

Computability and Complexity.

Homework 2

1. Let M is a poly-time DTM, $L=L(M)$, M' is a poly-time NTM, and $L'=L(M')$. What of the following is true? Explain why. If you cannot approve or disprove a statement, explain what of the unsolved problem is involved here.
 - a. $L, L' \in P$
 - b. $L, L' \in NP$
 - c. $L, L' \in R$
 - d. $L \cap L' \in P$
 - e. If L' is NP-hard then there is a poly-time reduction from L to L'
 - f. $L, L' \in PSPACE$
2. Let $A \in DTIME(n^2)$, $A \in SPACE(n)$ is an algorithm for modular multiplication (i.e. $A(x,y,m)=xy \bmod m$ when $|x|=|y|=|m|=n$). Build a deterministic poly-time algorithm for modular exponentiation $B(x,z,m)=x^z \bmod m$, when $|x|=|z|=|m|=n$. What time and space complexity does it have?
Hint: use algorithm A as a building block (a black box).
3. Prove or refute $DTIME(n^2) \setminus DTIME(n^{1.9}) \neq \emptyset$ (here, “\” stands for set minus, “ \emptyset ” stands for empty set).
4. Are the following languages RE-complete? R-complete? NP-complete? P-complete? PSPACE-complete? NL-complete? Why?
 - a. $3SAT = \{<\phi> | \phi \text{ is a satisfiable 3CNF}\}$
 - b. $EQ_{TM} = \{<M, M'> | L(M) = L(M')\}$
 - c. $PATH = \{<G, s, t> | G \text{ is a directed graph, and there is a path from node } s \text{ to node } t\}$
5. Show that if $L, L' \in NL$ then $L^* = \{xy | x \in L, y \in L'\} \in NL$
6. Prove that if L is PSPACE-hard then it is NP-hard.
7. An LBA (linearly bounded automaton) is a single-tape DTM with linearly bounded tape size (the number of cells equals to cn for some constant c and input length n). To what time and space complexity classes does the following language belong?
 $A_{LBA} = \{<M, x> | M \text{ is an LBA accepting } x\}$
8. Prove that $L = \{<M, x, t> | \exists w: \text{a DTM } M(x, w) \text{ stops in } \leq t \text{ steps}\}$ is NP-hard.
Hint: use 2 alternative definitions of NP

חישוביות וסיבוכיות

מטלה 2

1. תהי מכונה דטרמיניסטית M ונסמן $(M=L)$. תהי מכונה לא דטרמיניסטית $'M$ ונסמן $('M=L')$. אילו מהטענות הבאות נכונות? הסבירו מדוע. אם לא ניתן להוכיח או להפריך את הטענה, הסבירו איזו בעיה פתוחה קשורה.

- $L, L' \in P$.a
- $L, L' \in NP$.b
- $L, L' \in R$.c
- $L \cap L' \in P$.d
- אם L' הוא NP-hard אז קיימת רדוקציה פולינומית מ L אל L' .e
- $L, L' \in PSPACE$.f

2. יהי (n) $A \in DTIME(n^2)$, $A \in SPACE(n^2)$ אלגוריתם שמחשב כפל מודולרי (כלומר $m \mod xy = xy \mod (x,y,m)$ עבור $|x|=|y|=|m|=n$) בנו אלגוריתם דטרמיניסטי פולינומי עבור הולה בחזקת מודולרית, $m \mod xz = xz \mod m$ עבור $n=|m|=|z|=|x|$. איזו סיבוכיות מקומ וזמן יש לו?
רמז: השתמשו באלגוריתם A בתור קופסה שחורה.

3. הוכיחו או הפריכו $\emptyset \neq DTIME(n^{1.9}) \setminus DTIME(n^2)$ (כאן "\\", מסמן חיסור בין קבוצות " \emptyset ", מסמן את הקבוצה הריקה).

4. עבור השפות הבאות הסבירו האם הם (ומדוע):

RE-complete? R-complete? NP-complete? P-complete? PSPACE-complete?
NL-complete?

$3SAT = \{<\phi> | \phi \text{ is a satisfiable 3CNF}\}$.a
 $EQ_{TM} = \{<M, M'> | L(M) = L(M')\}$.b
 $PATH = \{<G, s, t> | G \text{ is a directed graph, and there is a path from node } s \text{ to }$.c
 $\text{node } t\}$

5. הראו שגם $L^* = \{xy | x \in L, y \in L'\} \in NL$ אך $L \in NL$, $L' \in NL$

6. הוכיחו כי אם L הוא NP-hard. PSPACE-hard.

7. (לינארי LBA (linearly bounded automaton) זהה מכונה דטרמיניסטית עם סרט אחד עם זיכרון לינארי (כלומר, עבור קבוע c , לכל קלט באורך n יש כנZN זיכרון). לאיזה מחלקות זמן ומקום השפה הבאה שייכת?

$ALBA = \{<M, x> | M \text{ is an LBA accepting } x\}$

8. הוכיחו כי $\{<M, x, t> | \exists w: \text{a DTM } M(x, w) \text{ stops in } \leq t \text{ steps}\}$ הוא NP-hard.
רמז: השתמשו בשתי ההגדרות של NP.