<u>תזכורת:</u>
<u>השאלה הפתוחה המרכזית (נוסח 1)</u>
האם לכל יחס דו מקומי S חסום פולינומי מתקיים שזיהוי יעיל גורר חיפוש יעיל?

<u>מ"ט אי- דטרמיניסטיות (א"ד):</u>
מ"ט א"ד מקבלת את הקלט x אם <u>קיים</u> מסלול בעץ החישוב המסתיים ב q_A.
$L(M) \triangleq \{x \mid x \text{ מקבלת את } M\}$

<u>טענה:</u> לכל מ"ט א"ד M קיימת מ"ט דטרמיניסטית M' כך ש $L(M') = L(M)$
<u>הוכחה:</u> (הכיוון ההפוך הוא כמובן טריוויאלי כי כל מכונה דטרמיניסטית היא מקרה פרטי של מ"ט א"ד).
<u>רעיונות:</u>
1. M' על קלט x תחפש בעץ החישוב של M על x האם מופיע בו q_A.
2. החיפוש יתבצע באמצעות אלגוריתם BFS (כי ב DFS למשל, החיפוש עלול לא להסתיים לעולם, אם בטעות נבחר ראשון מסלול שבו המכונה M לא עוצרת).
3. נתאים מחרוזת בינארית לכל מסלול בעץ.
4. חיפוש BFS הוא פשוט מעבר על המחרוזות הבינאריות לפי סדר לקסיקוגרפי.

נשתמש במכונה בעלת שלושה סרטים.
1. הסרט הראשון יכיל את הקלט x
2. הסרט השני יכיל מחרוזת בינארית w השקולה למסלול בעץ.
3. סימולציה של M על x במסלול w.

M' על קלט x:
בכל איטרציה:
1. מחשבת את w הבא ע"פ סדר לקסיקוגרפי.
2. מוחקת את סרט 3, כותבת את x לתוכו (מתוך סרט 1).
3. מבצעת סימולציה של M על x במסלול המתואר ע"י w.
אם הסימולציה מסתיימת ב q_A אז M' מקבלת.
אחרת היא עוברת לאיטרציה הבאה.

פירוט על מימוש הסימולציה:
אם $\delta_M(q,a) = ((p_0,b_0,d_0),(p_1,b_1,d_1))$ אז:
$$\delta_{M'}(q,*,0,a) = (p_0,*,0,b_0,S,R,d_0)$$
$$\delta_{M'}(q,*,1,a) = (p_0,*,1,b_1,S,R,d_1)$$
$$\delta_{M'}(q,*,b,a) = (q_{next},\ldots)$$

אם $x \in L(M)$ אז (ע"פ ההגדרה של מ"ט א"ד) קיים מסלול מקבל של M על x וקיימת מחרוזת בינארית w ראשונה לקסיקוגרפית המתארת מסלול כזה.
כאשר M' באיטרציה שבה w היא המחרוזת המבוקשת, אז M' תקבל.
(כל איטרציה סופית ובנוסף עוברים על w-ים ע"פ סדר לקסיקוגרפי) לכן $x \in L(M')$.
אם $x \notin L(M)$ אז לא קיים מסלול בו M על x עוצרת ב q_A ולכן M' לא עוצרת על x ולכן $x \in L(M')$.
לכן $L(M') = L(M)$

<u>הגדרה:</u> מ"ט א"ד M תקרא יעילה / פולינומית אם קיים פולינום $p(n)$, כך שלכל x ולכל מסלול חישוב של M על x, M עוצרת תוך לכל היותר $p(|x|)$ צעדים.

<u>המחלקה NP (הגדרה 1)</u>:
אוסף כל השפות L שקיימת עבורן מ"ט א"ד פולינומית.

<u>דוגמה:</u> $comp = \{x \mid \text{פריק } x\}$
ראינו בהרצאה הקודמת מ"ט א"ד עבור $comp$. המכונה הנ"ל רצה בזמן פולינומי ולכן $comp \in NP$.

<u>המחלקה NP (הגדרה 2)</u>:
אוסף כל השפות L שקיים עבורן יחס דו מקומי R_L המקיים:

א. R_L חסום פולינומית: $(x,y) \in R_L \Rightarrow |y| \le q(|x|)$ כאשר q הוא פולינום.

