מרתון - חישוביות - 23.12
משפט רייס - דרך להוכחה ששפה אינה כריעה או אינה מזוהה.

המשפט: כל תכונה לא טריוויאלית של שפות ב RE אינה כריעה.

פרקטית: נתונה שפה שאנו רוצים להראות שהיא לא כריעה: $L = \{< M >: תנאי\}$.
התנאים כדי שנוכל להשתמש במשפט:

1. מקבלים רק מכונה אחת ולא משהו אחר ולא יותר ממכונה אחת.
   לדוגמא: $L = \{< M_1, M_2 >: L(M_1) \subseteq L(M_2)\}$ - לא ניתן להשתמש ברייס.
2. התנאי של השפה הוא על מה שהמכונה מקבלת (שפת המכונה) ולא על התנהגות או מבנה המכונה.(צריך שהתכונה תהיה סמנטית)
   לדוגמא: $L = \{< M >: M \ halts \ on \ input \ '000'\}$ - לא ניתן להשתמש ברייס.
3. התכונה תהיה לא טריויאלית. שלא כל המכונות בעולם מקיימות אותו או כל המכונות בעולם לא מקיימות אותו. אם התכונה כן טריוויאלית - השפה תהיה ב R אך לא בגלל המשפט.
   לדוגמא: $L = \{< M >: |L(M)| \geq 0\}$ - לא ניתן להשתמש ברייס.

ברגע שמשתמשים במשפט רייס ניתן לומר מיידית שהשפה אינה ב R.

הרחבה: אם Φ (השפה הריקה) מקיימת את התכונה (בנוסף לתנאים לעיל) אז השפה L אינה ב RE.

דוגמאות:

- $L_1 = \{< M >: M \ accepts \ only \ even \ length \ inputs\}$.
  מקבלים רק מכונה אחת.
  התכונה: $S_1 = \{L \in RE: L \ contains \ only \ even \ length \ words\}$.
  התכונה סמנטית: כדי להוכיח זאת צריך להראות שכל 2 מכונות שיש להן את אותה שפה מקיימות ששתיהן ב L_1 או שתיהן לא ב L_1.
  אם $L(M_1) = L(M_2)$ אז או שב 2 השפות יש רק מילים באורך זוגי או שב 2 השפות יש גם מילים באורך אי זוגי ולכן או ש $< M_1 >, < M_2 > \in L_1$ או $< M_1 >, < M_2 > \notin L_1$.
  התכונה לא טרייויאלית: דוגמא לשפה שמקיימת: $L = \{00\}$, דוגמא לשפה שלא מקיימת: $L = \{0\}$

  לכן לפי משפט רייס, $L_1 \notin R$.
  כאן ניתן להשתמש בהרחבה: כי Φ מקיימת את התכונה (יש בה רק מילים באורך זוגי) ולכן: $L_1 \notin RE$.

- $L_2 = \{< M >: |L(M)| > 7\}$.
  מקבלים רק מכונה אחת.
  התכונה: $S_1 = \{L \in RE: |L| > 7\}$.
  התכונה סמנטית:
  אם $L(M_1) = L(M_2)$ אז $|L(M_1)| = |L(M_2)|$ ולכן $|L(M_1)| > 7$ אם ורק אם $|L(M_2)| > 7$ ולכן 2 המכונות שייכות לשפה או 2 המכונות לא שייכות לשפה.
  התכונה לא טרייויאלית: דוגמא לשפה שמקיימת: $L = \{0^n: 1 \leq n \leq 8\}$, דוגמא לשפה שלא מקיימת: $L = \{0\}$.
  לכן לפי משפט רייס, $L_2 \notin R$.
- $L_3 = \{< M >: \forall x \in L(M), M \ accepts \ x \ within \ 100 \ steps\}$.
  כאן לא ניתן להשתמש ברייס.
  התכונה אינה סמנטית. נראה דוגמא ל 2 מכונות עם אותה שפה כך שאחת מהן ב L_3 והשנייה לא.
  המכונה הראשונה: M_1 מקבלת קלט x וישר מקבלת אותו (צעד אחד).

המכונה השנייה: M_2 מקבלת קלט x, מבצעת 101 צעדים ואז מקבלת אותו.
מתקיים: $L(M_1) = L(M_2) = \Sigma^*$ אבל $< M_1 > \in L_3$.$< M_2 > \notin L_3$,

תרגיל ממבחן 2020 מועד ב:

.2 (30 נקודות) לכל אחת מהשפות הבאות, קבעו האם היא ב R והאם היא ב RE. הוכיחו את תשובתכם.

