תרגיל 1

נב"ש ש- $NP = DTIME(n)$.

נגיע עם זה למסקנה ש- $DTIME(n^3) = DTIME(n)$.

תהי שפה $L \in DTIME(n^3)$, ונרצה למצוא לה מ"ט שמכריעה אותה בזמן $O(n)$.

קיימת מכונה M_L שמכריעה את L בזמן $O(n^3)$.

נגדיר:

$$L_{pad} = \{x0^{|x|^3-|x|} \,:\, x \in L\}$$

נבנה מכונה $M_{L_{pad}}$: על קלט y, מגדירה את x להיות ה- $\sqrt[3]{|y|}$ תווים הראשונים של y. ומחזירה $M_L(x)$.

$M_L(x)$ עובדת בזמן $O(|x|^3)$, כלומר בזמן $O(|y|)$ כי $|x|^3 = \sqrt[3]{|y|}^3 = |y|$.

כלומר $M_{L_{pad}}$ מכריעה את L_{pad} בזמן $O(n)$. אז $L_{pad} \in DTIME(n)$.

אז מההנחה ש- $NP = DTIME(n)$, נקבל ש- $L_{pad} \in NP$.

אז קיימת $N_{L_{pad}}$ א"ד שמכריעה את L_{pad} בזמן פולינומי.

נבנה מכונה N_L שמכריעה את L בזמן $O(n)$:

על קלט x, נרפד: נגדיר

$$y = x0^{|x|^3-|x|}$$

ונריץ את $N_{L_{pad}}(y)$. זה רץ בזמן $O(|y|)$, שזה $O(|x|^3)$. זה זמן פולינומי, אז $L \in NP$.

ומההנחה ש- $NP = DTIME(n)$, נקבל ש- $L \in DTIME(n)$, כלומר $DTIME(n) = DTIME(n^3)$, בסתירה להירככיית הזמן.

תרגיל 2

נניח ש- $DTIME(n) = DTIME(n^2)$.

תהי שפה $L \in DTIME(n^4)$. נמצא מכונה שמכריעה אותה בזמן $O(n^2)$, וזה יוכיח ש- $DTIME(n^4) = DTIME(n^2)$.

קיימת מ"ט M_L שמכריעה את L בזמן $O(n^4)$.

נגדיר:

$$L_{pad} = \{x0^{|x|^2-|x|} : x \in L\}$$

$$x = abc \to |x| = 3, 3^2 = 9, 9 - 3 = 6 \to y = abc000000 \to |y| = |x|^2$$

נבנה מ"ט $M_{L_{pad}}$: על קלט y, היא לוקחת את $\sqrt{|y|}$ התווים הראשונים וקוראת להם x.

1. בודקת שכל השאר זה אפסים.
2. מריצה ומחזירה את $M_L(x)$ – בזמן $O(|x|^4)$.

$$|x| = \sqrt{|y|}$$

היא מכריעה את L_{pad} בזמן $O(|x|^4)$ שזה $O\left(\left(y^{1/2}\right)^4\right) = O\left(\sqrt{y}^4\right)$ שזה $O(|y|^2)$.

אז $L_{pad} \in DTIME(n^2)$. ומההנחה ש- $DTIME(n) = DTIME(n^2)$, נקבל ש- $L_{pad} \in DTIME(n)$.

כלומר קיימת מ"ט $N_{L_{pad}}$ שמכריעה את L_{pad} בזמן $O(n)$.

נבנה מכונה N_L שמכריעה את L בזמן $O(n^2)$.

על קלט x, נגדיר $y = x0^{|x|^2-|x|}$, אז $|y| = |x|^2$.

היא מריצה את $N_{L_{pad}}(y)$. זה קורה בזמן $O(|y|) = O(|x|^2)$.

כלומר $L \in DTIME(n^2)$.

תרגיל 3

צ"ל: $DTIME\left(2^{\sqrt{n}}\right) \neq NP$.

נב"ש שהם שווים, ונגיע למסקנה ש- $DTIME(2^n) = DTIME\left(2^{\sqrt{n}}\right)$, בסתירה להירכיית הזמן.

תהי שפה $L \in DTIME(2^n)$. כלומר קיימת לה מ"ט M_L שמכריעה אותה בזמן $O(2^n)$.

