משפטים

תוכן עניינים

0.1 מכונות טיורינג

0.1.1 טענה 4.1 : R סגורה למשלים

הוכחה:

תהי $L \in R$. נראה $\sum \in R$ מהגדרת R , קיימת מ"ט M המכריעה את L . נבנה מ"ט M' עבור $\bar{L}$ באופן הבא:

- $M'(x)$ מריצה את M על x ועונה הפוך.
  - כלומר אם M עצרה ב q_{acc} , נעצור ב q_{rej}
  - ואם עצרה ב q_{rej} נעצור ב q_{acc}.

נבדוק את שני המקרים:

- עבור $x \in \bar{L} \Leftarrow M$ דוחה את x (כי $x \notin L$) . לכן בסימולציה של M על x ע"י M' , M' תעצור, תזהה דחיה ואז תענה הפוך, כלומר q_{acc} - כנדרש
- עבור $x \notin \bar{L} \Leftarrow x \in L \Leftarrow M$ מריצה על x תקבל $\Leftarrow M'$ תסיים את הרצת הסימלוציה על M על x , תזהה קבלה ותענה הפוך, כלומר q_{rej}, כנדרש . בפרט M' תמיד עוצרת, ולכן מכריעה את $\bar{L}$.

0.1.2 טענה 4.2: R סגורה לאיחוד.

הוכחה:

- יהיו $L_1, L_2 \in R$. נרה ש $L_1 \cup L_2 \in R$ ע"י בניית מ"ט $M_{1,2}$ המכריעה את $L_1 \cup L_2$.
- יהיו M_1, M_2 המכירעות את L_1, L_2 בהתאמה :

1. $M_{1,2}(x)$: מריצה את M_1 על x שומרת את התוצאה במשתנה $out_1 = \left\{true_{q_{acc}}, false_{q_{rej}}\right\}$
2. $M_{1,2}(x)$: מריצה את M_2 על x שומרת את התוצאה במשתנה $out_2 = \left\{true_{q_{acc}}, false_{q_{rej}}\right\}$
3. עוצרת ב q_{acc} אם $out_1 \vee out_2 = T$, אחרת עוצרת ב q_{rej}

- נראה שM_{12} מכריע את $L_1 \cup L_2$
  - אם $x \in L_1 \cup L_2$: M_1 או M_2 תעצור ותקבל (או שתיהן) $\Leftarrow$ נגיע לשלב 3 וה OR שיחושב יהיה $T \Leftarrow M_{12}$ תקבל, כנדרש $(x \in L\left(M_{12}\right))$
  - אם $x \notin L_1 \cup L_2 \Leftarrow M_1$ ו M_2 יעצרו ב $q_{rej} \Leftarrow$ נגיע לשלב 3 הוא OR שיחושב $F \Leftarrow M_{12}$ תדחה את x, כנדרש

0.1.3 טענה 4.3 : RE סגורה לאיחוד

הוכחה:

ניסיון I : נבנה M_{12} כמו בהוכחה עבור R . הבעיה כאן היא במקרה ש $x \in L_2 \backslash L_1$. במקרה זה $x \in L_1 \cup L_2$, ולכל המכונה M_{12} צריכה לקבל את x (בפרט לעצור) ו M_{12} שבנינו תתקע בשלב 1 ולא תעצור לעולם.

ניסיון II : (עובד) הרעיון הוא להריץ את M_1, M_2 (המכריעות את L_1, L_2 בתאמה ב"מקביל")

כיצד נעשה זאת? נריץ את המכונות על x לסירוגין . בצעד ראשון נריץ צעד 1 של M_1 , בצעד 2 צעד 1 של M_2 , בצעד 3, צעד שני של M_1 וכו'

פורמלית:

1. $M_{12}(x)$ תריץ את M_1, M_2 במקביל על x

2. אם אחת מהן עצרה ב q_{acc} , מיד נעצור ונקבל

3. אם שתיהן עצרו ב q_{rej} , נעצור ונדחה.

נשאר להוכיח את נכונות הבניה. $x \in L(M_1)$ או $x \in L(M_2)$ (מנכונות M_1, M_2)

- אם $x \in L_1 \cup L_2$ לפחות אחת מהמכונות עוצרת על x ב q_{acc} נסמן ב i את הצעד שבו היא עוצרת. מהבניה M_{12} תזהה עצירה זו בסימולציה של הצעד הנ"ל בצעד סימולציה $2i$ לכל היותר. במקרה זה היא גם תעצור ותקבל. גם אם המ"ט השניה עצרה לפני כן, זה לא ישנה את התוצאה ל q_{rej}, כי M_{12} לא עוצרת ב $q-rej$ אלא אם שתי המכונות עצרו ב q_{rej}
- אם $x \notin L_1 \cup L_2 \Leftarrow x \notin L_1 = L(M_1)$ וגם $x \notin L_2 = L(M_2) \Leftarrow$ אף אחת מהמכונות לא תעצור ב $q_{acc} \Leftarrow M_{12}$ לא תעצור ב q_{acc} (אלא תעצור ב q_{rej} אם שתיהן עוצרות או לא תעצור מש"ל

0.1.4 טענה 4.6 : הגדרות 4.5 , 4.4 $CoRE$ שקולות

$4.4 \Rightarrow 4.5$:

תהי $L \in CoRE$ לפי הגדרה 4.4, נראה ש $L \in CoRE$ לפי הגדרה 4.5 .

- בניה: תהי M מ"ט המקבלת את $\bar{L}$. נבנה $\bar{M}$ מתאימה עבור L שתספק את הגדרה 4.5 . $\bar{M}(x)$ - תריץ את M על x ותענה הפוך. (אם לא עוצרת אז לא תעצור)
- נכונות:
  - אם $x \in L \Leftarrow x \notin \bar{L}$, ולכן M או תעצור ב q_{rej} או לא תעצור $\Leftarrow \bar{M}$ או תעצור ב q_{acc} או לא תעצור, כנדרש
  - אם $x \notin L \Leftarrow x \in \bar{L}$, מהגדרת $RE \Leftarrow M$ בריצתה על x עוצרת ב q_{acc} , מהבניה $\Leftarrow$ ב q_{rej} , כנדרש.

$4.4 \Leftarrow 4.5$:

תהי $L \in CoRE$ לפי הגדרה 4.5, נראה ש $L \in CoRE$ לפי הגדרה 4.4 .

- בניה: תהי M מ"ט המובטחת עבור L נבנה מ"ט $\bar{M}$ המקבלת את $\bar{L}$, ונסיק ש $L \in CoRE$ לפי הגדרה 4.4 - $\bar{M}(x)$: מריצה את M על x ועונה הפוך
- נכונות:
  - אם $x \in L \Leftarrow M$ תעצור ב q_{acc} או לא תעצור $\Leftarrow \bar{M}$ תעצור ב q_{rej}או לא תעצור $\Leftarrow x \in\notin L\left(\bar{M}\right)$, כנדרש.
  - אם $x \notin L$, מהגדרת $4.5 \Leftarrow M$ עוצרת ב q_{rej} , מהבניה $\Leftarrow \bar{M}$ עוצרת ב $q_{acc} \Leftarrow x \in L\left(\bar{M}\right)$,כנדרש.

0.1.5 טענה: $R = RE \cap CoRE$

הוכחה: נראה הכלה דו כיוונית.

כיון קל - $R \subseteq RE \cap CoRE$

זה מתקיים כי מ"ט M המכריעה את L ובפרט מקבלת את L ולכן $L \in RE$ וגם מקיימת את הדרישה של הגדרה 4.5 לשייכת ל $CoRE$ (אף פעם לא טועה ומותר לה לא לעצור רק אם $x \in L$ אבל במקרה שלנו היא תמיד תעצור, בפרט עבור כל $x \in \bar{L}$

כיוון מענין $RE \cap CoRE \subseteq R$

תהי $L \in RE \cap CoRE$. לכן קיימת מ"ט M_1, M_2 .בהתאמה כך ש:

1. כל M תמיד צודקת לגבי שייכות של x ל L במידה ועוצרת
2. אם $x \in L$, M_1עוצרת ב q_{acc}
3. (מהגדרה 4.5) אם $x \notin L$, M_2 עוצרת ב q_{rej}

נבנה M שמכריעה את L באופן הבא:

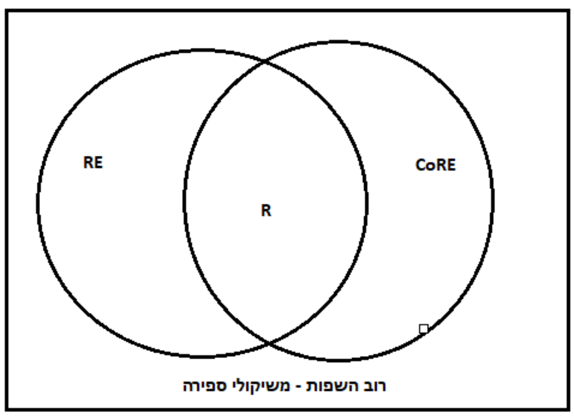
$M(x)$: מריצה את M_1 ו M_2 על x במקביל. (כמו שעשינו בהוכחה ש RE סגורות לאיחוד) ברגע שאחת מהן עצרה מיד עוצרת ועונה כמוה

נכונות הבניה:

אם $x \in L \Leftarrow$ בהכרח , M עוצרת על x ב $q_{acc} \Leftarrow$ יתכן אחד משני מקרים:

1. M_1 היא הראשונה שעצרה בצעד $\leq$ מהצעד שבו M_2 עוצרת אם בכלל) ,אז מהבניה M תעצור ב q_{acc} , כמוה . כנדרש.
2. M_2 עוצרת ראשונה . אבל מתכונה 1 , היא גם תעצור ב q_{acc} ו M תענה כמוה, כנדרש.
3. $x \notin L \Leftarrow$ באופן דומה לטעיון במקרה הקודם, מובטח ש M_2 תעצור ב q_{rej} וגם אם M_1 עוצרת לפניה, היא תעצור ב q_{rej} ו M תעצור ב q_{rej} , כנדרש.