ב. R_L ניתן לזיהוי יעיל:

קיימת מ"ט M הרצה בזמן פולינומי $p(|x|+|y|)$ ומכריעה האם $(x,y) \in R_L$.

ג. $L = \{x \mid \exists y (x,y) \in R_L\}$ - כל השמאליים ביחס שיש להם בן זוג.

<u>משפט:</u> שתי ההגדרות של NP שקולות.
דוגמה: $comp \in NP$ גם על פי ההגדרה השניה.
מספיק להראות יחס מתאים: $R_{comp} = \{(x,y) \mid (1 < y < x) \wedge (x \bmod y = 0)\}$
א. מיידי מההגדרה.
ב. בהינתן (x,y) אין בעיה לבדוק בזמן פולינומי האם זה מתקיים ש $(x,y) \in R_L$.
ג. זוהי בדיוק ההגדרה של $comp$.

<u>טענה:</u> $P \subseteq NP \subseteq R$
: $P \subseteq NP$
<u>הגדרה 1:</u> $L \in P$ לכן קיימת לה M דטרמיניסטית פולינומית שהיא גם מקרה פרטי של מ"ט א"ד פולינומית ולכן $L \in NP$.
<u>הגדרה 2:</u> $L \in P$ לכן קיימת לה M דטרמיניסטית פולינומית שרצה בזמן $p(n)$ ו $L(M) = L$.
נראה יחס R_L כנדרש מהגדרה 2:
$$R_L = \{(x,x) \mid x \in L\}$$
א. היחס חסום פולינומית כי אורך האיבר השני הוא כאורך האיבר הראשון.
ב. היחס ניתן לזיהוי פולינומי - בהינתן (x,y) נבדוק האם $x = y$ ואם כן אז נשתמש ב M כדי לבדוק האם $x \in L$ שזה אומר ש $(x,x) \in R_L$
ג. זוהי בדיוק ההגדרה של L.

$NP \subseteq R$: <u>הגדרה 1:</u> $L \in NP$ לכן קיימת מ"ט א"ד M שרצה בזמן פולינומי $p(|x|)$ בכל מסלול.
נתאר מ"ט דטרמיניסטית M' שעוצרת תמיד ומקיימת $L(M') = L(M)$.
M' עובדת כמו המכונה שבנינו במשפט השקילות עם התוספת הבאה:
אם הגענו ל w שאורכו יותר מ $p(|x|)$ אז נעצור ונדחה.

$NP \subseteq R$: <u>הגדרה 2:</u> $L \in NP$ לכן קיים יחס R_L כמובטח בהגדרה 2. נתאר מ"ט שעוצרת תמיד ו $L(M) = L$.

M על קלט x מחפשת y כך ש $(x,y) \in R_L$, כלומר עוברת על כל ה y-ים בסדר לקסיקוגרפי עד לאורך $q(|x|)$ (המובטח בסעיף א' של ההגדרה של NP). לכל y כזה בודקת האם $(x,y) \in R_L$ (ע"י המכונה המובטחת בסעיף ב'). אם מצאה y כזה אז מקבלת, אחרת עוברת ל y הבא. אם אין אף y כזה אז דוחה.
נכונות - ע"פ סעיף ג' בהגדרה של NP.
קיבלנו M כנדרש, ולכן $L \in R$.

<u>הוכחת המשפט</u>: (שתי ההגדרות שקולות):
א. נניח $L \in NP$ על פי הגדרה 2 ולכן קיים יחס R_L כמובטח בהגדרה 2. נבנה מ"ט א"ד פולינומית M עבור השפה L, ונקבל $L \in NP$ ע"פ הגדרה 1.
M (א"ד פולינומית) על קלט x:
1. M "תנחש" מחרוזת y באורך קטן או שווה ל $q(|x|)$.
2. תבדוק האם $(x,y) \in R_L$ ע"י המכונה המובטחת בהגדרה. אם כן, תקבל, אחרת תדחה.

<u>יעילות</u>:
1. $O(|x|)$ צעדים.
2. $p(|x|+|y|) = O(p(|x|)+q(|x|))$ ולכן פולינומי.