נגדיר:

$$L_{pad} = \left\{x0^{|x|^2-|x|} : x \in L\right\}$$

נתאר מ"ט $M_{L_{pad}}$ שמכריעה אותה. בהינתן קלט y:

1. ניקח את $\sqrt{|y|}$ התווים הראשונים – נקרא להם x.
2. נוודא שכל שאר התווים הם 0. $O(|y|)$
3. נריץ ונחזיר את $M_L(x)$. $O\left(2^{|x|}\right) = O\left(2^{\sqrt{|y|}}\right)$

אז $M_{L_{pad}}$ רצה בזמן $O\left(2^{\sqrt{|y|}}\right)$, כלומר $L_{pad} \in DTIME\left(2^{\sqrt{n}}\right)$. אז מההנחה, $L_{pad} \in NP$.

כלומר קיימת מ"ט א"ד $N_{L_{pad}}$ שמכריעה את L_{pad} בזמן פולינומי.

נבנה מ"ט N_L שמכריעה את L בזמן פולינומי.

על קלט x, נרפד את x:

$$y = x0^{|x|^2-|x|}$$

ונריץ ונחזיר את $N_{L_{pad}}(y)$.

$N_{L_{pad}}(y)$ רצה בזמן פולינומי א"ד בגודל של y, שזה:

$$O(|y|^c) = O((|x| + |x|^2 - |x|)^c) = O((|x|^2)^c) = O(|x|^{2c})$$

שזה מקום פולינומי א"ד ב- $|x|$. אז $L \in NP$, ומההנחה ש- $DTIME\left(2^{\sqrt{n}}\right) = NP$, נקבל $L \in DTIME\left(2^{\sqrt{n}}\right)$.

אז $DTIME(2^n) = DTIME\left(2^{\sqrt{n}}\right)$, בסתירה להירכיית הזמן.

תרגיל 4

צ"ל $DSPACE(n) \neq NL$. נב"ש שהם שווים, נגיע למסקנה ש- $DSPACE(n) = DSPACE(n^2)$. שזו סתירה ל-THT.

תהי $L \in DSPACE(n^2)$.

נגדיר:

$$L_{pad} = \left\{x0^{|x|^2-|x|} : x \in L\right\}$$

נתאר מ"ט $M_{L_{pad}}$ שמכריע אותה. בהינתן y:

1. ניקח את $\sqrt{y}$ התווים הראשונים – נקרא להם x.
2. נוודא שכל שאר התווים הם 0.
3. נריץ ונחזיר את $M_L(x)$.

$M_L(x)$ רצה במקום $|y| = \sqrt{y}^2 = |x|^2$. כלומר $L_{pad} \in DSPACE(n)$.

מההנחה ש- $DSPACE(n) = NL$, נקבל שקיימים מ"ט א"ד $N_{L_{pad}}$ שמכריעה את L_{pad} במקום לוגריתמי.

נתאר מ"ט N_L שמכריעה את L במקום $O(n)$:

בהינתן x, נרפד אותו: $y = x0^{|x|^2-|x|}$.

נריץ ונחזיר את $N_{L_{pad}}(y)$. זה רץ במקום לוגריתמי ב- $|y|$, שזה מקום לינארי ב- $|x|$.

כלומר $L \in DSPACE(n)$. אז $DSPACE(n) = DSPACE(n^2)$. בסתירה ל-THT.

תרגיל 5

צ"ל $NL \neq DTIME(n)$. נב"ש שהם שווים ונגיע למסקנה ש- $DTIME(n) = DTIME(n^2)$, בסתירה ל-THT.

תהי שפה $L \in DTIME(n^2)$ כלומר קיים M_L DTM המכריע אותה בזמן $O(n^2)$. נגדיר:

$$L_{pad} = \{x0^{|x|^2-|x|} : x \in L\}$$

נתאר אלגוריתם עבורה: בהינתן y:

1. נמצא את $\sqrt{|y|}$ ונגדיר $x \leftarrow y[0:\sqrt{|y|}]$.
2. נוודא שכל השאר אפסים.
3. נריץ ונחזיר את $M_L(x)$.

