פתרון שאלות בממ"ן 13 סמסטר 2016א

שאלה 2

א. השפה שמזהה אוטומט סופי לא דטרמיניסטי היא אינסופית אם ורק אם יש באוטומט מסלול מהמצב ההתחלתי אל מצב מקבל שיש בו (במסלול) מעגל.

אפשר תחילה (למשל, בעזרת חיפוש לרוחב) למצוא את כל המצבים שהם בני הגעה מן המצב ההתחלתי.

לאחר מכן, לכל מצב q שהוא בר הגעה, מוצאים (למשל, בעזרת חיפוש לרוחב) את כל המצבים שהם בני הגעה מ-q, ובודקים האם q בר הגעה מ-q (יש מעגל) והאם יש מצב מקבל שהוא בר הגעה מ-q. אם נמצא מצב q כזה, מקבלים. אחרת, דוחים.

זמן הריצה: מבצעים $O(n)$ פעמים חיפוש לרוחב, כאשר n הוא מספר המצבים באוטומט. חיפוש לרוחב ניתן לביצוע בזמן פולינומיאלי בגודל הקלט. לכן זמן הריצה פולינומיאלי.

ב. לכל זוג מצבים p ו-q, מבצעים חיפוש (למשל, לרוחב) מ-p, כדי לדעת האם יש בגרף מסלול מ-p ל-q.

זמן הריצה: מספר זוגות המצבים הוא מסדר גודל של n^2. חיפוש לרוחב ניתן לביצוע בזמן פולינומיאלי בגודל הגרף. לכן זמן הריצה פולינומיאלי.

שאלה 3

ההוכחה לא טובה.

הזמן הדרוש להרצת M על w t צעדים הוא לפחות t.

הזמן הזה (t צעדים) איננו פולינומיאלי בגודל הקלט. אפשר לייצג את המספר t בקלט במקום לוגריתמי ב-t (למשל, בייצוג בינרי), ואז מספר הצעדים t הוא אקספוננציאלי בייצוג של t.

שאלה 4

על קלט $\langle n \rangle$, האימות יהיה הפירוק לגורמים של n: $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$.

המאמת יוודא שכל אחד מן הגורמים $p_1, p_2, \ldots, p_k$ הוא מספר ראשוני.

המאמת יוודא שאכן $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$.

המאמת יוודא שבאמת n שווה לסכום המחלקים שלו הקטנים ממנו.

אם אחת הבדיקות תיכשל, המאמת ידחה. אחרת, הוא יקבל.

כעת נסביר כיצד מתבצע כל שלב, ולמה זמן הריצה של כל שלב פולינומיאלי בגודל הקלט.

כל ראשוני איננו קטן מ-2. לכן מספר הגורמים הראשוניים (k) הוא $O(\log n)$. כלומר, ליניארי בגודל הקלט.

אפשר לבדוק בזמן פולינומיאלי האם מספר הוא ראשוני. לכן אפשר לבדוק בזמן פולינומיאלי האם כל אחד מן הגורמים $p_1, p_2, \ldots, p_k$ הוא באמת ראשוני.

אורך הקלט הוא לפחות $m_1+m_2+\cdots+m_k$ (בדקו!). לכן חישוב $p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$ ניתן לביצוע בזמן פולינומיאלי בגודל הקלט. גם ההשוואה של $p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$ ל-n ניתנת לביצוע בזמן פולינומיאלי.

כל מחלק של n הוא מהצורה $p_1^{d_1}p_2^{d_2}\cdots p_k^{d_k}$ כאשר לכל $1\le i\le k$, $d_i\le m_i$.

לכן הסכום של כל המחלקים, כולל n עצמו, שווה ל-

$$(1+p_1+p_1^2+\cdots+p_1^{m_1})(1+p_2+p_2^2+\cdots+p_2^{m_2})\cdots(1+p_k+p_k^2+\cdots+p_k^{m_k})$$

המכפלה הזו ניתנת לחישוב בזמן פולינומיאלי. (שימו לב שכל אחד מן הגורמים הוא סכום של טור הנדסי).

ההשוואה של תוצאת המכפלה הזו ל-$2n$ ניתנת גם היא לביצוע בזמן פולינומיאלי.

(משווים ל-$2n$ כי סכום כל המחלקים כולל גם את n).

שאלה 5

א. "על קלט $<M, w>$ כאשר M מכונת טיורינג ו-w מילה:

1. החלף ב-M כל כניסה למצב q_{reject} בכניסה למצב q_{accept}.
   תהי M' המכונה שהתקבלה.
2. החזר את $<M', w>$."

הרדוקציה ניתנת לחישוב בזמן פולינומיאלי בגודל הקלט. (מעבר על פונקציית המעברים של M).

ב. לא קיימת רדוקצית מיפוי של ALL_{TM} ל-E_{TM}, כי המשלימה של ALL_{TM} איננה מזוהה-טיורינג והמשלימה של E_{TM} כן מזוהה-טיורינג.

שאלה 8 סעיף א

a. תהי σ השמת-≠. בכל פסוקית יש ליטרל שערכו 1 ויש ליטרל שערכו 0.
אם נהפוך את הערך שנתנו לכל משתנה, יהיה בכל פסוקית ליטרל שערכו 0 וליטרל שערכו 1.
לכן גם זו השמת-≠.

b. הרדוקציה המוצעת תקפה:
נניח שהנוסחה המקורית ספיקה. נוכיח שלנוסחה שנבנתה על-ידי הרדוקציה יש השמת-≠:
לנוסחה המקורית יש השמה שבה לפחות אחד מתוך y_1, y_2, y_3 מקבל ערך 1.
נקבע ל-b ערך 0. אם ל-y_1 או ל-y_2 נקבע ערך 1, אז נקבע ל-z_i ערך 0.
אם גם ל-y_1 וגם ל-y_2 נקבע ערך 0, אז בהכרח ל-y_3 נקבע ערך 1. במקרה זה נקבע ל-z_i ערך 1.
בכל מקרה יש לנוסחה שנבנתה השמת-≠.

נניח שלנוסחה שנבנתה על-ידי הרדוקציה יש השמת-≠, ונוכיח שהנוסחה המקורית ספיקה:
לפי מה שהראינו בסעיף a, אפשר להניח שבהשמת-≠ של הנוסחה שנבנתה ערכו של b הוא 0.
אם ערכו של z_i הוא 0, אז אחד מתוך y_1, y_2 חייב לקבל ערך 1.

אם ערכו של z_i הוא 1, אז ערכו של y_3 חייב להיות 1.

בכל מקרה, לפחות אחד מתוך y_3 ,y_2 ,y_1 מקבל ערך 1. כלומר, הנוסחה המקורית ספיקה.

קל להראות שהרדוקציה המוצעת ניתנת לחישוב בזמן פולינומיאלי.

c. הרדוקציה של סעיף b ניתנת לחישוב בזמן פולינומיאלי. לכן $3SAT \leq_P \neq SAT$.

הוכיחו ש- $\neq SAT$ שייכת ל-NP ותקבלו ש- $\neq SAT$ היא NP-שלמה.