אוטומט סופי דטרמיניסטי DFA $M=(Q,\Sigma,\delta,q_0,F)$ **:**

סגירות תחת משלים: אם $L\in DFA$ אז גם $\overline{L}\in DFA$.

הוכחה: $M=(Q,\Sigma,\delta,q_0,F)$ כך ש- $L(M)\in DFA$ נבנה $M'=(Q',\Sigma',\delta',q_0',F')$ כך: $Q'=Q$ $\Sigma'=\Sigma$, $\delta'=\delta$, $q_0'=q_0$,

$F'=Q\setminus F$ $L(M')=\{w\in\Sigma^*:(\delta')^*(q_0',w)\in F'\}=\{w\in\Sigma^*:\delta^*(q_0,w)\in Q\setminus F\}=\{w\in\Sigma^*:w\notin L(M)\}=\overline{L(M)}$

סגירות תחת חיתוך: אם $L_1,L_2\in DFA$ אז גם $L_1\cap L_2\in DFA$.

$$L_1=L(M_1),L_2=L(M_2)\Rightarrow M=(Q,\Sigma,\delta,s,F):Q=Q_1\times Q_2,\Sigma=\Sigma_1=\Sigma_2,s=(s_1,s_2)$$

$$F=F_1\times F_2=\{(q_1,q_2):q_1\in F_1,q_2\in F_2\},\delta((q_1,q_2),a)=(\delta_1(q_1,a),\delta_2(q_2,a))$$

$$L(M)=\{w\in\Sigma^*:\delta^*(s,w)\in F\}=\{w\in\Sigma^*:\delta^*((s_1,s_2),w)\in F_1\times F_2\}=\{w\in\Sigma^*:(\delta_1^*(s_1,w),\delta_2^*(s_2,w))\in F_1\times F_2\}=$$

$$\{w\in\Sigma^*:\delta_1^*(s_1,w)\in F_1\wedge\delta_2^*(s_2,w)\in F_2\}=\{w\in\Sigma^*:\delta_1^*(s_1,w)\in F_1\}\cap\{w\in\Sigma^*:\delta_2^*(s_2,w)\in F_2\}=L(M_1)\cap L(M_2)$$

סגירות תחת איחוד: אותו דבר כמו חיתוך בשינוי- $F=\{(q_1,q_2):q_1\in F_1\vee q_2\in F_2\}$.

סגירות תחת חיסור: אותו דבר כמו חיתוך בשינוי- $F=\{(q_1,q_2):q_1\in F_1\vee q_2\notin F_2\}$.

אוטומט סופי לא דטרמיניסטי NFA $M=(Q,\Sigma,\Delta,q_0,F)$ **:**

NFA=DFA=REG

NFA/DFA סגורות תחת שרשור וחזקה: מכיוון שלכל אסל״ד ניתן להניח כי יש לו מצב מקבל יחיד נוכל לשרשר בעזרת מעבר אפסילון למצב ההתחלתי של האוטומט הבא וכך הלאה.

שרשור: אם $L_1,L_2\in DFA$ אז גם $L_1\circ L_2\in DFA$.

$$L_1=L(M_1),L_2=L(M_2)\Rightarrow M=(Q,\Sigma,\delta,s,F):Q=Q_1\cup Q_2,\Sigma=\Sigma_1=\Sigma_2,q_0=q_1,\Delta=\delta_1\cup\delta_2\cup(F_1\times\{\varepsilon\}\times\{q_2\},F=F_2$$

משפט: לכל שפה רגולרית יש אוטומט סופי לא דטרמיניסטי המקבל אותה.

למת הניפוח לשפות רגולריות: לכל שפה רגולרית L קיים מספר n_0 כך שלכל מילה ב- L $w\in L$ כך ש- $|w|\ge n_0$ קיים פירוק

$w=x\circ y\circ z$ עבור $x,y,z\in\Sigma^*$ עם התכונות הבאות: $1.\ \varepsilon\neq y\ \ 2.\ |x\circ y|\le n_0\ \ 3.\ x\circ y^k\circ z\in L\ \ \forall k$

דוגמא לשימוש בלמה:

השפה $L=\{1^{n_1}01^{n_2}01^{n_1+n_2}\}$ אינה רגולרית.