א.
$$L_1 = \{< M1 > | \exists \text{ infinitely many } < M_2 >' s \text{ such that } L(M_1) = L(M_2)\}$$

בעברית: זוהי שפת כל קידודי המכונות $< M_1 >$ שקיימים עבורן אינסוף קידודי מכונות $< M_2 >$ כך שהשפה של M_1 שווה לשפה של M_2.

ב. $L_2 = \{< M1 >, < M2 > \mid \text{There exist at least 2 words } x_1, x_2$
ι that each x_i is in $L(M_i)$ but not in the language of the other $M_j(\text{ where } j = 3 - i)\}$
בעברית: זוהי שפת כל זוגות קידודי מכונות $< M_2 >, < M_1 >$ כך שקיים זוג מילים x_1, x_2 כך שלכל $i \in \{1,2\}$ $x_i \in L(M_i) \setminus L(M_{3-i})$.

ג. $L_3 = \{< M1 >, < M2 > \mid \text{There exist at least 2 words } x_1, x_2$

such that each x_i is in $L(M_i)$ and is rejected by the other $M_j(\text{ where } j = 3 - i)\}$
בעברית: זוהי שפת כל זוגות קידודי מכונות $< M_2 >, < M_1 >$ כך שקיים זוג מילים x_1, x_2 כך שלכל $i \in \{1,2\}$ $x_i \in L(M_i)$ וגם M_{3-i} דוחה את x.

פתרון:
א. השפה ב R כי התנאי הוא טריוויאלי.
לכל שפה ב RE יש אינסוף מכונות שונות שמקבלות אותה.
ולכן התנאי מתקיים תמיד ואין צורך לבדוק אותו ומכאן השפה L_1 היא $\Sigma^* \in R$.

ב. אינטואיציה: אפילו אם נניח ש 2 המילים הללו ידועות לנו, עדיין אם לדוגמא M_1 מקבלת את x_1 ולא עוצרת על x_2 , לא נוכל לדעת שהיא אכן לא עוצרת על x_2 ולכן זה לא ב RE.
השפה $L_2 \notin RE$.
הוכחה: נראה רדוקציה: $\bar{HP} \le L_2$ ע"י: $f(< M, x >) =< M_1, M_2 >$. כאשר:
M_1: על קלט w:
- אם $w = 0$ - קבל.
- אם $w = 1$ - הרץ את M על x ואם היא עצרת - קבל.
- אחרת - דחה.

M_2: על קלט w:
- אם $w = 0$ - דחה.
- אם $w = 1$ - קבל.
- אחרת - דחה.

הרדוקציה מלאה וניתנת לחישוב - כתיבת תיאור של 2 מכונות שמריצות מכונה אחרת, משוות בין מילים ומקבלות או דוחות.
תקפות: אם $< M, x > \in \bar{HP}$ אז M לא עוצרת על x. מכאן עבור $w = 0$ נקבל ש M_1 מקבלת, M_2 דוחה ועבור $w = 1$ נקבל ש M_1 לא עוצרת (לא מקבלת), M_2 מקבלת ולכן תנאי L_2 מתקיים ולכן: $< M_1, M_2 > \in L_2$
אם $< M, x > \notin \bar{HP}$ אז M עוצרת על x אז לא קימת מילה ש M_1 לא מקבלת ואילו M_2 כן כי את 0,1 M_1 מקבלת ואת שאר המילים שתיהן דוחות. ולכן: $< M_1, M_2 > \notin L_2$.

לפי משפט הרדוקציה: $\bar{HP} \notin RE$ ולכן $L_2 \notin RE$.

ג. מתקיים: $L_3 \in RE \backslash R$.
הוכחת שייכות ל RE: נראה מ"ט א"ד המקבלת את L_3:
M_3: על קלט $< M_1, M_2 >$:
- נחש 2 מילים: x_1, x_2.
- הרץ את M_1 על x_1. אם דחתה - דחה.
- הרץ את M_1 על x_2. אם קיבלה - דחה.
- הרץ את M_2 על x_1. אם קיבלה - דחה.
- הרץ את M_2 על x_2. אם דחתה - דחה.
- קבל.