לכן, נוכל לעדכן את מפת העולם:



0.1.6 טענה: $L_D \in RE \backslash R$

הוכחה:

שייכות ל RE - נבנה מ"ט המקבלת את L_D , (אבל לא תכריע אותה)

$M_D(\langle M \rangle)$:

תבדוק "חוקיות" של $\langle M \rangle$. אם לא חוקי מיד תעצור ותקבל (אז $\langle M \rangle$ הוא קידוד של M_{stam} וזו מקבלת הכל, בפרט את $\langle M_{stam} \rangle$)

אחרת, : תריץ את M על $\langle M \rangle$, ותענה כמוה.

נכונות: בבית

אי שייכות ל R **:** נראה ש $\bar{L}_D$ אינה ב RE ומכך נסיק בקלות ש: $L_D \in R$. כיצד נוכיח?

נוכיח באמצעות טעון לכסון.

נתבונן בטבלה הבאה:

	0	1	1	0	$\dots$			
$M\setminus\sum^*$	$\langle M_1\rangle$	$\langle M_2\rangle$		$\langle M_i\rangle$			$\langle M_j\rangle$	
$\langle M_1\rangle$	**0**	1	1					
$\langle M_2\rangle^2$	1	**0**	1	1	0	0	1	$\dots$
			_					
$\langle M_i\rangle$				_		0^1		
$\langle M_j\rangle$					_	_		

1 . כל משבצת מופיע 1 אם M_i מקבלת את $\langle M_j\rangle$ ו 0 אחרת

2. בשורה $\langle M_2\rangle$ ישנו וקטור של 0ים ו1ים כך שה1ים מופיעים במקומות המתאימים למילים ב $L(M_2)$

נתבונן בשפה $\bar{L}_D$ (מופיע מעל השורה הראשונה) ־ זוהי שורה אינסופית כלשהי של 0ים ו1ים. האבחנה הקריטית היא ששורה זו אינה שווה לאף אחת מהשורות בטבלה שהן רשימת כל השפות ב RE , ואז נסיק שאינה RE .

מדוע? עבור השורה של $\langle M_i\rangle$כלשהי, $\bar{L}_D$ שלנו אינה מסכימה עם M_i לגבי הקלט $\langle M_i\rangle$:

- אם M_i מקבלת את $\langle M_i\rangle$, אז $\langle M_i\rangle\in L_D$ (כתוב 1 בכניסה (i,i)) , אבל מהגדרת $\bar{L}_D$, $\langle M_i\rangle\notin\bar{L}_D$
- אם M_i לא מקבלת את $\langle M_i\rangle$, אז $\langle M_i\rangle\in L_D$ וכתוב 1 בשורה של $\bar{L}_D$ לעומת 0 ב (i,i)

כנדרש

כעת נראה ש $L_D\notin R$:

נניח בשלילה שכן:

אז $L_D\in R\overset{def'}{\Leftarrow}\overline{L_D}\in R\overset{R\subseteq RE}{\Leftarrow}\overline{L_D}\in RE$, וזו סתירה

$\square$

0.1.7 **טענה** 5.2 **:** $L_u\in RE\setminus R$

הוכחה: **נראה קודם ש** $L_u\in RE$ (סטנדרטי) . נבנה מ"ט N_u המקבלת את L_u

$M_u(y)$:

1. אם y אינה מהווה קידוד חוקי $(\langle M\rangle,\langle X\rangle)$ של זוג מכונה וקלט עבורה, נעצור ונדחה. תקינות סינטקטית כזו, אפשרית לבדיקה (למשל צריך לוודא התאמה בין $\sum$ של M של x וכו'...)
2. נריץ את M על x (בדומה למכונה האונבריסלית שבינינו בהרצאה 3 נבצע סימולציה צעד־צעד)

   אם M קיבלה, נקבל ואם דחתה, נדחה.

נכונות

אם $L_u\ni y=(\langle M\rangle,\langle X\rangle)$: M מקבלת את x (מהבניה) $\Leftarrow L_u$ תזהה שהקלט תקין ב 1 וב 2 הסימולציה תעצור ותזהה קבלה. מהבניה של M_U ,גם M_U תעצור ותקבל

אם $y\notin L_u$ ישנם שלושה מקרים:

1. y אינו קידוד תקין. M_U תזהה זאת בשלב 1 ותדחה $\Leftarrow y \notin L(M_U)$, כנדרש.

2. M בריצה על x (והקידוד חוקי) דוחה. במקרה זה, M_U תעצור בשלב 2 (בסימולציה), ותזהה דחיה ותדחה גם $\Leftarrow y \notin L(M_U)$ כנדרש,

3. M לא עוצרת על x (הקידוד חוקי). M_U בסימולציה בשלב 2 לא תסיים את הסימולציה (על כל צעד של M בריצה על M_U מסמלצת את הצעד, כיוון שיש ∞ צעדים יהיו ∞ צעדי סימולציה), ולא תעצור (על y) $\Leftarrow y \notin L(M_U)$, כנדרש.

נראה ש $L_u \notin R$

איך? נשתמש בעובדה ש $L_D \notin R$ (הוכחנו בשבוע שעבור): נניח בשלילה ש $L_U \notin R$ נשתמש במכונה המובטחת M_U (שמכריעה את L_U, לפי ההנחה בשלילה) כדי לבנות מ"ט M_D שתכריע את L_D. אבל זו תהיה סתירה כי $L_D \notin R$ ולכן אין מכונה כזו.

כיצד M_D תוגדר?

$M_D(\langle M \rangle)$:

- נריץ את M_U על הקלט $x = (\langle M \rangle, \langle M \rangle)$ (האם המכונה מקבלת את הקידוד של עצמה) ונענה כמוה (אינטואיטבית, כי M_U יודעת לענות בדיוק על השאלה האם מכונה עוצרת על קלט נתון, ואותנו מעניינת התשובה לגבי המכונה M והקלט $\langle M \rangle$).
- כיצד נעשה זאת: בדומה למימוש של המכונה האוניברסלית. בפרט, הקידוד של M_u (שמהמכונה האוניברסלית צריכה) יגיע מ δ של M_D. כלומר נרשום את $\underbrace{(\langle M \rangle, \langle M \rangle)}_{input}, \underbrace{\langle M_u \rangle}_{machine}$ בתור קלט לפרוצדורה שתריץ את המכונה האוניברסלית.

  הערה לגבי הקלט: קל לייצר (להכפיל את $\langle M \rangle$ זה אפשרי ב RAM, אפילו ראינו מימוש במ"ט בהרצאה 2)

נשאר להראות ש M_U מכריעה את L_D :

$\langle M \rangle \in L_D \Leftarrow M$ מקבלת את $\langle M \rangle \Leftarrow$ בסימולציה של M_u על קלט $(\langle M \rangle, \langle M \rangle)$ M_u תקבל ולכן גם M_D תקבל את (את $\langle M \rangle$) $\Leftarrow \langle M \rangle \in L(M_D)$ כנדרש.

$\langle M \rangle \notin L_D \Leftarrow M$ אינה מקבלת את $\langle M \rangle$ (נתעלם מחוקיות קידוד) $\Leftarrow$(מההנחה ש M_U מכריעה את L_U) של M_U דוחה את $(\langle M \rangle, \langle M \rangle) \Leftarrow M_D$ דוחה את $\langle M \rangle$, ובפרט עוצרת על $\langle M \rangle$

כלומר לסיכום, M_D תמיד עוצרת עם התשובה הנכונה לגבי שייכות של $\langle M \rangle$ ל $L_D \Leftarrow M_D$ מכריעה את L_D וזו סתירה. לכן M_U שמכריעה את L_U אינה קיימת, ולכן $L_U \in R$

$\square$

0.2 רידקוציות

0.2.1 $L_D \leq L_U$

הפונקציה שהגדרנו היא:

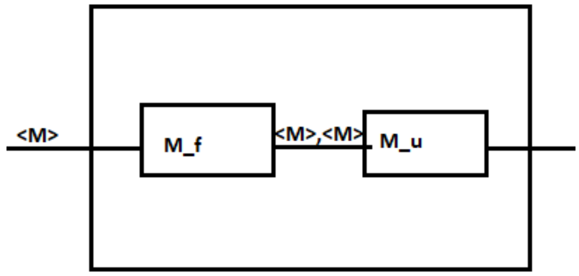
$$f(\langle M \rangle) \to (\langle M \rangle, \langle M \rangle)$$

נראה שהיא אכן מקיימת את שלושת התכונות של פונק' רדוקציה מ L_D ל L_n)

1. f מלאה (כל מחרוזת נתן לפרש כקידוד של מכונה) בפרט ההגדרה של f לא דורשת אפילו את זה.
2. f נתנת לחישוב - קל לקחת מחרוזת ולשכפל אותה

3. תקפה: $f(\langle M\rangle) = (\langle M\rangle, \langle M\rangle) \in L_U \Rightarrow M$ מקבלת את $\langle M\rangle \Rightarrow \langle M\rangle \in L_D$
ואם: $f(\langle M\rangle) = (\langle M\rangle, \langle M\rangle) \notin L_U \Rightarrow M$ לא מקבלת את $\langle M\rangle \Rightarrow \langle M\rangle \notin L_D$

מה הוכחה עשתה? בנתה M_D מתוך M_U (דמיונית שהנחנו בשלילה את קיומה) בעזרת f . כיצד? נסמן ב M_f מ"ט המחשבת את f . בנינו את M_D כ:



כיוון ש M_f , וM_u תמיד עוצרות ו M_f תקפה, התשובה של M_u לגבי שייכות $f(\langle M\rangle)$ ל L_u זהה להאם $\langle M\rangle$ שייכת ל L_D כלומר M_D הזו מכריעה את L_D . וזו סתירה.

