקבל נוסחה בוליאנית שהיא ספיקה אם ורק אם הקלט המקורי שייך ל-B.

נריץ על הנוסחה את המכונה ההסתברותית המתאימה ל-SAT.

מכיוון שלפי ההנחה SAT שייכת ל-RP, אם הנוסחה ספיקה, המכונה תקבל אותה בהסתברות של לפחות ½, ואם הנוסחה לא ספיקה, המכונה תדחה אותה בהסתברות 1. כמו כן זמן הריצה של המכונה פולינומיאלי בגודל של הנוסחה.

בסך הכל קיבלנו מכונה הסתברותית שמקבלת כל קלט מ-B בהסתברות לפחות ½, ודוחה כל קלט שלא שייך ל-B בהסתברות 1. כמו כן, גודל הנוסחה שמייצרת הרדוקציה פולינומיאלי בגודל הקלט המקורי. לכן זמן הריצה של המכונה שתיארנו פולינומיאלי בגודל הקלט. לכן B שייכת ל-RP.