1) נניח בשלילה ש- L רגולרית, אז קיים n_0 כך שמתקיימים תנאי הלמה.
2) נסתכל על המילה $w=1^{n_0}01^{n_0}01^{2n_0}$, ברור כי היא שייכת לשפה L.
3) מכיוון שעפ״י תנאי הלמה $|xy|\le n_0$, מתקיים ש- $y=1^t$ כך ש- $1\le t\le n_0$ בגלל ש- $y\neq\varepsilon$.
4) נבחר $k=n_0+1$ אזי $u=xy^{n_0+1}z$.
5) $|y^{n_0+1}|\ge n_0+1$ אבל $(n_0+1)+n_0\neq 2n_0$ ולכן u לא שייכת לשפה.

דוגמאות לשפות לא רגולריות:

$$L=\{1^P:P\ \text{is a prime number}\},\ L=\{a^nb^n:n\ge 0\},\ \ L=\{w\in\Sigma^*:\text{w has an even num of a and b}\},L=\{1^{n^2}:n\in N\}$$

משפט מייהיל-נרוד: עבור שפה L מעל א״ב סופי Σ מגדירים את שני יחסי השקילות על Σ^* :

1. $w_1\sim_L w_2$ אם קורה אחד משני מקרים: $w_1,w_2\in L$ או $w_1,w_2\notin L$
2. $w_1\equiv_L w_2$ אם לכל $u\in\Sigma^*$ $w_1u\sim_L w_2u$.

נגדיר לכל $a\in A$ את מחלקת השקילות שלו: $[a]_R=\{b:(a,b)\in R\}$, ואת קבוצת המנה: $A/R=\{[a]_R:a\in R\}$

עבור L רגולרית $\#_L$ מודד את מספר המצבים באס״ד המינימלי המקבל את L. L רגולרית $\Leftrightarrow$ $\#_L$ מספר טבעי סופי.

אוטומט מחסנית (PDA) לא דטרמיניסטי $M=(Q,\Sigma,\Gamma,\Delta,q_0,F)$ **:**

פונקציה: $\Delta\subseteq(Q\times\Sigma_\varepsilon\times\Gamma_\varepsilon)\times(Q\times\Gamma_\varepsilon)$ קונפיגורציה התחלתית: (q_0,w,ε) , קונפיגורציה סופית: $(q_f,\varepsilon,\varepsilon)$

יחס המעבר: $(q,\sigma x,\gamma_1 y)\underset{M}{\vdash}(q',x,\gamma_2 y)$, $L(M)=\{w\in\Sigma^*:(q_0,w,\varepsilon)\overset{*}{\underset{M}{\vdash}}(q_f,\varepsilon,\varepsilon)\}$

דוגמאות לשפות המתקבלות ע״י אוטומט מחסנית:

$$L=\{ww^R:w\in\Sigma^*\},\ L=\{a^nb^n:n\ge 0\},\ \ L=\{w\in\Sigma^*:\text{w has an even num of a and b}\}$$

דקדוקים חסרי הקשר $G=(V,\Sigma,R,S)$ **CFL:**

דקדוק שיש לו יותר מעץ גזירה אחד נקרא רב-משמעי, כל דקדוק רב משמעי ניתן להפוך לחד-משמעי ע״י החלפת נונטרמינאלים בשמות אחרים.

דוגמא: הדקדוק: $E\to E+E\,|\,E\times E\,|\,(E)\,|\,a\,|\,b$ הוא רב משמעי.

הצורה החד-משמעית שלו: $E\to E+T\,|\,T\ \ ,\ \ T\to T\times F\,|\,F\ \ ,\ \ F\to a\,|\,b\,|\,(E)$

משפט: **PDA=CFL** שפות אלו נקראות **שפות חסרות הקשר**. (הוכחה בעזרת אוטומט מחסנית מוכלל):

$$CFL\subseteq PDA\to GPDA\subseteq PDA, PDA\subseteq GPDA, PDA\subseteq CFL$$

הוכחה: נתון דקדוק נבנה את האוטומט כך: מהמצב ההתחלתי יהיה מעבר שידחוף למחסנית את סמל ההתחלה S ויעבור למצב q_1 . במצב זה באופן לא דטר׳ ניתן לבצע שני סוגים של מעברים: צעד גזירה: הוצאת נונטרמינל מהמחסנית, לא לקרוא כלום מהקלט ולדחוף למחסנית על פי כלל הגזירה של הנונטרמינל. צעד קריאה: אם בראש המחסנית יש a אפשר לקרוא מהקלט a ולהוציא אותו מהמחסנית.