0.2.2 משפט הרידוקציה:

אם $L_1 \le L_2$ אז:

1. אם $L_2 \overset{*}{\in} R$ אז גם $L_1 \in R$
2. אם $L_2 \overset{**}{\in} RE$ אז גם $L_1 \in RE$
3. אם $L_2 \in CoRE$ אז גם $L_1 \in CoRE$

ניסוח שקול (ושימושי) למשפט הרדוקציה: אם $L_1 \le L_2$ אז:

- אם $L_1 \notin R$ אז גם $L_2 \notin R$
- אם $L_1 \notin RE$ אז גם $L_2 \notin RE$
- אם $L_1 \notin coRE$ אז גם $L_2 \notin CooRE$

הוכחה - עבור 1

- נניח ש $L_1 \le L_2$ וגם $L_2 \in R$ אז:
  - קיימת מכונה M_2המכריעה את L_2
  - וכן קיימת מ"ט M_f המחשבת את פונ' הרדוקציה בין L_1 ל L_2
- נתאר מכונה מכריעה M_1 עבור L_1
- M_1 על קלט $x \in \sum^*$
  - תריץ את M_f על x ותקבל $f(x)$
  - תריץ את M_2 ותקבל על $f(x)$ ותענה כמוה
- מכיוון שפונ' הרדוקציה מלאה וניתנת לחישוב החישוב של M_1 לא יתקע בשלב 1 ,
- ומכיון שפונ' תקפה התשובה של M_2 על השייכות של $f(x)$ ל L_2 זהה לתשובה הדרושה עבור השייכות של x ל L_1

תכונות של רדוקציה

- אם $L_1 \leq L_2$ אז גם $\bar{L}_1 \leq \bar{L}_2$ - (תוצאה ישירה של תקפות הרידוקציה)
- היחס $\leq$ הוא רפלקסיבי: לכל שפה $L \subseteq \sum^*$, $L \leq L$ - הוכחה לפי פונ' הזהות.
- היחס $\leq$ טרנזיטיבי: אם $L_1 \leq L_2$ וגם $L_2 \leq L_3$ אז: $L_1 \leq L_3$ - הוכחה הרכבת פונקציות
- היחס $\leq$ אנטי־סימטרי: אם $L_1 \leq L_2$ אז לא בהכרח ש: $L_2 \leq L_1$

$L_{=3} \notin RE \cup coRE$

$$L_{=3} = \{\langle M \rangle \,|\, |L(M)| = 3\} \notin RE \cup coRE$$

הוכחה ־יש להראות 2 רדוקציות:

1. $HP \leq L_{=3}$ נקבל $L_{=3} \notin R$, $L_{=3} \notin coRE$
2. $\overline{HP} \leq L_{=3}$ נקבל $L_{=3} \notin RE$

הוכחה 1 : $HP \leq L_{=3}$

נגדיר $f(\langle M, x \rangle) = \langle M^* \rangle$, כך ש M^* על קלט $y \in \sum^*$

1. מריצה את M על x
2. אם $y \in \{0,1,01\}$ קבל
   אחרת - דחה.

f מלאה וניתנת לחישוב - כי ראינו שניתן לקודד מ"ט

f תקפה:

- $\langle M, x \rangle \in HP \Leftarrow M$ עוצרת על $x \Leftarrow M^*$ תקבל כל $y \in \{0,1,01\} \Leftarrow L(M^*) = \{0,1,01\} \Leftarrow |L(M^*)| = 3 \Leftarrow$ $\langle M^* \rangle \in L$
- $\langle M, x \rangle \notin HP \Leftarrow M$ לא עוצרת על $x \Leftarrow M^*$ תמיד תכנס ללואה $\Leftarrow L(M^*) = \phi \Leftarrow |L(M^*)| = 0 \neq 3 \Leftarrow \langle M^* \rangle \notin L$

הוכחה 2 : $\overline{HP} \leq L_{=3}$

נגדיר $f(\langle M, x \rangle) = \left\langle \widetilde{M} \right\rangle$ כך ש: $\tilde{M}$ על קלט $y \in \sum^*$

1. אם $y \in \{0,1,01\}$ קבל
2. הרץ את M על x, אם עצרה - קבל

f מלאה וניתנת לחישוב כי ראינו שניתן לקודד מ"ט

f תקפה:

- $\langle M, x \rangle \in \overline{HP} \Leftarrow M$ לא עוצרת על $x \Leftarrow \tilde{M}$ תקבל רק את $y \in \{0,1,01\}$(משלב 1) $\Leftarrow \left| L\left(\tilde{M}\right) \right| = 3 \Leftarrow \left\langle \tilde{M} \right\rangle \in L_{=3}$

- $\langle M,x\rangle\notin\overline{HP}$ ⇐ M עוצרת על x ⇐ $\tilde{M}$ בשלב 1 תקבל את כל $y\in\{0,1,01\}$ ובשלב 2 תקבל $\sum^*$ = $L\left(\tilde{M}\right)$ ⇐ $3 \neq \infty = \left|\sum^*\right|$ ⇐ $\left\langle\tilde{M}\right\rangle\notin L_{=3}$

נתונה השפה: $L_\infty=\{\langle M\rangle \mid |L(M)=\infty|\}\notin RE\cup coRE$

הוכחה ע"י

1. $HP\le L_\infty$ - בבית
2. $\overline{HP}\le L_\infty$ - קצת טריקית

0.2.3 $\overline{HP}\le L_\infty$

נגדיר $f(\langle M,x\rangle)=\langle M_x\rangle$, כך ש M_x על קלט $y\in\sum^*$

1. הרץ את M על x למשל $|y|$ צעדים
2. אם M לא עצרה - קבל
   אחרת - דחה

f מלאה וניתנת לחישוב...

f תקפה:

- $\langle M,x\rangle\in\overline{HP}$ ⇐ M לא עוצרת על x ⇐ $L(M_x)=\sum^*$ ⇐ $\langle M_x\rangle\in L_\infty$
- $\langle M,x\rangle\notin\overline{HP}$ ⇐ M עוצרת על x , אחרי t כלשהו של צעדים, נפצל למקרים:
  - אם $|y|\ge t$ ⇐ M_x תדחה
  - אם $|y|<t$ ⇐ M_x תקבל
- בכל מקרה, $L(M_x)=\{y|y<t\}$ וזאת שפה סופית! ⇐ $\langle M_x\rangle\notin L_\infty$

0.2.4 טענה 7.2 : $L_{eq}\notin RE\cup CoRE$

הוכחה: נוכיח באמצעות רדוקציה $L_\infty\le L_{eq}$, שימו לב שכיוון ש $L_\infty\notin RE\cup CoRE$ נתן להוכיח את שני הדברים "בבת אחת" ספציפית מ $L_\infty\le L_{eq}$:

1. $L_{eq}\notin RE$, כי $L_\infty\notin RE$ - משפט הרדוקציה סעיף 2
2. $L_{eq}\notin CoRE$,כי $L_\infty\notin CORE$ - הרצאה קודמת - משפט הרדוקציה סעיף 3

נבנה רדוקציה מתאימה: $f(\langle M\rangle)=(\langle M_1\rangle,\langle M_2\rangle)$

כאשר:

- $\langle M_2\rangle=\left\langle M_{\sum^*}\right\rangle$ מ"ט שמיד עוצרת ומקבלת כל מילה (מיד מ q_0 הולכת ל q_{acc})
- $M_1(y)$: מריצה את M על $\sum^*$ בהרצה מבוקרת. אם בצעד מסויים i של ההרצה המבוקרת התקבלו כבר $|y|$ מילים, נעצור ונקבל את y .

נסביר רגע בדוגמה:

- נגיד ש M מקבלת את 11 (המילה ה 7 בסדר לקסקוגרפי), בצעד ה 328 ,
- את 0 (מילה 2 בסדר הלקס' בצעד 512),
- ועוד ∞ מילים בצעדים יותר מאוחרים.
- אז M_1 על קלט $y = 10$ תקבל את y בצעד 512 (כאשר מתקבלת המילה השניה) בציור:

$string \backslash step$	1	2	$\dots$					
ε_0						X		X
								$\dots$

נחזור לרידוקציה - נכונות:

1. f מלאה - כל מחרוזת ניתן לפרש כקידוד של מכונה (לפי המוסכמה שלנו של M_{stam}), לכן f אכן מוגדרת על כל קלט.
2. f נתנת לחישוב: כדי לחשב את f מבצעים פעולת קומפילציה, בפרט אין צורך להריץ מכונות על קלטים כלשהם. (זה וריאנט של המכונה האוניברסלית, ו M_1 תדאג לרשום לה את $\langle M \rangle$ בתור המכונה שמריצים - את כל זה לא קשה לקודד)
3. תקפות :

- עבור $\langle M \rangle \in L_\infty$: M_1 תקבל כל y , כי M מקבלת ∞ מילים, ולכן בהנתן y מסוים, תקבל $|y|$ מילים תוך מס' סופי של צעדים ברצה מבוקרת
$\Leftarrow$ $L(M_1) = \sum^*$ $\Leftarrow$ $L = L(M_1) = L(M_2) = L\left(\sum^*\right) = \sum^*$, מכאן ש $f(\langle M_1 \rangle) = (\langle M_1 \rangle, \langle M_2 \rangle) \in L_{eq}$ כנדרש.
- עבור $\langle M \rangle \notin L_\infty$ $\Leftarrow$ M מקבלת N (מס' סופי של מילים) $\Leftarrow$ M_1 תקבל אך ורק את הyים שאורכם $\geq N$ $\Leftarrow$ $L(M_1)$ שפה סופית $\Leftarrow$ $L(M_1) \neq L(M_2) = \sum^*$ $\Leftarrow$ $(\langle M_1 \rangle, \langle M_2 \rangle) \notin L_{eq}$, כנדרש.