זה לוקח זמן $O(|y|) = O\left(\sqrt{|y|}^2\right) = O(|x|^2)$, אז $L_{pad} \in DTIME(n)$.

ומההנחה ש- $NL = DTIME(n)$, נקבל $L_{pad} \in NL$.

נתאר אלגוריתם N_L ל-L. בהינתן x:

1. נרפד את x: $y = x0^{|x|^2-|x|}$.
2. נריץ ונחזיר את $M_{L_{pad}}(y)$.

זה רץ במקום $O(\log|y|) = O(\log|x|^2) = O(2\log|x|) = O(\log|x|)$. אז $L \in NL$. ומההנחה ש- $NL = DTIME(n)$, נקבל $L \in DTIME(n)$.

כלומר $DTIME(n) = DTIME(n^2)$, בסתירה ל-THT.

תרגיל 6

הוכח או הפרך: כל $L \in NP$ ניתנת לרדוקציה ל-$HALT$, ע"י רדוקציה *many-to-one* פולינומית.

הוכחה: מכיוון ש- $L \in NP$, קיימת מ"ט דטרמיניסטית M שמכריעה את L בהינתן עד w מתאים. נבנה מכונה N שמריצה את M עם כל w אפשרי, ועוצרת אם מצאנו w מתאים כך ש-M מקבלת. אם היא לא מקבלת, נמשיך לרוץ.

בהינתן x, נחזיר את $\langle N, x\rangle$. N מריצה את $M(x,w)$ לכל w אפשרי. אם $N(x)$ עוצרת, אז קיים w. אחרת, לא קיים.

$$x \in L \Leftrightarrow N(x) \in HALT$$

הבנייה של המכונה N היא פולינומית – כי רק צריך "לעטוף" את M בהוראות, לא צריך להריץ או לסמלץ דברים. אז $L \leq_p HALT$.

תרגיל 7

הוכח או הפרך: כל שפה שהיא *PSPACE-hard* היא גם *NP-hard*.

הוכחה: אם שפה היא *PSPACE-hard*, יש רדוקציה פולינומית מכל שפה ב-*PSPACE* אליה. וכל שפה ב-*NP* היא גם ב-*PSPACE* כי $NP \subseteq PSPACE$.

תרגיל 8

סיווג מינימלי לשפה:

$$\{a\#b\#c : a,b,c > 0 \;\; \land \;\; a+b=c\}$$

אלגוריתם נאיבי: בדיקת תקינות (גדולים מ-0), חיבור $a+b$ והשוואה ל-c. $PSPACE$, P.

אלגוריתם אופטימלי: במקום לשמור את תוצאת החיבור, לבדוק כל ביט מול c (ולא לשמור). צריך מקום לוגריתמי בשביל קאונטרים. L, P.

תרגיל 9

P^{SAT} – קבוצת כל השפות שיש להן DTM שמכריע אותן בזמן פולינומי, **אם** יש אורקל ל-SAT.

תהי $L \in NP$. אז יש רדוקציה f פולינומית $L \leq_p SAT$.

אז אם יש אורקל ל-SAT, יש אלגוריתם פולינומי ל-L:

1. ניקח $x \in_? L$.
2. נייצר את $f(x)$. - $f(x) \in_? SAT$. פולינומי.
3. נבדוק אם $f(x) \in SAT$. $O(1)$
4. אם כן, אז $x \in L$.

אז יש ל-L DTM שמכריע אותה בזמן פולינומי, **אם** יש אורקל ל-SAT. אז $L \in P^{SAT}$.

$$NP \subseteq P^{SAT}$$

תרגיל 10

נמצא סיווג מינימלי מתוך $R, RE, coRE, \overline{RE \cup coRE}$ לשפה:

$$L = \{M : L(M) \text{ is finite}\}$$

כדי להראות ש- $L \notin RE$, נשתמש במשפט רייס החזק:

1. התכונה היא תכונה לא טריוויאלית: המכונה M_{accept} לא מקיימת, והמכונה M_{reject} כן מקיימת.
2. התכונה היא תכונה של שפה: אם יש שתי מכונות שמקבלות את אותה שפה, לא אפשרי שאחת תהיה אינסופית והשנייה לא.
3. השפה הריקה מקיימת את התכונה, אז $L \notin RE$.