המצב q_1 הוא מצב מקבל. צ״ל: $L(G)=L(M)$ נעזר בטענת העזר: $(q_0,w,\varepsilon)\overset{*}{\underset{M}{\vdash}}(q_1,\varepsilon,v)$ אז $S\overset{*}{\underset{G}{\Rightarrow}}wv$ באינד׳ על מס׳ צעדי האוטומט. הראינו $CFL\subseteq PDA$.

$PDA\subseteq CFL$: בהינתן אוטומט מחסנית נבנה דקדוק. בכל מעבר באוטומט יש או push או pop אך לא שניהם. נגדיר חוקים שיתארו את המעברים באוטומט. הנונטרמינאלים יראו כך: $A_{p,q}$.

למת הניפוח לשפות ח"ה: לכל שפה ח"ה L קיים מספר n_0 כך שלכל מילה ב- L $w \in L$ כך ש- $|w| \ge n_0$ קיים פירוק $w = u \circ v \circ x \circ y \circ z$ עבור $u,v,x,y,z \in \Sigma^*$ עם התכונות הבאות: $1.\ \varepsilon \ne v \circ y\ \ 2.\ |v \circ x \circ y| \le n_0\ \ 3.\ u \circ v^k \circ x \circ y^k \circ z \in L\ \ \forall k$

דוגמא לשפות שאינן ח"ה: $L = \{a^n b^n c^n : n \ge 0\}, L = \{ww : w \in \Sigma^*\}, L = \{0^n \# 0^{2n} \# 0^{3n} : n \ge 0\}, L = \{a^i b^j c^k : i < j < k\}$

שפות ח"ה אינן סגורות תחת חיתוך ומשלים: $L_2 = \{a^k b^n c^n\}$ $L_1 = \{a^n b^n c^m\}$ ח"ה אך $L_1 \cap L_2 = \{a^n b^n c^n\}$ לא.

$L_1 = \{u = ww^R : w \in \Sigma^*\}$ ח"ה, $L_2 = \{u = ww : w \in \Sigma^*\}$ לא ח"ה, $\overline{L_1} = \{u = w_1 w_2 : w_2 \ne w_1^R \wedge |w_2| = |w_1|\}$ ח"ה אבל $\overline{L_2} = \{u = w_1 w_2 : w_2 \ne w_1 \wedge |w_2| = |w_1|\}$ לא.

מכונות טיורינג דטרמיניסטית ($M = (Q, \Sigma, \Gamma, \delta, q_0, q_{accept}, q_{reject})$ **:**

פונקצית המעבר: $\delta : (Q \times \Gamma) \times (Q \times \Gamma \times \{R, L\})$, קונפיגורציה: (w_1, q, w_2) .

במכונה לא דטרמיניסטית השפה מוכרעת רק אם כל המסלולים עצרו וקיבלו או דחו ומקבלת אם אחד המסלולים קיבל.

משפט: מ"ט דטרמיניסטית יכולה לסמלץ מ"ט לא דטרמיניסטית.

מדפסת: מכונה שהסרט שלה מגיע ריק וניתן לרשום עליו משמאל לימין בלבד ולא ניתן לקרוא ממנו. מכונות אלו נקראות מונים, נאמר שמכונה M מונה את שפה L אם לכל מילה $w \in L$ באיזשהו שלב M כותבת אותה לסרט הפלט ואלה כל המילים שהיא כותבת לפלט. למכונה כזאת אין קלט, יש לה סרט עבודה שגם הוא מתחיל ריק. שפה כזאת נקראת "ניתנת למניה רקורסיבית/אפקטיבית".

משפט: L ניתנת למניה אס"ם L ניתנת לקבלה.

מ"ט אוניברסאלית:

מקבלת כקלט מ"ט M וקלט w ומסמלצת את פעולת M על w.

הצורה הנורמלית של חומסקי:

דקדוק ח"ה $G = (V, \Sigma, R, S)$ הוא בצורה הנורמלית של חומסקי אס"ם $R \subseteq (V \setminus \Sigma) \times (V \setminus \Sigma)^2 \cup (V \setminus \Sigma) \times \Sigma \cup \{(S, \varepsilon)\}$

משפט: יהי G דקדוק, אזי קיים G' כך ש- G' בצורה הנורמלית של חומסקי והם מתארים את אותה שפה.