$\square$

0.3 $Rice$

0.3.1 משפט $Rice$ 7.4 :

תהי S תכונה של שפות ב RE , נגדיר: $L_S = \{\langle M \rangle | L(M) \in S\}$ אז:

$$L_S \in R \iff S \text{ טריויאלית}$$

$\Leftarrow$ כיון קל:

- תהי S תכונה טריוויאלית של שפות ב RE . נראה ש $L_S \in R$. ישנן שתי אפשרויות:

1. $S=RE$ אזי: $L_S=\{\langle M\rangle|L(M)\in RE\}$
אבל, מהגדרת RE , לכל N , $L(M)$ ב RE כי M היא מ"ט המקבלת את $L(M)$. מהמוסכמה שכל מחרוזת היא קידוד של מכונה כלשהי , $L_S=\sum^*$ אכן $\sum^*\in R$ (קל לבנות מ"ט שתקבל אותה).
2. $S=\phi$ אז $L_S=\{\langle M\rangle|L(M)\in\phi\}=\phi$, אכן $\phi\in R$ (קל לבנות מ"ט שתכריע אותה)

$\Rightarrow$ כיוון שני:

- תהי S לא טריוויאלית נוכיח ש $L_S\notin R$ באמצעות רדוקציה שתעבוד לא S (נחלק לשני מקרים) - "משפחה" של רדוקציות.

מקרה 1: נניח $\phi\notin S$. נראה $HP\leq L_S$. כיון ש $HP\notin R$, משפט הרדוקציה , $L_S\notin R$

$f(\langle M\rangle,\langle x\rangle)=\langle M_x\rangle$ כאשר:

$M_x(y)$:

1. מריצה את M על x
2. (המקרה בו עברנו את המחסום) תהי $L\in S$ קיימת כזו, כי S לא טריוויאלית, כיון ש $S\subseteq RE$ קיימת לה מ"ט M_L המקבלת אותה נריץ את M_L על y ונענה כמוה

נוכיח נכונות של f :

1. f מלאה - למעשה כמו שהגדרנו אותה אינה מלאה כי לא טיפלנו במקרה $(\langle M\rangle,\langle X\rangle)$לא תקין סינטקטית . אבל תמיד אפשר לטפל בזה ע"י בדיקת סינטס (קל לעשות), ואם לא עובר, פולטים M' קבוע שאינה ב L_s (במקרה הזה M_ϕ כלשהי שמיד דוחה הכל) בהמשך נתעלם מענייני תקינות סינטקטית
2. f ניתנת לחישוב - פעולת קומפילציה
3. תקפות:

- $(\langle M\rangle,\langle x\rangle)\in HP \Leftarrow$ M עוצרת על x $\Leftarrow$ לכל y M_x מגיעה לשלב 2 ועונה כמו M_L $\Leftarrow$ $L(M_x)=L(M_L)$ (מבחירת $L\in S$ $\Leftarrow$ $L(M_x)\in S$ (הגדרת L_S)$\Leftarrow$ $\langle M_x\rangle\in L_s$
- $(\langle M\rangle,\langle x\rangle)\notin HP \Leftarrow$ M לא עוצרת על x $\Leftarrow$ לכל קלט y , M "מתנקעת" בשלב 1 $\Leftarrow$(מהנחה) $L(M_x)=\phi\notin S$ $\Leftarrow$ $\langle M_x\rangle\notin L_S$

כנדרש

מקרה 2: $\phi\in S$. נשים לב ש:

$$L_S=\{\langle M\rangle|L(M)\in S\}=\overline{L_{\overline{s}}}=\{\langle M\rangle|L(M)\in RE\backslash S\}$$

כי לכל $S\subseteq RE$, M מסוימת , $L(M)\in S$ או $L(M)\in RE\backslash S$

- כעת, $\phi\in S$,אז בהכרח $\bar{S}=RE\backslash S\not\ni\phi$. $\phi\notin\bar{S}=RE\backslash S$.
- לכן $L_{\bar{S}}$ אינה ב R בגלל המקרה הקודם.
- בפרט $\bar{S}$ אינה טריוויאלית כי S אינה טריוויאלית
- מסגירות של R למשלים, גם $L_S=\overline{L_{\bar{S}}}$ אינה ב R (אחרת גם $L_{\bar{S}}$ הייתה ב R). מש"ל.

$\square$

0.3.2 $L_\varepsilon \in RE\backslash E$ בעזרת $Rice$

דוגמה 1 : נגדיר $L_\varepsilon = \{\langle M\rangle \,|\mathrm{M\ accept}\ \varepsilon\}$ (מקבלת את ε) , נראה ש

הוכחה:

- כדי להראות שייכות ל RE , נתן לבנות מ"ט M_ε המקבלת את L_ε שעל קלט $\langle M\rangle$ מריצה את M על ε ועונה כמוה (בפרט אם M לא עוצרת, גם היא לא תעצור).
- כדי להראות $L_\varepsilon \notin R$ נשתמש במשפט $Rice$.
- נגדיר תכונה לא טריויאלית של שפות S כך ש $L_\varepsilon = L_S$ במקרה זה: $S = \{L \in RE|\varepsilon \in L\}$. כדי להשמתש ב $Rice$ צריך להראות ש S לא טריויאלית
  - $S \neq RE$: $\phi \in RE\backslash S$ לדוגמה
  - $S \neq \phi$, למשל : $\sum^*, \{\varepsilon\}, \{\varepsilon, 01101\} \in S$
- לכן מ $Rice$ נסיק ש $L_\varepsilon \notin R$

$L'_\varepsilon = \{\langle M\rangle \,|\mathbf{M\ doesnt\ accept}\ \varepsilon\} \notin R$ (לא מקבלת את ε) בעזרת $Rice$

האם ניתן להשתמש ב$Rice$ כדי להוכיח שאינה ב R (למעשה היא השפה המשלימה של L_ε ולכן אינה ב R מסגירות למשלים ־ אבל כאן מעניין אותנו ספציפית $Rice$). אפשר . נגדיר

$$S = \{L \in RE|\varepsilon \notin L\}$$

גם כאן S לא טריוויאלית. (אפשר להפוך סימנים בין הדוגמאות ל L_ε)

0.3.3 $L"_\varepsilon = \{\langle M\rangle \,|\mathbf{M\ reject}\ \varepsilon\}$

האם ניתן להשתמש כאן ב $Rice$ כדי להראות ש $L_\varepsilon \notin R$ (זה לכשעצמו נכון נכון)? כאן זה לא אפשרי, כלומר לא קיימת S מתאימה כך ש $L"_\varepsilon = L_S$. אינטואיטיבית $L"_\varepsilon$ בודקת תכונה של M שאינה רק תכונה של $L(M)$. אפשר להראות זה במפורש: נראה זוג מכונות $\langle M_1\rangle, \langle M_2\rangle$ שאחת ב $L"_\varepsilon$ והשניה לא, אבל $L(M_1) = L(M_2)$

$M_1(y)$: מיד עוצרת ודוחה:$L(M_1) = \phi$ וגם $\langle M\rangle \in L_\varepsilon$ (דוחה את ε)

$M_2(y)$: למשל תמיד נכנסת ללואה על q_0 . $L(M_2) = \phi$ כאן $\langle M_1\rangle \notin L"_\varepsilon$ (לא דוחה את ε)

נשים לב ש L'_ε שראינו היא אינה ב RE . $Rice$ נתן לנו חלק מהאבחנה ־ מוכיח ש L'_ε . כדי להראות ש $L'_\varepsilon \notin RE$, נתן להסתמך על כך ש $L_\varepsilon \notin RE$ (דוקא אבחנה "חיובית")

וכיון ש $L_\varepsilon = \overline{L'_\varepsilon}$, נסיק מידית שלא יתכן $L'_\varepsilon \in RE$, אחרת היה $L'_\varepsilon \in RE \cup CoRE = R$ בסתירה ל $L_\varepsilon \notin RE$ ל $\overline{L_\varepsilon} \in R$ (סגירות R למשלים)

0.3.4 משפט 7.5 ל $Rice\ RE$: **תהי S תכונה לא טריוויאלית של שפות ב RE אז אם $\phi \in S$ אז $L_s \notin RE$**

הערה: זה אפיון מלא כמו במקרה של R . ידוע אפיון, אבל לא לא נלמד אותו בקורס.

הוכחה:

- נראה ש $\overline{HP} \leq L_S$, ונסיק ש $L_S \notin RE$, כי $\overline{HP} \notin RE$, ברידוקציה
- $f(\langle M\rangle, \langle X\rangle) = \langle M_x\rangle$ כאשר $M_x(y)$:

1. מריצה את M על x
2. תהי $L \in RE \backslash S$ קיימת כזו כי S לא טריוויאלית. תהי M_L מכונה שמקבלת את L. M_xתריץ את M_L על y ותענה כמוה.

נכונות הרדקוציה:

- f מלאה ונתנת לחישוב - פעולת קומפילציה
- תקפות:
  - $(\langle M\rangle, \langle x\rangle) \in \overline{HP}$ $\Leftarrow$ M לא עוצרת על x $\Leftarrow$ M_x תתקע בשלב 1 (לכל y) $\Leftarrow$(מהנחה) $L(M_x) = \phi \in S$ $\Leftarrow$ $\langle M_x\rangle \in L_S$, כנדרש.
  - $(\langle M\rangle, \langle x\rangle) \notin \overline{HP}$ $\Leftarrow$ M עוצרת על $x$$\Leftarrow$ M_x תגיע ל 2 (לכל y) ואז תענה כמו M_2 (בחירת L)$\Leftarrow$ $L(M_x) + L \notin S$ $\Leftarrow$ $\langle M_x\rangle \notin L_S$, כנדרש.