נכונות: אם $< M_1, M_2 > \in L_3$ אז קיימות 2 מילים כך שאחת מתקבלת במכונה הראשונה ונדחית בשנייה והמילה השנייה מתקבלת במכונה השנייה ונדחית בראשונה ולכן קיים מסלול חישוב בו ננחש בדיוק את 2 המילים הנ"ל בסדר הנ"ל ולכן M_1 תקבל את x_1 ותדחה את x_2 ואילו M_2 תקבל את x_2 ותדחה את x_1 ולכן נעבור את כל הבדיקות ונקבל.
אם M_3 קיבלה אזי קיים ניחוש של 2 מילים x_1, x_2 כך ש: M_1 קיבלה את x_1 ודחתה את x_2 ואילו M_2 דחתה את x_1 וקיבלה את x_2 ולכן בפרט תנאי השפה L_3 מתקיים עבור 2 מילים אלו ולכן $< M_1, M_2 > \in L_3$.

הוכחת אי שייכות ל R:
נראה רדוקציה: $HP \leq L_3$ ע"י: $f(< M, x >) = < M_1, M_2 >$. כאשר:
M_1: על קלט w:
- אם $w = 0$ - הרץ את M על x ואם עצרה - קבל.
- אם $w = 1$ - דחה.
- אחרת - דחה.

M_2: על קלט w:
- אם $w = 0$ - דחה.
- אם $w = 1$ - קבל.
- אחרת - דחה.

הרדוקציה מלאה וניתנת לחישוב - כתיבת תיאור של 2 מכונות שמריצות מכונה אחרת, משוות בין מילים ומקבלות או דוחות.
תקפות: אם $< M, x > \in HP$ אז M עוצרת על x ולכן M_1 תקבל את 0 ותדחה את 1 ואילו M_2 תדחה את 0 ותקבל את 1 ולכן: $< M_1, M_2 > \in L_3$.
אם $< M, x > \notin HP$ אז M לא עוצרת על x ולכן M_1 לא תקבל אף מילה ומכאן בפרט: $< M_1, M_2 > \notin L_3$.
לפי משפט הרדוקציה: $HP \notin R$ ולכן $L_3 \notin R$.

סיבוכיות

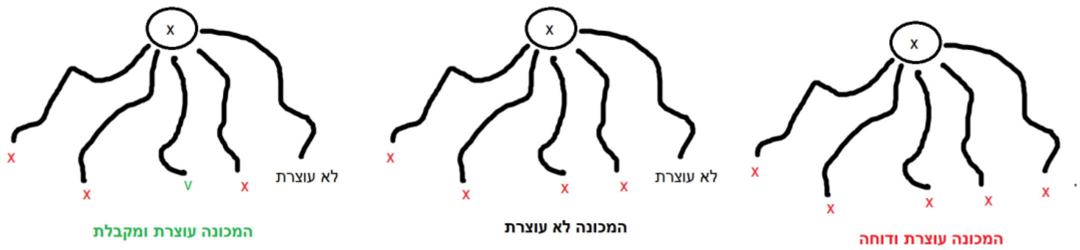
כל הבעיות הן כריעות בחלק זה - כלומר שייכות ל R.
אנו רוצים לדעת מה ניתן לחשב באופן יעיל ומה לא ניתן.
יעיל = זמן ריצה פולינומי: $O(n^c)$ כאשר c הוא קבוע! ואפילו $O(n^{1000})$ נחשב "יעיל".
לא יעיל = אקספוננציאלי: $O(c^n)$ כאשר $c > 1$. או $O(n!)$ או $O(n^n)$.

כאן לא נדרשים לנתח סיבוכיות באופן מדוייק היות ומדובר במכונת טיורינג ובמימוש הקידוד.

דגש חשוב: סיבוכיות זמן ריצה מודדים ביחס לגודל הקלט!!!
כלומר: אם הקלט בגודל: $N = 2^n$ ומבצעים $N = 2^n$ פעולות אז הסיבוכיות תהיה: $O(N)$.
לדוגמא: אם הקלט הוא n - מספר המיוצג בבינארי.

ואנו רוצים לבדוק האם הוא ראשוני ולכן רצים על כל המספרים מ 2 עד $n-1$ ובודקים האם הוא מתחלק בהם. אז הסיבוכיות היא אקספוננציאלית.
גודל הקלט: $N = log_2 n$ ביטים. זמן ריצה: $O(n) = O(2^N)$. אקספוננציאלי.