התהליך: נוסיף משתנה התחלתי חדש וחוק חדש $S' \to S$, נטפל בחוקים מהצורה $A \to \varepsilon$: כל עוד יש חוקים מסוג זה ו- $A \ne S'$ נוריד את החוק הזה ולכל מופע של המשתנה A בצד ימין של חוק כלשהו נוסיף חוק חדש ובו מופע של A מוחלף ב- ε , אבל לא נוסיף חוקים שכבר מחקנו בעבר. נטפל בחוקים מהצורה $A \to B$, כל עוד יש חוק מסוג זה נמחק אותו וכל חוק מהצורה $B \to u, u \in V^*$ נוסיף את החוק $A \to u$, אלא אם החוק $A \to u$ הוא חוק מהצורה $A \to C$ וכבר הורדנו אותו בעבר. אם ישנו חוק מהצורה $A \to u_1 u_2 ... u_k$ נחליפו בחוקים: $A \to u_1 A_i, A_i \to u_{i-1} A_{i-1}$, אם יש חוק מהצורה $A \to u_i u_j$ וגם u_i או u_j הם טרמינלים אז נוסיף חוק חדש $U_i \to u_i$ או $U_j \to u_j$ ונשכתב את החוק $A \to u_i u_j$ ע"י החלפת אחד מהם בנונטרמינל החדש.

כריעות:

שפות הניתנות לקבלה:

* $HALT = \{< M >, w : M \text{ stops on w}\}$

שפות לא כריעות:

* $L = \{< M >:$ M עוצרת על הקלט הריק$\}$ - ברדוקציה מ- HALT - R על קלט <M,w> בונה מ"ט T אשר על קלט x אם $x \ne \varepsilon$ דוחה אחרת מסמלצת את M על w ודוחה. נניח $< M, w > \in HALT$ אז T על הקלט ε (עפ"י בניה) תעצור מכיוון שהסימלוץ של M יעצור. נניח $< M, w > \notin HALT$ אזי M לא עוצרת על w, לכן הסימלוץ של M על ε לא יעצור ולכן $< T > \notin L$.
* $ACCEPT = \{< M >, w : M \text{ accepts w}\}$ - הנחה בשלילה ש- ACCEPT כריעה, קיים M_{accept} , בנית D על קלט <M> , נריץ את M_{accept} על קלט <M>,<M>, אם קיבלה D תדחה, אחרת תקבל.

D מקבלת את <D> $\Leftarrow$ $M_{accept}(< D >, < D >) = reject$ $\Leftarrow$ D לא מקבלת את <D> $\Leftarrow$ סתירה.

D לא מקבלת את <D> $\Leftarrow$ $M_{accept}(< D >, < D >) = accept$ $\Leftarrow$ D מקבלת את <D> $\Leftarrow$ סתירה.

* $HALT = \{< M >, w : M \text{ stops on w}\}$ - הנחה בשלילה, קיים M_{halt} , ולכן קיימת M_{accept} בסתירה לכך ש- ACCEPT לא כריעה.
* $EMPTY = \{< M >: L(M) = \phi\}$ - ברדוקציה מ- ACCEPT , הנחה בשלילה, קיים M_{empty} ,מכונת הרדוקציה על קלט <M>,w תייצר M' שעל קלט x אם $x \ne w$ תדחה, אחרת תריץ את w על M ותנהג כמוה. מקרה א': $< M >, w \in ACCEPT$ אז $w \in L(M')$, כלומר M מקבלת את w ולכן $L(M') \ne \phi$. מקרה ב': $< M >, w \notin ACCEPT$ בהינתן $x \ne w$ M' תדחה, בהנתן x=w M לא מקבלת וכך גם M' ולכן $L(M') = \phi$.
* $EQUAL = \{< M_1 >, < M_2 >: L(M_1) = L(M_2)\}$ - רדוקציה מ- EMPTY , M_2 מקבלת את השפה הריקה, $< M > = < M_1 >$, מכונה שעל קלט <M> מוציאה $< M_1 >, < M_2 >$. אם $< M > \in EMPTY$ אז $L(M) = \phi$ ובפרט $L(M_1) = L(M_2)$ ולכן $< M_1 >, < M_2 > \in EQUAL$. אם $< M > \notin EMPTY$ אז $L(M) \ne \phi$ ולכן $L(M_1) \ne L(M_2)$ ולכן $< M_1 >, < M_2 > \notin EQUAL$ לכן EQUAL לא כריעה, אחרת היה אפשר להכריע את EMPTY.