מש"ל

0.4 מ"ט אי־דרמינסטית

0.4.1 $RE = RE_{ND}$

הוכחה (סקיצה) - הכלה דו־כיוונית

כיון קל - $RE \subseteq RE_{ND}$:

- תהי M דטרמינסטית, נבנה M' א"ד המקבלת את אותה שפה ע"י "שכפול של δ
- כלומר , לכל $\delta(q,a) = (p,b,m)$ נגדיר $\delta'(q,a) = ((p,b,m), (q,b,m))$
- לא קשה להראות ש $L(M') = L(M)$ (עץ החישוב של δ יורכב משכפולים של מסלול החישוב של M)
- אופציה אחרת: $\delta'(q,a) = \left((p,b,m), \left(q_{a_j}, b, m\right)\right)$ - שומרים על המסלול המקורי, ומוסיף הרבה מסלולים שנתקעים

כיון שני - $RE_{ND} \subseteq RE$:

נסיון I : תהי M מ"ט א"ד .נבנה M' דטר' שקולה באופן הבא: $M'(x)$ תבצע DFS על עץ החישוב של M על x (תפתח את עץ־הקונפיגרוציות) אם זיהתה 'קבל' תקבל מייד.

זה לא עובד, כי ייתכן שנתקע במסלול אינסופי לפני שנגיע ל q_{acc} .

נסיון II: נסרוק את עץ החישוב של M על x ב BFS . בצעד ה i נפתח את רישות המסלולים עד אורך i . אם נזהה קבלה, נקבל.

המשפט שהוכחנו יכול להקל על הוכחות ששפה מסוימת L כן ב RE ולהחליף הרצה מבוקרת. לדוגמה: נתבונן ב L מהצורה:

$L = \{M \mid\mid |x_1| < |x_2| < |x_3|$ וגם x_2 ודוחה את x_1, x_2 מקבלת את M ש x_1, x_2, x_3 קיימת 3 מילים $\}$

$L \in RE$ נתן להוכיח זאת ע"י בניית מ"ט שמבצעת הרצה מבוקרת, אבל גם להוכיח ע"י בניית מ"ט א"ד מתאימה.

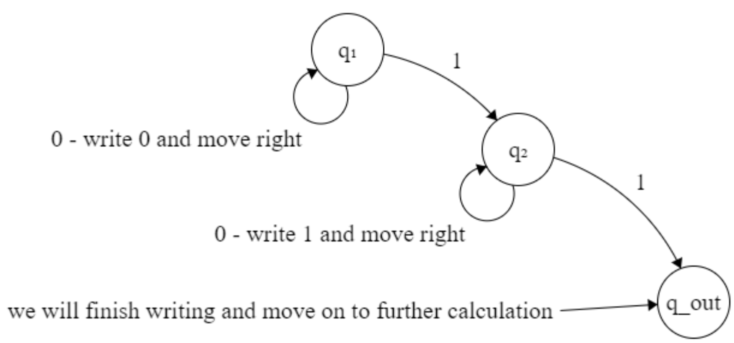
$M_L(\langle M \rangle)$:

1. תנחש מילים x_1, x_2, x_3
2. אם $|x_1| < |x_2| < |x_3|$ תריץ את M על $x_1, x_2, x3$ סדרתית.
   - אם M קבלת את x_1, x_3 ודחתה את x_2 נקבל
   - (אחרת, או נתקע אם M נתקעת על אחד הקלטים).

כעת נבהיר מהו הניחוש וכיצד ממשים אותו. נוכיח ראשית נכונות:

- אם $\langle M \rangle \in L$: קיימים x_1, x_2, x_3 מתאימים $\Leftarrow$ קיים ניחוש שמנחש את x_1, x_2, x_3 $\Leftarrow$ במסלול שבו מנחשים אותו M בהכרח תקבל $\Leftarrow$ קיים מסלול מקבל $\Leftarrow$ $\langle M \rangle \in L(M)$, כנדרש.
- אם $\langle M \rangle \notin L$: לא קיימים x_1, x_2, x_3 כנדרש $\Leftarrow$ לכל ניחוש x_1, x_2, x_3 לא נקבל (נדחה או נתקע)

כיצד נממש את תהליך הניחוש? (זה תמיד יעבוד), ננחש מחרוזת ש $0,1$ ים ובסוף נפרסר אותה בתור $x_1 \underbrace{,}\ x_2 \underbrace{,}\ x_3$ (אם יתאפשר , ויצאה לנו מחרוזת חוקית, אחרת מיד נדחה). בכל צעד נרצה להוסיף ביט $0/1$ או לעצור (סיימנו לכתוב את המחרוזת) , כלומר יש 3 אפשרויות אבל δ מרשה רק 2 . נממש ע"י שני מצבים (שגרת ניחוש):



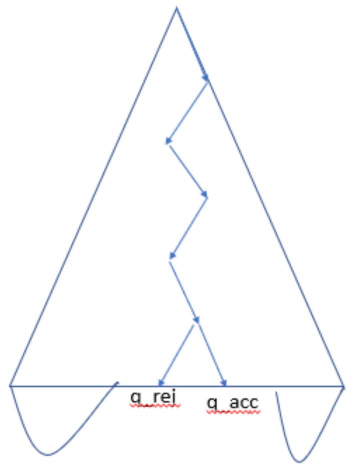
0.5 סיבוכיות

0.5.1 משפט 9.4 : הגדרות 9.3 ו 8.9 לNP שקילות

הוכחה: נראה הכלה דו־כיוונית (של המחלקות הרלוונטיות

כיון 1 : תהי $L \in NP$ לפי הגדרה 8.9

- תהיה M מ"ט א"ד המקבלת את L בזמן החסום ע"י פולינום pm . נבנה יחס־NP R כך ש $L = L_R$
- $R(x,y)$ (אם $(x,y) \in R$ נקרא ל y "עד" (לשייכות x ל L_R)) y: הוא מסלול בעץ החישוב של M על xהמסתיים ב q_{acc} לדוגמה $y = 1101101$ ־ מגדיר רצף בחירות של δ ־ מתוך 0 או 1) עד לשייכות x לשפה עבור הדוגמה להלן, אבל 110110 או 1101100



- ראשית נבדוק שאכן $L = L_R$:
  - $x \in L$: M מקבלת את x $\Leftarrow$ קיים מסלול y ב M המקבל את x $\Leftarrow$ (מהגדרת y - y המתאים למלסלול זה) קיים y כך ש $R(x,y)$
  - $x \notin L$: לא קיים מסלטל מקבל ב M $\Leftarrow$ כל y יקיים $(x,y) \notin R$
- נשאר לוודא ש R הוא אכן יחס NP :

1. חסום פולינומית: מהגדרת R , $(x,y) \in R$ $\Leftarrow$ $|y| \le p(|x|)$, החסם על זמן הריצה של M בכל מסלול
2. נתן לזיהי פולינומי בהנתן (x,y) , נסמלץ את ריצת M על x על המסלול המוגדר ע"י y .

- נפרט קצת מדוע החישוב אכן פולינומי - נקבל אם"ם המסלול y מסתיים ב q_{cc} :
  - הסימולציה מתבצעת בדומה למ"ט אוניברסלית. בכל מקרה, אורך המסלול שבודקים הוא $\min((|y|, p(|x|))) \le |y| + p(|x|)$
  - במהלך ההרצה נשמור קונ' הנוכחית ונעדכן בכל פעם (תוכן סרט + מקום ומצב) , זמן החישוב:

$$\underbrace{\#\text{Calculation steps}}_{\le |y|+p(|x|)} \times \underbrace{\text{Next configuration's calculation time}}_{O(|x|+p(|x|)+y)*}$$

$*$ הסבר: בערך לינארי אורך הקונפ' , אורכה $O(..)$ כי בכל צעד חישוב הסרט גדל ב1 לכל היותר

- כלומר סה"כ מספר צעדים פולינומי בקלט $|(x,y)|$.

כיון שני: תהי L שפה ב NP לפי הגדרה 9.3 נראה $L \in NP$ לפי הגדרה 8.9

- יהי R יחס NP מתאים עבור L, ויהי $P(x))$ החסם מ1 ו $q(n)$ חסם זמן ריצה הריצה של אלג' המזהה את $\tilde{L}_R$ (מהגדרה $1,2$ שניהם פולינומים).
- נבנה מ"ט א"ד פולינומית עבור L :

בניה:

- $M(x)$: בגדול M תנחש את y , ותבדוק אם אכן $R(x,y) = True$
- נפרט:

1. M תחשב את $P\left(|x|\right)$
2. תהליך הניחוש: תקצה קטע : $\underbrace{*\_\_\_\_\_\_\_\_\_\_\_\_*}_{p(|x|)}$

תעבור לתחילתו ותנחש מחרוזת של 0ים ו1ים שמסתיימת לכל היותר לפני ה $*$ השניה. (כלומר כל עוד לא הגענו ל $*$ "ננחש" ביט חדש b ונשרשר אותו, או שנעצור כאן. בכל מקרה כשעוצרים y הוא:

$$\underbrace{*\_\_\_\_\_\_\_\_|\downarrow....*}_{y}$$

3. תבדוק האם $R\left(x,y\right)=T$, ותקבל אם כן, אחרת תדחה.

נכונות:

1. יורכב משלושה שלבים:

(א) נמיר מ $|x|$ בעצם נתון באונארי, לבינארי. יקח בערך $O\left(|x|\log|x|\right)$ פעולות. (מעדכנים מונה באורך $\log|x|$) , נסמן את המונה ב Cnt .