הרחבה: מ"ט אי דטרמיניסטית.
מ"ט שפונקציית המעברים שלה מחזירה מספר אופציות לצעד הבא.
לדוגמא: $\delta(q_0, a) = \{(q_1, a, R), (q_0, b, L)\}$.
השפה של מ"ט א"ד היא $L(M)$ - כל הקלטים שקיים עבורם מסלול חישוב שמגיע למצב מקבל.
ולכן ניתן לחשוב על מכונה זו כאילו היא מנחשת את המסלול הנכון המגיע למצב מקבל.
מילה מתקבלת - אם יש אפילו מסלול אחד שמגיע למצב מקבל (לא משנה מה קורה באחרים).
מילה נדחית - אם כל המסלולים מגיעים לדחייה.
מילה שהמכונה לא עוצרת עליה - אם כל המסלולים לא מקבלים ויש לפחות אחד שהוא אינסופי.



הערה: אם הופכים בין המצבים המקבלים והלא מקבלים במכונה א"ד לא בהכרח שנקבל את השפה המשלימה.

סיבוכיות של מ"ט א"ד = אורך המסלול הארוך ביותר.
ולא לוקחים בחשבון את סכום אורכי כל המסלולים ולכן יוצא מכאן שניתן לעשות חיפוש שלם בסיבוכיות זמן של חיפוש אלמנט אחד. ולכן מה שאפשר לעשות במ"ט רגילה בזמן אקספוננציאלי, ניתן לעשות ב"ט א"ד בזמן פולינומי.

שקילות כוח חישוב:
בחישוביות = אי דטרמיניסטית שקולה לדטרמיניסטית. (טובה להוכחה ששפה היא ב R\RE\coRE)
בסיבוכיות = לא ידוע האם היא שקולה (מאמינים שהיא לא)

מחלקות סיבוכיות:
P - קבוצת כל השפות שיש להן מ"ט דטרמיניסטית המכריעה אותן בזמן פולינומי.
NP - קבוצת כל השפות שיש להן מ"ט אי דטרמיניסטית המכריעה אותן בזמן פולינומי.
$coNP$ - קבוצת כל השפות שהמשלימה שלהן ב NP.

תכונות:
- $P \subseteq NP$.
- $P = NP$ - לא ידוע (בעיה פתוחה)
- $P \subseteq coNP$
- $P = NP \cap coNP$ - לא ידוע (בעיה פתוחה)

תכונות סגור:
עבור $\boldsymbol{P}$:
סגורה ל: איחוד, חיתוך, משלים, שרשור, הפרש, איטרציה, היפוך, חזקה.
עבור $\boldsymbol{NP}$:

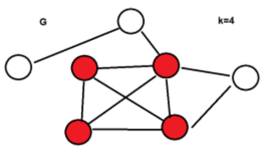
סגורה ל: איחוד, חיתוך, שרשור, איטרציה, היפוך, חזקה.
עבור $\boldsymbol{coNP}$:
סגורה ל: איחוד, חיתוך, שרשור, איטרציה, היפוך, חזקה.

רדוקציה פולינומית:
רדוקציה רגילה (כמו בחישוביות) כאשר בנוסף, זמן הריצה שלה (כלומר זמן ההמרה של הקלט משפה אחת לאחרת) הוא פולינומי.
סימון: $L_1 \leq_p L_2$.

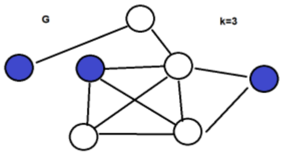
תכונות:
1. $L \leq_p L$.
2. אם $L_1 \leq_p L_2$ וגם $L_2 \leq_p L_3$ אז $L_1 \leq_p L_3$.
3. אם $L_1 \leq_p L_2$ אז $\bar{L_1} \leq_p \bar{L_2}$.
4. אם $L \in P$ אז: $L \leq_p L'$ לכל שפה אחרת L'.
5. משפט הרדוקציה לסיבוכיות: אם $L_1 \leq_p L_2$ אז:
   - אם $L_2 \in P$ אז $L_1 \in P$.
   - אם $L_2 \in NP$ אז $L_1 \in NP$.