שפות לא ניתנות לקבלה:

* $\overline{ACCEPT} = \{< M >, w : M \text{ dosent accepts w}\}$

משפט: לכל שפה L , אם L ניתנת לקבלה וגם $\overline{L}$ ניתנת לקבלה אזי L כריעה.

משפט RICE:

TM קבוצת כל המ"ט, נסתכל בשפות $P \subseteq TM$ למשל: $P = \{<M>: L(M) \text{ is regular}\}$, נאמר שתכונה P היא לא טריוויאלית אם $P \neq TM \wedge P \neq \phi$. נאמר ש- P היא תכונה של שפות של מ"ט אם לכל $<M_1>, <M_2>$ מתקיים שאם $L(M_1) = L(M_2)$ אז או ש- $<M_1>, <M_2> \in P$ או ש- $<M_1>, <M_2> \notin P$. לכל תכונה לא טריוויאלית P, P לא כריעה.

הוכחת המשפט: נגדיר M_{loop} שהיא מ"ט שעל כל קלט נכנסת ללולאה אינסופית. נראה כי $<M_{loop}> \in P$ וגם כי $<M_{loop}> \notin P$.

P לא טריוויאלית $\Leftarrow$ יש מכונה ששייכת ל- P נקרא לה $M_{other} \in P$ וידוע כי $\phi = L(M_{loop}) \neq L(M_{other})$, ברדוקציה מ- HALT:

נבנה רדוקציה כך ש: $M \Rightarrow L(M') = L(M_{other})$ עוצרת על w, $M \Rightarrow L(M') = L(M_{loop}) = \phi$ לא עוצרת על w.

בהינתן <M>,w נבנה קידוד של מ"ט M' כך: M' בהינתן קלט x תרשום אותו על סרט כלשהו ותרשום על סרט העבודה שלה את <M>,w M' תסמלץ את M על w (ויתכן שלא תעצור). אם הסימולציה תעצור אז נריץ את M_{other} על x וננהג כמוה. נראה שלרדוקציה יש את התכונות שאנו רוצים: אם M עוצרת על w אז כאשר M' מקבלת קלט x אז M' מבצעת עליו את ההרצה של M_{other} על x ובפרט $L(M') = L(M_{other})$. אם M לא עוצרת על w אז לכל קלט x M' איננה עוצרת על x ובפרט $L(M') = L(M_{loop}) = \phi$.

נגדיר תכונה חדשה $\overline{P} = TM \setminus P$ אז $\overline{P}$ לא טריוויאלית כי $\phi \neq P \neq TM$ ולכן $\phi \neq \overline{P} \neq TM$ ו- $\overline{P}$ תכונה של מ"ט. עבור $\overline{P}$ מתקיים $\overline{P} \notin P$ ולכן לפי ההוכחה $\overline{P}$ לא כריעה. ידוע לנו שאם L כריעה אז גם $\overline{L}$ כריעה. מכך ש- $\overline{P}$ לא כריעה אפשר להסיק ש- P לא כריעה.

דוגמא לשימוש במשפט RICE:

נסתכל על השפה: $L = \{<M>: L(M) \neq \Sigma^*\}$ נוכיח על ידי משפט רייס כי היא אינה כריעה: בשביל להשתמש במשפט רייס נראה ש- L אינה טריוויאלית וש- L היא תכונה של שפות של מ"ט: קיימת מ"ט M_1 כך ש- $L(M_1) = \phi$ כלומר $<M_1> \in L \Leftarrow L \neq \phi$. מצד שני קיימת מ"ט M_2 כך ש- $L(M_2) = \Sigma^*$ כלומר $<M_2> \notin L \Leftarrow L \neq TM$ - השפה אינה טריוויאלית.

יהיו מ"ט M_1, M_2 כך ש- $L(M_1) = L(M_2)$ אם $<M_1> \in L \Leftarrow L(M_1) \neq \Sigma^*$ כלומר גם $L(M_2) \neq \Sigma^*$ ולכן $<M_2> \in L$.

אם $<M_1> \notin L$ אזי $L(M_1) = \Sigma^*$ כלומר $L(M_2) = \Sigma^*$ ולכן $<M_2> \notin L$.