(ב) חשוב הפולינום $p\left(Cnt\right)=Cnt^{d}\cdot c$ - פולינומי באורך המונה השוטף שהוא $d\left(\log|x|\right)$ בכל רגע עושים $d-1$ הכפלות כופל בקבוע. סה"כ $poly\left(\log|x|\right)$

(ג) חלק מ2 - נקצה את השטח $*\_\_\_\_\_\_\_\_*$ שלמעשה דורש תרגום מבינארי חזרה לאונארי של $Cnt=p\left(|x|\right)$ בערך $p\left(|x|\right)\cdot poly\left(\log|x|\right)$. פעולות (נוריד 1 מהמונה על כל תא שנקצה עד שנגיע ל 0)

2. הסברנו

3. לוקח זמן :

עבור הy שחישבנו:

$$q\left(|x|+\underbrace{|y|}_{\leq p(|x|)}\right)\approx O\left(q\left(\underbrace{p\,|x|}_{\text{A polynomal too}}\right)\right)$$

הסכום עדיין פולינומי

נשאר להראות נכונות:

- $x\in L$ קיים y כך ש $R\left(x,y\right)\Leftarrow$ כיון ש M מ אפשרת לנחש כל y שארוכו $\geq P\left(|x|\right)$, בפרט יהיה קיים מסלול (אפילו הרבה- בכלל השלבים הדטרמינסטים בחישוב אם נממש על ידי הכפלה) שבו M תנחש את ה y המתאים (אורכו $\geq p\left(|x|\right)$) כי $p\left(n\right)$ חסם הנובע מכך שR חסום פולינומית שקבענו) $\Leftarrow$ מקבלת את $x \Leftarrow x\in L\left(M\right)$
- $x\in L \Leftarrow$ לא קיים y מתאים $\Leftarrow$ (בניית M) M תדחה בכל המסלולים

$\square$

0.5.2 נראה ש$factory\in NP$

$$factory=\{(x,k)\,|y\neq1 \text{ וכן } k\leq y<x \text{ המקיים } x \text{ של } y \text{ קיים מחלק } x,k\in\mathbb{N}^{+}\}$$

הוכחה:

נוכיח באמצעות בניית מ"ט א"ד יעילה.

בניה:

$M_{factoring}(n,k)$:

1. ננחש מספר y (באורך $\log_2 n \geq$ ביטים, עם אפסים מובילים). המספר הוא פשוט מחרוזת באורך n שבהמשך נפרסר כמספר.
2. נבדוק שאכן $y|n$ וכן $1 < k \leq y < n$ $(*)$. אם כן, נקבל אחרת נדחה.

נוכיח נכונות וסיבוכיות של הבניה:

נכונות:

- עבור $(n,k) \in factoirng$ $\Leftarrow$ קיים y המקיים את $(*)$. מהבניה, כל yשאורכו כאורך n (כלומר בפרט מכסה את כל המספרים $n \geq$ אבל רק אותם) $\Leftarrow$ קיים מסלול שבו מנחשים y מתאים והבדיקה שלו עובדרת $\Leftarrow$ $(n,k) \in L\left(M_{factoring}\right)$, כנדרש.
- עבור $(n,k) \notin factoring$ $\Leftarrow$ לא קיים y המקיים את $(*)$ $\Leftarrow$ בכל מסלול y יתגלה ב2 כלא מקיים את $(*)$ $\Leftarrow$ $M_{factoing}$ $\Leftarrow$ תדחה בכל המסלולים $\Leftarrow$ $(n,k) \notin L\left(M_{factring}\right)$, כנדרש.

יעילות:

- נראה פולינום $p(n)$ כך שזמן הריצה בכל מסלול חסום ע"י $p(n)$:
  - ראשית, $|y| = |n| \leq |k|$ (x הקלט)
  - הבדיקה ב2 דורשת פעולת חילוק על מס' באורך $\underbrace{O\left(\log n\right)}_{|x|}$ ביטים גם פולינומי ב$|x|$ לפי פעולת חילוק שלמדנו בכיתה ג' - בערך $O\left(m^2\right)$ פעולות על ביטים , עבור חלוקה של שני מס' באורך m ביטים .

אפשר לשים לב, שבהגדרת NP ישנה אסימטריה :

- אם הקלט $x \notin L$, אכן מסלול דוחה .
- ואם $x \in L$ אז נדרש רק קיום של מסלול מקבל אבל הרבה מסלולים אחרים יכולים לדחות.

במילים אחרות, (לפי ההגדרה האלטרנטיבית) מובטח עד קצר לשייכות לשפה שנתן לבדוק ביעילות, אבל לאי שייכות אין (באופן כללי) עד כזה.

0.5.3 $P \subseteq NP \cap coNP$

- תהי $L \in P$, אזי $\overline{L} \in P$ (P סגורה למשלים), נראה:
  1. $L \in NP$ ע"י בניית יחס NP מתאים.
     - למשל היחס הוא $\{(x,1)\,|x \in L\}$
     - חסום פול' - כי:
       (א) $|y| = 1$ אם $(x,y) \in R$
       (ב) ניתן לזיהוי פולינומי ע"י בדיקת:
          i. $y = 1$
          ii. $x \in L$ (אפשרי כי $L \in P$)
  2. $\overline{L} \in NP$ ע"י בניית יחס NP מתאים ל $\overline{L}$
     - באופן דומה נגדיר $R = \left\{(x,1)\,|x \in \overline{L}\right\}$ ....

0.5.4 $factoring \in NP$ הראנו, נותר להראות שייכות ל$coNP$.

הוכחה:

- נבנה יחס NP עבור $\overline{factoring}$, כיצד יראה עד y' לטענה $(n,k) \notin factroing$
  - $y' = (p_1, e_1), ..., (p_1, e_k)$ (הפירוק של n לגורמים ראשונים), כאשר $p_1 < p_2 < ... < p_t$ ראשוניים
  - מתקיים ש: $n = \prod_{i=1}^{t} p_i^{e_i}$
- $R((n,k), y')$ - צ"ל ש R אכן יחס NP עבור $\overline{factroing}$ (ענת בלבלה את הסדר בסה"כ צ"ל אלגוריתם + נכונות +יעילות):

1. אכן $\overline{factroing} = \{x | \exists y R(x,y)\}$, כי בדקנו בעזרת (y') האם המחלק הכי גדול של n k קטן/שווה או לא (ב $\overline{factoring}$ לא)
2. R חסום פול': (כי t קטן)
3. נתן להזיהוי פולי' -הסברנו תוך כדי

- האלגוריתם:

1. יבדוק שאכן $p_1 < ... < p_t$,וכולם ראשוניים. זה יעיל בדיקת ראשונית היא ב P (נמצא אלג' AKS רק ב 2002 שלוקח לפחות $\Omega(n^6)$ זמן)
2. בנוסף יבדוק שאכן, $n = \prod_{i=1}^{t} p_i^{e_i}$ זה יעיל כי $\sum e_i$ בפירוק אמיתי היא לכל היותר $\log_2 n = O(|x|)$ ו נבצע לכל היותר מס' כזה של כפליל על מס' באורך $O(|x|)$ (ה p_i- ים)
3. לבסוף נבדוק האם $y = \frac{n}{p_1}$ (p_1 המחלק הכי גדול) מקיים $y|n$ ו $1 < k \le y < n$ אם אכן לא מתקיים, מחזיר "כן" אחרת מחזיר "לא"

0.5.5 תכוונת היחס $\le_p$

אבחנה היחס $\le_P$ (יחס בינארי המוגדר על קב' השפות $P(\sum^*)$ מקיים:

1. רפלקסיבי : לכל $L \in P(\sum^*)$ מתקיים $L \le_P L$ - ע"י פונ' הזהות $f(x) = x$שהיא כמובן ב $POLY$
2. לא סימטרי:
   (א) נקח: $L_2 = HP, L_1 = \sum^*$:
   - אז $L_1 \le_p L_2$ (נמפה הכל למילה קבוע ב HP)
   - בכיון השני $\sum^* \not\le_p HP$ כי אפילו $\sum^* \not\le HP$ - (בגלל תקפות - "אין לאן" למות מילים ב HP)

   (ב) נשים לב שכל $L \in RE$ (ובפרט כל $L \in NP$, כי $NP \le RE$) מקיימת: $L \le_P L_u$.
   מדוע? עבור L נתונה תהי M_L מ"ט המקבלת את L . אזי $f(x) = (\langle M_L \rangle, \langle x \rangle)$ היא פונק' רידוקציה מתאימה שבפרט נתנת לחישוב בזמן פולינומי
   - בכיון השני, אם נבחר $L \in R$ כלשהי, $L_u \le_P L$ (אחרת נקבל סתירה למשפט הרדקוציה, כי ידוע ש $L_u \notin R$)
3. טרנזיטבית:

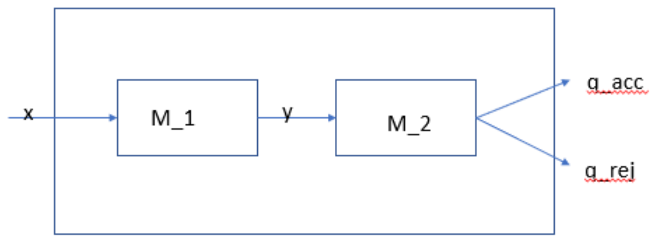
- אכן אם, $L_1 \le_p L_2$, וגם $L_2 \le_p L_3$ אז $L_1 \le_p L_3$: נרכיב את פונק' הרדוקציה בין 1 ל 2 לזו בין 2 ל 3 .בפרט הפונצקיה החדשה נתנת לחישוב (בזמן) פולינומי (החסם הוא הרכבה של החסמים הפולי' לשתי פונק' שהוא גם פולינום)

המשפט המרכזי בהקשר של NPC הוא משפט הרדוקציה לפונ' רדקוציה פונילנומיות. נזכיר:

משפט הרדוקציה 10.3: **יהיו** $L_1, L_2 \subseteq \sum^*$ **כך ש** $L_1 \leq_p L_2$. **אזי** $L_2 \in P \Leftarrow L_1 \in P$