<u>נכונות</u>:
על פי סעיף ג' בהגדרה: $x \in L \Leftrightarrow$ קיים y כך ש $(x,y) \in R_L \Leftrightarrow$ קיים מסלול בו M מקבלת את x.
לכן $L(M) = L$.

ב. נניח $L \in NP$ על פי הגדרה 1 ולכן קיימת מ"ט א"ד פולינומית M הרצה זמן $q(|x|)$ המכריעה את L ונוכיח ש $L \in NP$ ע"פ הגדרה 2, ע"י הגדרת יחס R_L כנדרש ע"י ההגדרה.
$R_L = \{(x,y) \mid y$ המכונה M מקבלת את הקלט x במסלול המתואר ע"י המחרוזת הבינארית $\}$.

א. $|y| \le q(|x|)$ כאשר q הוא הפולינום החוסם את זמן הריצה של M.
ב. סימולציה של M על x במסלול המתואר ע"י y לוקח $O(|y|) = O(q(|x|))$ צעדים.
ג. זו בדיוק ההגדרה של השפה.

האם $P = PN$?
<u>זוהי השאלה המרכזית במדעי המחשב (נוסח 2)</u>

<u>משפט</u>: שני הנוסחים של הבעיה הפתוחה המרכזית שקולים, כלומר:
$P = PN$ אם ורק אם לכל יחס דו מקומי S חסום פולינומי מתקיים שזיהוי יעיל של S גורר חיפוש יעיל של S.

כיוון $\Rightarrow$: נניח שלכל יחס חסום פולינומית S מתקיים שזיהוי יעיל גורר חיפוש יעיל, ונראה $P = NP$.
(ברור ש $P \subseteq NP$ ולכן מספיק להוכיח $NP \subseteq P$).
נתבונן בשפה כלשהי $L \in NP$ ונוכיח $L \in P$.
לצורך זה נתבונן ב $L \in NP$ ע" הגדרה 2.

יהי R_L היחס המובטח בהגדרה 2 עבור L.

R_L בפרט חסום פולינומית (ע"פ א') וניתן לזיהוי יעיל (ע"פ ב') ולכן מההנחה נקבל ש R_L ניתן לחיפוש יעיל, כלומר קיימת מ"ט פולינומית M כך שעל קלט x, אם קיים y כך ש $(x,y)\in R_L$ אז M עוצרת ב q_A עם y בפלט ואחרת (אם אין y כנ"ל) M עוצרת ב q_R.

לכן M הנ"ל היא מ"ט פולינומית עבור L. לכן $L\in P$.

הנכונות נובעת מההגדרה של R_L, בפרט, סעיף ג'.

כיוון $\Leftarrow$: נניח ש $P=NP$ ונתון יחס דו מקומי S חסום פולינומית, הניתן לזיהוי יעיל.

נראה ש S ניתן לחיפוש יעיל.

נגדיר יחס חדש $S'=\{((x,z),w)\mid (x,zw)\in S\}$

$L_f'=\{(x,y)\mid f(x)$ רישא של $y\}$

S' יחס פולינומי כי S כזה.

S' ניתן לזיהוי פולינומי כי S כזה.

$L_{S'}=\{(x,z)\mid \exists w:((x,z),w)\in S\}$

$L_{S'}\in NP$ כי S' הוא היחס המתאים לפי הגדרה 2.

לפי ההנחה $S'\in P$.

כלומר בהינתן (x,z) ניתן להכריע ביעילות האם קיים w כך ש $(x,zw)\in S$.

בקצרה (כמו הוכחה עבור פונקציות)

<u>אתחול:</u> נבדוק האם $(x,\varepsilon)\in L_{S'}$ אם כן, נאתחל: $y\leftarrow\varepsilon$. אחרת נעצור ב q_R.

איטרציות שבהן y הוא רישא של פתרון, ובכל איטרציה, לכל $a\in\Sigma$ נבדוק האם $(x,ya)\in L_{S'}$. אם כן אז נחליף את y ב ya ואם לא נעבור לאות הבאה, ואם ניסינו את כולן, אז y הוא ה y המבוקש.