שלמות בתוך מחלקה:
שפה L תקרא NPNPC (שלמה) אם:
1. $L \in NP$.
2. לכל $L' \in NP$ מתקיים: $L' \leq_p L$. (שפה NP קשה - NPH)

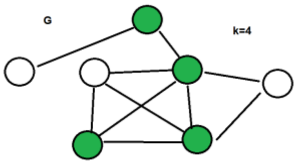
במקום להוכיח את 2 אנו מוכיחים את הדבר הבא: אם $L \leq_p L_1$ כאשר כבר ידוע ש L היא NPC אז $L_1 \in NPC$
ולכן צריך לזכור רשימה של שפות שידוע עליהן שהן NPC.
הרשימה:
- שפות הקשורות לגרפים:
1. $CLIQUE = \{< G, k >: G \text{ is graph}, k \in N, \text{and exists clique of size } k \text{ in } G\}$
מקבלים גרף ומספר ומחזירים האם יש בגרף קליקה בגודל k.
קליקה = תת גרף שבו כולם מחוברים לכולם ישירות.



2. $IS = \{< G, k >: G \text{ is graph}, k \in N, \text{and exists independent set of size } k \text{ in } G\}$
מקבלים גרף ומספר ומחזירים האם יש בגרף קבוצה בלתי תלויה בגודל k.
קבוצה בלתי תלויה = תת גרף שבו אף אחד לא מחובר לאף אחד ישירות.

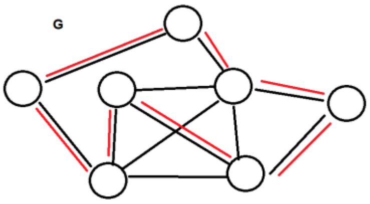


3. $VC = \{< G, k >: G \text{ is graph}, k \in N, \text{and exists vertex cover of size } k \text{ in } G\}$
מקבלים גרף ומספר ומחזירים האם יש בגרף כיסוי צמתים בגודל k.
כיסוי צמתים = קבוצת קודקודים שנוגעת בכל צלעות הגרף.



4. $HC = \{< G >: G\ is\ graph, and\ exists\ hamiltonian\ cycle\ in\ G\}$

מקבלים גרף ומחזירים האם יש בגרף מעגל המילטוני.
מעגל המילטוני = מעגל שעובר בכל קודקודי הגרף בדיוק פעם אחת (פרט לראשון שבו מסיימים), אין צורך לעבור בכל הצלעות.

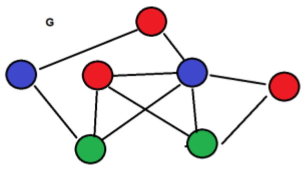


5. $HP = \{< G >: G\ is\ graph, and\ exists\ hamiltonian\ path\ in\ G\}$

מקבלים גרף ומחזירים האם יש בגרף מסלול המילטוני.
מסלול המילטוני = מסלול שעובר בכל קודקודי הגרף בדיוק פעם אחת.

6. $3COL = \{< G >: G\ is\ graph\ and\ g\ is\ 3-colorable\}$

מקבלים גרף ומחזירים האם הוא 3-צביע.
גרף 3-צביע = גרף שניתן לצבוע את קודקודיו ב 3 צבעים כך שלא יהיו 2 סמוכים עם אותו צבע.



- שפות הקשורות לנוסחאות לוגיות:

1. $SAT = \{< \varphi >: \varphi\ is\ CNF\ formula\ and\ \varphi\ has\ satisfiable\ assignment\}$.

מקבלים נוסחא לוגית בצורת CNF ומחזירים האם יש השמה למשתני הנוסחא שתגרום לנוסחא כולה להיות true. (להשמה כזו קוראים - השמה מספקת).
נוסחת CNF = נוסחא מהצורה: $(x_1 \vee \neg x_2) \wedge (x_2 \vee x_3 \vee \neg x_4) \wedge ..$ - "או" בתוך הסוגריים ו"וגם" בחוץ.
ליטרל = משתנה או שלילתו.
סוגריים = פסוקית.
לכל משתנה יש הצבה: T או F.
אנו רוצים לדעת האם יש הצבה לכל המשתנים שתגרום לנוסחא כולה להיות T.

2. $3SAT = \{< \varphi >: \varphi\ is\ 3CNF\ formula\ and\ \varphi\ has\ satisfiable\ assignment\}$.

כמו SAT רק שבכל פסוקית יש בדיוק 3 ליטרלים.

- שפות הקשורות לקבוצות (מערכים):

1. $SS = \{< a_1, a_2, ..., a_n, s >: exists\ subset\ of\ \{a_1, a_2, ..., a_n\}\ with\ sum\ of\ s\}$.