הוכחה(דוגמה להוכה של מפשט הרדקוציה המקורי):

נבנה מ"ט פול' יעילה עבור L_1 :



M_1 מ"ט יעילה (דטר) עבור f $(f \in POLY)$

נתוח הבניה:

- נכונות:
  - תקפות f: $x \in L_1 \underbrace{\Leftrightarrow}_{f} f(x) \in L_2 \underbrace{\Leftrightarrow}_{M_1} M_1$ מקבלת את x
- יעילות: יהיו p_1, p_f פולינומים החוסמים את זמן הריצה של M_2, M_f בהתאמה.
  - אז M_1 רצה בזמן $\leq \underbrace{p_2(p_f(|x|))}_{\text{because: } |y| \leq p_f(|x|)} + \underbrace{p_f(|x|)}_{\text{f(x) - calculation time}}$

0.5.6 **משפט** 11.2 : **תהי** $L \in NPC$ **אז** $L \in P \Leftrightarrow P = NP$

הוכחה

כיון 1 :

- נניח $L \in P$ מהגדרת NPC (חלק 2)
- לכל $L' \in NP$ $L' \leq_p L$
- עכשיו ממשפט הרידקוציה $L' \in P \Leftarrow P = NP$ (כי L' שפה כלשהי ב NP)

כיון 2 :

- נניח ש $P = NP$, אז מהגדרת NPC (חלק 1) $L \in NP = P$ -

0.6 בעיות שונות ב NPC

0.6.1 **טענה** 11.3 **: תהי** $L \in NPC$ **ותהי** $L' \in NP$ **. אזי אם** $L \leq_p L'$ **אז** $L' \in NPC$

הוכחה ־נראה ש L'מקיימת את שתי הדרישות

1. $L' \in NP$ (נתון)
2. $L' \in NPH$.כלומר, מקיימת $L \leq_p L'$, וגם לכל $L" \in NP$

$L" \leq_p L$ (כי $l \in NPC$ ובפרט $L \in NPH$) כעת מטרנזיטביות של $\leq_p$, $L" \leq_p L'$ כלומר $L' \in NPH$ (כי $L"$ שפה כלשהי ב NP)

0.6.2 **משפט** 11.5 **:** $BH \in NPC$

הוכחה:

רעיון ההוכחה (לפחות לחלק של NPH) דומה לשלמות של L_u ב RE שראינו . בפרט לא מאוד מפתיע שהבעיה ב NPC (נובע כמעט מיידית מהגדרת NP)

פורמלית:

יש להראות ע"פ הגדרת NPC :

1. $BH \in NP$

נבנה א"ד פולינומית מתאימה:

: $M_{BH}\left(\langle M\rangle, 1^P, \langle x\rangle\right)$

1. תנחש מסלול חשוב בעץ של M על x שאורכו $\geq l$ (ראינו איך עושים זאת)

   כלומר המחרוזת y שמנחשים היא מהצורה $y = y_1, y_2, ...y_t$, כאשר y_i מגדיר אם בוחרים אפשרות 0 או 1 ב δ בצעד i
2. מריצה את M על x במסלול המוגדר ע"י y אם המסלול מסתיים בדיוק כך שy מסתיים, ומסתיים ב q_{acc} נקבל ,אחרת נדחה

נכונות הבניה:

נכונות :

$\left(\langle M\rangle, 1^P, \langle x\rangle\right) \in BH \iff$ ב M קיים מסלול y באורך $t \leq l$ המקבת את $x \iff$ (מהבניה) M_{BH} תנחש מסלול y מקבל כזה $\iff \left(\langle M\rangle, 1^P, \langle x\rangle\right) \in L\left(M_{BH}\right)$

יעילות:

- שלב 1 : ניחוש y : $O\left(l\right)$ צעדים
- שלב 2 (הרצה) : המכונה האוניברסלית שבנינו על קבלט $\langle M\rangle, \langle x'\rangle$ אכן רצה בזמן פולינומי ב $|M|$ ומספר צעדי הסימולציה ו $|x|$. (שמירה ועדכן קונפיגרוציה נוכחית.

  כאן מס' צעדי הסימולציה , היא $\geq l \Leftarrow$ פולינומי בקלט שאורכו $|\langle M\rangle| + l + |\langle x\rangle|$

2. $BH \in NPH$

תהי $L \in NP$ נגדיר רדקוציה פול'י מ L ל BH :

$f(x)$ פולטת: $\left(\langle M_L \rangle, 1^{P_L(|x|)}, \langle x \rangle\right)$, כאשר M_L מ"ט א"ד פולינומית (קיימת כי $L \in NP$), ו $P_L(|x|)$ חסם המובטח עבור M_L

נראה ש f אכן פונק' רידקוציה פלונומית תקפה מ L ל BH :

2. תקפות - ישירות מהגדרת NP וחסם זמן ריצה עבור מכונה א"ד פולינומית:

$$x \in L \iff \text{קיים ב } M_L \text{ מסלול המקבל את } x \overset{1}{\iff} \left(\langle M_L \rangle, 1^{P_L(|x|)}, \langle x \rangle\right)$$

1. כיון ש P_L חסם על אורך כל מסלול, מסלול מקבל, אם , קיים אורכו $\geq P_L(x)$

1 . $\delta \in POLY$: נבנה מ"ט פול' עבור M_f, f

$M_f(x)$:

1. כתיבת $\langle M_L \rangle$ - זמן קבוע $O(1)$. לא תלוי ב $|x|$.
2. חישוב זמן כתיבת x , לנארי ב $|x|$ (מקודדים אות־אות)
3. חישוב $P_L(|x|)$:

(א) נחשב את x בבינארי, בעצם נמיר את x מאונארי לבינארי , דורש בערך $O(n \log n)$ זמן

(ב) נחשב את הפולינום $P_L(b)$ - דורש מס' קבוע של כפלים על מספרים בגודל $O(\log |x|)$.

- לדוגמה אם $p = 17 \cdot n^4$: נבצע שלושה כפלים כדי לחשב n^4 נצבור בכל פעם את המכפלה עד כדי n, n^2, n^3 ואז נכפול ב 17 $\Leftarrow$ זמן $poly(\log |x|)$ - נשתמש באלג' בית לכפל. תהי c התוצאה

(ג) נמיר את c חזרה לאונארי = זמן $O(c \log c)$ שזה פולינומי ב $|x|$ בערך $P_L |x|$.

סה"כ פולנומי ב $|x|$

הערה: למה חשוב ב BH לייצג את החסם l על מס' הצעדים באונארי? למה לא בבינארי?

אם l היה נתון בבינארי אז M_{BH} שבינינו לא היתה בהכרח יעילה. למה?

M_{BH} מבצעת לפחות l צעדים באחד המסלולים (שבו מנחשים y באורך l) , בייצוג בינארי הקלט היה נראה כך $\langle\langle M \rangle, l, \langle x \rangle\rangle$ כאשר אם l בבינארי , הוא דורש $O(\log l)$ ביטים, זמן הריצה שלנו היה במקרה הגרוע אקספו' בקלט (לא מובטח ש $\langle M \rangle, \langle x \rangle$ מספיק ארוכים יחסית ל l)

0.6.3 משפט 12.4 $VC \in NPC$

הוכחה

1. 1. $VC \in NPC$ מ"ט א"ד פולינומית עבור VC - $M_{VC}(\langle G \rangle, k)$ תנחש קב' $U \subseteq V$ בגודל k , ותבדוק שהיא מהווה VC (כל הקשתות מכוסות על ידה)

לא קשה לראות שהמכונה אכן פולינומית (בפרט $|U|$ שמנחשים היא באורך $k \log n$ ביטים , לדוגמה והבדיקה גם ניתנת לבצוע בזמן פולינומי בגרף)

2. 2. $VC \in NPC$ - אחר ההפסקה

0.6.4 משפט 12.5 $HS \in NPC$

הוכחה:

1. $HS \in NP$: מ"ט א"ד פולי' מתאימה תחשב U ותבדוק שאכן $\forall i\ U \cup C_i \neq \phi$

2. $HS \in NPH$: נראה ע"י רדוקציה מ VC ממשפט 12.4 , נקבל ש $HS \in NPH$ (כי $VC \in NPH$)

רעיון הרדוקציה:

כאן , נשים לב ש VC הוא מקרה פרטי של HS : קיים מיפוי מאוד פשוט מקבל עבור VC לקלט עבור HS :

$f(\langle G \rangle, x)$: מזהה בין $V = \{v_1, ..., v_n\}$ ל $[n]$ (למשל נזהה בין v_i למספר i)

$k = k'$

נזהה בין E לבין הקב' $C_1, ..., C_t$ כל $e_i = \{v_{i1}, v_{i2}\}$ תמופה ל $C_i = \{i1, i2\}$

נפלוט :

$\left(n, k, C_1, ..., C_{t=|E|}\right)$ שקבלנו

נכונות הרידוקציה f :

f פולינומית: עוברים על הגרף, סופרים קודקודים ומעתיקים את מס' הקדקדים שיצא , את k ,ו את הקשתות (תוך כדי מיפוי למספרים התאימים) - זה פולינומי (ב $|\langle G \rangle, k|$)

תקפות f:

הרעיון כאן הוא (תמיד) להראות כיצד עד עבור x , מתרגם לעד עבור $f(x)$ ולהיפך (נרחיב עוד מעט)

כיון $\Leftarrow$:

יהיה $(\langle G \rangle, k) \in VC \Leftarrow$ קיימת $\{V_{i1}, ..., v_{ik}\}$ המהווה VC עבור $G \Leftarrow$ קיימת $\{i1, ..., ik\}$ המכסה את כל הקב' C_i ,שכן אם U הוא VC אז מתקיים בעצם $\forall e \in E\ e \cap U \neq \phi$, ולכן לכל C_i שהתקבל מe_i כלשהו $C_i \cap U' = \phi \Leftarrow f(\langle G \rangle, k) \in HS$

כיוון$\Rightarrow$:

בשונה מהחלק הראשון בקורס לא נוכיח: שאם $x \notin L_1$ אז $f(x) \notin L_2$, אלא נוכיח טענה שקולה שלפיה אם $f(x) \in L_2$ אז $x \in L_1$

במקרה שלנו:

נניח ש $f(\langle G \rangle, k) \in HS \Leftarrow$ קיימת קב' $U \in [n]$, $U = \{i_1, i_2, ..., i_k\}$ כך ש $\forall i\ U' \cap C_i \neq \phi \Leftarrow$ (בניה בפרט $k = k'$) קיים VC $\{v_{i1}, ..., v_{ik}\} = U$ עבור $G \Leftarrow (\langle G \rangle, k) \in VC$ כנדרש.