כדי להראות ש- $L \notin coRE$, נראה רדוקציה $SHALT \leq L$:

בהינתן $M \in_? SHALT$, נייצר את M'. אנחנו רוצים שיתקיים:

$$M \in SHALT \Leftrightarrow L(M') \text{ is finite}$$

M' על קלט $x \in \{0,1\}^*$:

1. מריצה את $M(\varepsilon)$ למשך x צעדים. (נתייחס לקלט בתור מספר בינארי).
2. אם $M(\varepsilon)$ עצרה בזמן הזה, נדחה.
3. אחרת, נקבל.

אם $M(\varepsilon)$ לא עוצרת, אז לכל x שנבדוק, לא נעצור תוך x צעדים. אז נקבל כל x, כלומר $|L(M')| = \infty$.

ואם $M(\varepsilon)$ כן עוצרת, אז החל ממקום מסויים, כל x שנבדוק, $M(\varepsilon)$ תעצור בזמן הזה אז נדחה. כלומר נקבל רק מספר סופי של x, אז $|L(M')| \neq \infty$.

$$M \notin SHALT \Longrightarrow \forall x: M'(x) = 1 \Longrightarrow M' \notin L$$

$$M \in SHALT \Longrightarrow \exists t: \forall x > t: M'(x) = 0 \Longrightarrow M' \in L$$

תרגיל 11

נמצא סיווג מינימלי מתוך $R, RE, coRE, \overline{RE \cup coRE}$ לשפה:

$$L = \{M : L(M) \text{ is infinite}\}$$

כדי להראות ש- $L \notin coRE$, נשתמש במשפט רייס החזק:

1. התכונה היא תכונה לא טריוויאלית: המכונה M_{accept} לא מקיימת, והמכונה M_{reject} כן מקיימת.
2. התכונה היא תכונה של שפה: אם יש שתי מכונות שמקבלות את אותה שפה, לא אפשרי שאחת תהיה אינסופית והשנייה לא.
3. השפה הריקה לא מקיימת את התכונה, אז $L \notin coRE$.

כדי להראות ש- $L \notin RE$, נעשה רדוקציה $\overline{SHALT} \leq L$:

בהינתן $M \in_? \overline{SHALT}$, נייצר את M'. אנחנו רוצים שיתקיים:

$$M \in \overline{SHALT} \Leftrightarrow L(M') \text{ is infinite}$$

M' על קלט $x \in \{0,1\}^*$:

1. מריצה את $M(\varepsilon)$ למשך x צעדים. (נתייחס לקלט בתור מספר בינארי).
2. אם $M(\varepsilon)$ עצרה בזמן הזה, נדחה.
3. אחרת, נקבל.

אם $M(\varepsilon)$ לא עוצרת, אז לכל x שנבדוק, לא נעצור תוך x צעדים. אז נקבל כל x, כלומר $|L(M')| = \infty$.

ואם $M(\varepsilon)$ כן עוצרת, אז החל ממקום מסויים, כל x שנבדוק, $M(\varepsilon)$ תעצור בזמן הזה אז נדחה. כלומר נקבל רק מספר סופי של x, אז $|L(M')| \neq \infty$.

$$M \in \overline{SHALT} \Longrightarrow \exists t: \forall x > t: M'(x) = 1 \Longrightarrow M' \in L$$

$$M \notin \overline{SHALT} \Longrightarrow \forall x: M'(x) = 0 \Longrightarrow M' \notin L$$

$$L_1 = \{\langle M_1, M_2\rangle \mid L(M_1) \setminus L(M_2) \neq \varnothing\}$$

(which is $\overline{L_2}$), and

$$L_2 = \{\langle M_1, M_2\rangle \mid L(M_1) \subseteq L(M_2)\}.$$

$$L_1 = \{\langle M_1, M_2\rangle : L(M_1) \setminus L(M_2) \neq \emptyset\}, \qquad L_2 = \{\langle M_1, M_2\rangle : L(M_1) \subseteq L(M_2)\} = \overline{L_1}, \qquad L_1, L_2 \in \overline{RE \cup coRE}$$

$L_1 \notin coRE$ ע"י רדוקציה מ-$HALT$: בהינתן M, x נייצר את $f(M,x) = A, B$:

A על קלט y: מריצה את $M(x)$ ואז מקבלת. B דוחה הכל.

