

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, " \setminus " 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. $3SAT = \{ \langle \phi \rangle \mid \phi \text{ is a satisfiable 3CNF} \}$
 - b. $EQ_{TM} = \{ \langle M, M' \rangle \mid L(M) = L(M') \}$
 - c. $PATH = \{ \langle G, s, t \rangle \mid G \text{ is a directed graph, and there is a path from node } s \text{ to node } t \}$
5. Show that if $L, L' \in NL$ then $L^* = \{ xy \mid x \in L, y \in L' \} \in NL$
6. Prove that if L is PSPACE-hard then it is NP-hard.
7. An LBA (linearly bounded automat) 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?
 $A_{LBA} = \{ \langle M, x \rangle \mid M \text{ is an LBA accepting } x \}$
8. Prove that $L = \{ \langle M, x, t \rangle \mid \exists w: \text{ a DTM } M(x, w) \text{ stops in } \leq t \text{ steps} \}$ is NP-hard.
Hint: use 2 alternative definitions of NP

חשוביות וסיבוכיות

מטלה 2

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

a. $L, L' \in P$

b. $L, L' \in NP$

c. $L, L' \in R$

d. $L \cap L' \in P$

e. אם L' הוא NP-hard אז קיימת רדוקציה פולינומית מ L אל L'

f. $L, L' \in PSPACE$

2. יהי $A \in DTIME(n^2), A \in SPACE(n)$ אלגוריתם שמחשב כפל מודולרי (כלומר $A(x,y,m)=xy \bmod m$ עבור $|x|=|y|=|m|=n$). בנו אלגוריתם דטרמיניסטי פולינומי עבור העלה בחזקה מודולרית, $B(x,z,m)=x^z \bmod m$, עבור $|x|=|z|=|m|=n$. איזו סיבוכיות מקום וזמן יש לו? רמז: השתמשו באלגוריתם A בתור קופסא שחורה.

3. הוכיחו או הפריכו $DTIME(n^2) \setminus DTIME(n^{1.9}) \neq \emptyset$ (כאן " \setminus ", 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?

a. $3SAT = \{ \langle \phi \rangle \mid \phi \text{ is a satisfiable 3CNF} \}$

b. $EQ_{TM} = \{ \langle M, M' \rangle \mid L(M) = L(M') \}$

c. $PATH = \{ \langle G, s, t \rangle \mid G \text{ is a directed graph, and there is a path from node } s \text{ to node } t \}$

5. הראו שאם $L^* = \{ xy \mid x \in L, y \in L' \} \in NL$ אז $L, L' \in NL$

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

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

$ALBA = \{ \langle M, x \rangle \mid M \text{ is an LBA accepting } x \}$

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