מקבלים קבוצה של n מספרים ומספר s ומחזירים האם יש תת קבוצה של מספרים מתוך הקבוצה שסכומה הוא s.

2. $SC = \{< n, A_1, A_2, ..., A_m, k > : exists\ k\ sets\ from\ A_1, .., A_m\ such\ that\ the\ union\ of\ them\ is\ [n]\}$

מקבלים מספר שלם n, רשימת קבוצות: $A_1, .., A_m$ ומספר שלם k ומחזירים האם יש k קבוצות מתוך הקבוצות הנ"ל שהאיחוד שלהן נותן את קבוצת כל המספרים מ 1 עד n.

3. $HC = \{< U, A_1, A_2, ..., A_m, k >: exists\ X \subseteq U,\ |X| = k\ such\ that\ \ X \cap A_i \neq \Phi\}$

מקבלים קבוצה U, רשימת קבוצות: $A_1, .., A_m$ ומספר שלם k ומחזירים האם יש תת קבוצה של U בגודל k שהחיתוך שלה עם כל תתי הקבוצות הנתונות אינו ריק.

כל השפות הנ"ל הן NPC.
משפט: אם קיימת רדוקציה משפה שהיא NPC לשפה שהיא ב P אז $P = NP$.

3. (22 נקודות)

א. (8 נקודות) בהרצאה למדנו (ללא הוכחה) ש $P \subsetneq R$. בסעיף זה מותר להשתמש במשפט זה. הוכח או הפרך: קיימות זוג שפות L_1, L_2 כך ש $L_1 \leq L_2$ אבל לא $L_1 \leq_p L_2$.

ב. (6 נקודות) בסעיף זה נניח כי $P \neq NP$. הוכח או הפרך: קיימת תת קבוצה אינסופית $H \subseteq NP \setminus P$, כך ש $\forall L_1, L_2 \in H, L_1 \leq_p L_2$.

ג. (8 נקודות) תהי L_1 שפה כלשהי. אזי קיימת שפה L_2 כך ש לא מתקיים $L_2 \leq_p L_1$.

פתרון:

א. נשתמש במשפט ש: $P \subset R$. מכאן קיימת שפה $L \in R \backslash P$.

ניקח: $\Phi, \Sigma^* \neq L_2 \in P$ ובפרט: $L_2 \in R$. וניקח: $L_1 = L$.

מתקיים: $L_1 \leq L_2$ לפי המשפט שכל שפה ב R ניתנת לרדוקציה (חישובית) לכל שפה אחרת שאינה טריוויאלית.

אבל לא מתקיים: $L_1 \leq_p L_2$ כי אז לפי משפט הרדוקציה (סיבוכיות): $L_2 \in P$ ולכן: $L_1 \in P$ - סתירה.

ב. ניקח את $H = NPC$. מתקיים: $NPC \subseteq NP \backslash P$ כי:

לפי ההגדרה: כל שפה ב NPC היא בפרט שייכת ל NP.

ולפי המשפט, אם הייתה שפה שהיא ב P בתוך NPC אז $P = NP$ והנחנו בשאלה זו ש $P \neq NP$.

בנוסף, $H = NPC$ אינסופית כי יש בה לדוגמא את: $\{3SAT, 4SAT, 5SAT, \ldots.\}$.

כעת, לכל $L_1, L_2 \in NPC$

מתקיים: $L_1 \leq_p L_2$ (כי $L_2 \in NPC$ ולכן יש רדוקציה מכל שפה ב NP אליה ובפרט מ L_1 אליה)

ומתקיים: $L_2 \leq_p L_1$ (כי $L_1 \in NPC$ ולכן יש רדוקציה מכל שפה ב NP אליה ובפרט מ L_2 אליה)

ג. הוכחה: נוכיח באמצעות שיקולי ספירה.

לכל שפה L_2 קיימת רדוקציה אחרת: $L_2 \leq_p L_1$ (או שלא קיימת).

כמות הרדוקציה הקיימות בעולם חסומה בכמות המ"ט הקיימות כיוון שכל רדוקציה היא ניתנת לחישוב ולכן הכמות חסומה ב $\aleph_0$ (בת מניה). לעומת זאת, כמות השפות השונות הקיימות היא: $|P(\Sigma^*)| = \aleph > \aleph_0$ ולכן לא תיתכן רדוקציה מכל שפה L_2 בעולם לשפה L_1 ובפרט קיימות שפות L_2 שעבורן אין רדוקציה ל L_1.