הערה: הכיון ההפוך $HS \leq_P VC$ יותר מסובך, כי VC הוא מקרה פרטי, רידוקציה אפשרית:

$$HS \leq_P SAT_P \leq_p 3SAT \leq_p VC$$

0.6.5 משפט 12.6 $SC \in NPC$

הוכחה:

1. $SC \in NP$. ננחש $i \subseteq [t]$ בודק k , ובודקים האם $\bigcup_{i \in I} C_i = [n]$

2. $SC\in NPH$: נראה $VC\leq_p SC$, ונסיק $SC\in NPH$ על סמך משפט 12.4

רעיון הבניה

העבודה שמחפשים k קב' רומזת שנרצה $k=k'$ ונרצה אישהו לזהות בין הקודקדים לבין הקבוצות $C_1,...C_t$ ובין E ל $[n]$

כיצד נזהה בין הצמתים לקבוצות? לכל קדקוד v נתאים לו את קב' הקשתות $E_v=\{e|v\in e\}$, כלומר הקשתות היוצאות מv . נסכם:

$$f\left(\langle G\rangle,k'\right)=\left(n=|E|,k=k',C_1,...,C_{t=|V|}\right) \text{ כאשר } C_i=E_{v_i}$$

נכונות הרדוקציה f:

פולינומית : סופרים קשתות, ואז עוברים על הצמתים ולכל צומת מחשבים את E_v

תקפות:

$\Leftarrow$

נניח $(\langle G\rangle,k')\in VC \Leftarrow$ קיים VC $U=\{V_{i1},...,V_{ik'}\}\Leftarrow$ קיים SC $I=\{i1,...,ik\}$ כאשר $k=k'$ (מהבניה) כך ש

$$\bigcup_{i\in I}C_i\overset{*}{=}\bigcup_{i\in I}E_{v_i}\overset{vc}{=}\!\!\rightarrow[|E|] \text{ מתרגם חזרה ל}$$

$*$ עד כדי מספור שמות

$\Rightarrow$

נניח $f(\langle G\rangle,k')\in SC \Leftarrow$ קיימת קב' $I\subseteq[n]$ $\{i_1,...,i_k\}=$ כך ש $\bigcup_{i\in I}C_i=[n]$ $\Leftarrow$ (מהבניה) קיימת קב' קדקודים $U=\{v_{i1},....,v_{ik'=k}\}$ המהווה VC עבור E (כי מבחירת I , היא מכסה את כל הקשתות , כי כל C_{i_j} היא למעשה $E_{v_{i_j}}$ -קב' הקשתות היצאות מ V_{i_j} מש"ל

0.6.6 משפט 12.7 $3SAT\in NPC$

הוכחה:

1. $3SAT\in NP$, ננחש השמה ϕ ונבדוק שהיא מספקת ונקבל את $\varphi(x)$ אם"ם ϕ אכן מספקת

2. נראה על ידי $SAT\leq_p 3SAT$ - נראה בשבוע הבא, נקבל ש $3SAT\in NPH$

הערה: זה שימושי לפשט את SAT ל $3SAT$ (כשפה NPC) כדי להקל על רדוקציות לפשות חדשות בגלל המבנה היותר פשוט של $3SAT$

רעיון הרידוקציה:

עבור קלט $\varphi(x_1,..,x_n)$ לרדוקציה $\varphi(x)=\bigwedge_{i=1}^{m}C_i$ נפלוט $\varphi'(x,y)$ מהצורה $\varphi(x,y)=\bigwedge_{i=1}^{m}C'_j$ כאשר C'_i יהיה פסוק $3CNF$.

שימו לב שלמרות ש C'_i הוא לא בהכרח פסוקית בודדת ל $\bigwedge_{i=1}^{m}C'_i$ יהיה מבנה של $3CNF$

לדוגמה, נגדיר ש:

$$C'_1=(x_1\vee\overline{x_3}\vee y_1)\wedge(x_{17}\vee\overline{y_1}\vee\overline{x_3})$$
$$C'_2=(x_2\vee x_3\vee x_7)\wedge(x_1\vee x_1\vee\overline{x_8})$$
$$than:$$
$$C'_{1'}\wedge C'_2=(x_1\vee\overline{x_3}\vee y_1)\wedge...\wedge(x_1\vee\overline{x_3}\vee y_1)$$

כיצד נבצע את ההתאמה בין C_i ל C'_i נחלק למקרים:

1. $C_i = l_1 \vee l_2 \vee l_3$ ⇐ 3 ליטרלים ניקח $C'_1 = C_i$
2. $C_i = l_1 \vee l_2$ ⇐ 2 ליטרלים , ניקח $C'_i = (l_1 \vee l_2 \vee l_2)$
3. $C_i = l_i$ ⇐ 1 ליטרלים , נכפיל כמו ב2
4. $C_i = \bigvee\limits_{j=1}^{t} l_{i,j}$ כאשר $t \geq u$. נתאים

$$C'_i = (l_{i_1} \vee l_{i_2} \vee y_{i_1}) \wedge (\overline{y_{i_1}} \vee l_{i_2} \vee y_{i_2}) \wedge (\overline{y_{i_2}} \vee l_{i_4} \vee y_{i_3}) \wedge .... \wedge \wedge (\overline{y_{i_{t-3}}} \vee l_{i_{t-1}} \vee y_{i_t})$$

בראשון והאחרון יש שתי משתנים מקוריים ומשתנה 1 חדש

באמצעים יש את המשתנה שהוספנו בשלילה , ומשתנה חדש נוסף

לדוגמה:

$$C_{14} = x_1 \vee \overline{x_{14}} \vee x_{12} \vee \overline{x_3 \vee} x_2$$

הופך ל:

$$C'_{14} = (x_1 \vee \overline{x_{14}} \vee y_{14,1}) \wedge (\overline{y_{14,1}} \vee x_{12} \vee y_{14,2}) \wedge (\overline{y_{14,2}} \vee \overline{x_3} \vee x_2)$$

נשים לב ש C'_i לא שקול לוגית ל C_i (אפילו סט המשתנים עליו הם מוגדרים שונה - אם נסתכל על C_i כמוגדר מעל (x,y) עדיין לא תהיה שקילות לוגית)

נתוח $f(\varphi(X))$ **:**

פולינומית

כל פסוקית הופכת לפסוקית שאורכו פי 3 מהפסוקית המקורית (מבחינת מס' ליטרלים) וגם קל לחשב את C'_i . בערך לינארי ב$|\varphi(x))|$על מכונת RAM (כולל הקצאת ה $y_{i,j}$ ים)

תקפות

⇐

נניח ש $\varphi(x_1,..,x_n) \in SAT$ ותהי $\phi(x)$ השמה מספקת עבור φ , נבנה השמה $\phi'(x,y)$ המספקת את φ'

- נגדיר $\phi'(x) = \phi(x)$ ונקוה שנצליח להשלים השמה ל yים שסה"כ ϕ' תספק את φ' (אכן נצליח)
- לכל C'_i , נשלים את ההשמה לϕ' ל $y_{i,j}$ כך ש C'_i תסתפק. אם נצליח, אז גם $\varphi = \bigwedge C'_i$ יסתק ע"י ϕ' . נחלק למקרים:

1. C'_i לא מכיל $y_{i'j}$ים במקרה זה היא שווה ל C_i . כיון ש $\phi'(x) = \phi(x)$, ו ϕ מספקת את φ' אז ϕ מספקת גם את C_i כי $\varphi = \bigwedge C_i$) ולכן גם את C'_i
2. אם $C_{i'}$ מכיל $y_{i,j}$ ים : נשים לב שקיים ליטרל $l_{i,j} = x_{r_i}$ המסתפק ע"י ϕ בגלל השמה של ל x , כי ϕ מספקת כל פסוקית C_i , וכדי שC_i תסתפק לפחות ליטרל אחד שלה צריך להסתפק. נחלק למקרים:

(א) $l_{i,j}$ אינו שייך לפסוקיות ה"קצה" ב C'_i כלומר

$$C'_i = ... \left(\overline{y_{i,j-3}} \vee l_{ij-1} \vee \underbrace{y_{i,j-2}}_{T}\right) \wedge \left(\underbrace{\overline{y_{i,j-2}}}_{F} \vee \underbrace{l_{ij}}_{T} \vee \underbrace{y_{i,j-1}}_{F}\right) \wedge \left(\underbrace{\overline{y_{i,j-1}}}_{T} \vee l_{ij+1} \vee y_{i,j}\right)$$

$l_{i,j}$ הוא T (כי ההשמה מספקת) נקבע $y_{i,j-1} = \overline{y_{i,j-2}} = F$, ואז ה"גל" יתפשט

כלומר ה"גל של Tים יתפשט שמאלה וימינה ויאפשר לקבוע את $y_{i,j}$ ים כך שכל הפסוקיות ב C'_i יסתפקו.

⇒ נניח ש $\varphi'(x,y) \in SAT$ ונוכיח ש $\varphi(x) \in SAT$ - שיעור הבא