אז אם $M(x) \in HALT$, A תקבל הכל ואז $L(A) \setminus L(B) = \Sigma^* \neq \emptyset$. כלומר $M(x) \in HALT \Longrightarrow f(M,x) \in L_1$.

ואם $M(x) \notin HALT$, אז A לא מקבלת כלום ואז $L(A) \setminus L(B) = \emptyset \setminus \emptyset = \emptyset$. כלומר $M(x) \notin HALT \Longrightarrow f(M,x) \notin L_1$.

אז $L_2 \notin RE$ כי אחרת, L_1 הייתה ב-$coRE$.

$L_1 \notin RE$ ע"י רדוקציה מ- $\overline{HALT}$: בהינתן M, x נייצר את $f(M,x) = A, B$:

B על קלט y: מריצה את $M(x)$ ואז מקבלת. A מקבלת הכל.

אז אם $M(x) \in \overline{HALT}$, B לא תקבל כלום ואז $L(A) \setminus L(B) = \Sigma^* \setminus \emptyset \neq \emptyset$. כלומר $M(x) \in \overline{HALT} \Longrightarrow f(M,x) \in L_1$.

ואם $M(x) \notin \overline{HALT}$, אז B מקבלת הכל ואז $L(A) \setminus L(B) = \Sigma^* \setminus \Sigma^* = \emptyset$. כלומר $M(x) \notin \overline{HALT} \Longrightarrow f(M,x) \notin L_1$.

אז $L_2 \notin coRE$ כי אחרת, L_1 הייתה ב-RE.

חישוביות (קיץ תשפ"ו)

$$MULT = \{a\#b\#c : a, b, c \text{ are natural nums in binary, s.t. } ab = c\}$$

אלגוריתם: נחשב את ab לפי ביטים – כל פעם נשמור רק את הביט של תוצאת הכפל (והחיבור בין לבין, בתוך העמודה). אם יש ביט שונה – נדחה. אם הגענו לסוף של c לפני הסוף של ab או הפוך – נדחה.

זה דורש מקום לוגריתמי (כל חישוב של ביט והחיבור, ספירה של הגודל של הקלטים). אז L ולכן גם P.

prove that $NL \neq DTIME(n)$

נב"ש ש- $NL = DTIME(n)$. ונגיע למסקנה ש- $DTIME(n) = DTIME(n^2)$, בסתירה ל-THT.

תהי $L \in DTIME(n^2)$. אז קיים לה DTM M_L שמכריע אותה בזמן $O(n^2)$.

נגדיר את השפה:

$$L_{pad} = \left\{x0^{|x|^2-|x|} : x \in L\right\}$$

נתאר DTM עבורה. בהינתן y:

1. ניקח את $x = y\left[0{:}\sqrt{y}\right]$.
2. נוודא שכל שאר המקומות של y הם 0.
3. נריץ ונחזיר את $M_L(x)$.

$M_L(x)$ רץ בזמן $O(|y|) = O\left(\sqrt{|y|}^2\right) = O(|x|^2)$. כלומר $L_{pad} \in DTIME(n)$.

אז מההנחה ש- $NL = DTIME(n)$, מתקיים $L_{pad} \in NL$ כלומר קיים לה NTM $N_{L_{pad}}$ שמכריע אותה במקום $O(\log n)$.

אז נתאר מכונה N_L: בהינתן x:

1. נייצר את $y = x0^{|x|^2-|x|}$.
2. נריץ ונחזיר את $N_{L_{pad}}(y)$.

$N_{L_{pad}}$ רצה במקום $O(\log|x|) = O(2\log|x|) = O(\log|x|^2) = O(\log|y|)$.

כלומר יש NTM שמכריע את L במקום $O(\log n)$, אז מהגדרה $L \in NL$.

ומההנחה ש- $NL = DTIME(n)$, נקבל ש- $L \in DTIME(n)$.

כלומר $DTIME(n) = DTIME(n^2)$, בסתירה ל-THT.

.