משפט: כל שפה ח"ה היא כריעה.

משפט: השפה $ALL_{CFG} = \{<G>: L(G) = \Sigma^*\}$ לא כריעה. הוכחה ברדוקציה מ- $\overline{ACCEPT}$, הא"ב של הדקדוק יכיל את הא"ב של המכונה ובנוסף את כל המצבים של M ועוד סימן מיוחד #. ניצור דקדוק G שיגזור את כל המילים מהצורה $\#c_1\#c_2\#c_3\#...\#c_n\#$ (קונפיגורציות של M) אבל הדקדוק לא יוכל לגזור רצף כזה שמתחיל בקונפיגורציה התחלתית על w ומסתיים בקונפיגורציה מסיימת.

במקום דקדוק נבנה אוטומט מחסנית, נתאר את האוטומט בצורה כללית: יקבל w, יקבל רק בתנאי שאחד התנאים הבאים מתקיים:
1. המילה אינה רצף תקין של קונפיגורציות. 2. הקונפיגורציה הראשונה אינה התחלתית. 3. הקונפיגורציה האחרונה אינה מקבלת.

4. קיים i כך ש- $c_i \not\vdash_M c_{i+1}$ (האוטומט יבדוק באופן לא דטרמיניסטי זוגות של קונפיגורציות ויחליט אם הן תקינות, על מנת שהוא יוכל לעשות זאת הקלט צריך לבוא בצורה הבאה: $\#c_1\#c_2{}^R\#c_3\#...{}^R\#c_n\#$.

מורכבות חישובית:

עבור מ"ט M וקלט x נגדיר: $TIME(M, x) = \{number \text{ of steps of M on x}\}$ כך ש- M עוצרת על x. נאמר שמ"ט רצה בזמן t(n) אם לכל n>0 כך ש- $|x| = n$ מתקיים $TIME(M, x) \leq t(n)$.

משפט: כל מ"ט חד סרטית המכריעה את L רצה בזמן t(n) כך ש $t(n) = \Omega(n^2)$ (חסם תחתון).

משפט: ניתן לסמלץ מ"ט k סרטית שרצה בזמן t(n) ע"י מ"ט חד סרטית שרצה בזמן $O(t(n^2))$.

מחלקת השפות הניתנות לחישוב ביעילות: $P = TIME(n) \cup TIME(n^2) \cup TIME(n^3) \cup ... \cup TIME(n^l) \cup .... = \bigcup_{k=1}^{\infty} TIME(n^k)$, P היא מחלקת כל השפות שניתנות לחישוב בזמן פולינומיאלי באורך הקלט.

דוגמאות לשפות ב- P: $PATH = \{(G, s, t): s-t \text{ is a path on G}\}$ קיים אלג' יעיל הפותר את השפה (BFS).

מכונות טיורינג לא דטרמיניסטיות לא נכללות בתזה של צ'רץ' טיורינג ביחס לסיבוכיות זמן.

עבור מ"ט לא דטרמיניסטיות M נאמר ש- M רצה בזמן t(n) אם: לכל x, $|x| = n$, ולכל מסלול חישוב על x אורך המסלול הוא לכל היותר t(n). נגדיר מחלקה מקבילה ל- P ביחס למכונות לא דטרמיניסטיות:

$NTIME(t(n)) = \{L$: קיימת מ"ט לא דטרמיניסטית שרצה בזמן O(t(n)) ומכריעה את L$\}$ ואת המחלקה: $NP = \bigcup_{k=1}^{\infty} NTIME(n^k)$

שהיא המחלקה של שפות שניתנות להכרעה בזמן פולינומי ע"י מ"ט לא דטרמיניסטית.

משפט: לכל פונקציה t(n) $NTIME(t(n)) \subseteq TIME(2^{o(t(n))})$ לכל מ"ט לא דטר' שמכריעה שפה L בזמן O(t(n)) קיים קבוע c (שתלוי בא"ב ובמספר המצבים) כך שיש מ"ט דטר' שרצה בזמן $2^{c \cdot t(n)}$.

הוכחה: נזכר בהוכחה שכל מ"ט לא דטר' יכולה להיות מוכרעת ע"י מ"ט דטר' (עם העץ ו-3 הסרטים עם הניחושים), מס' הקדקודים בעץ $\leq O(b^{t(n)}) = O((2^{\log b})^{t(n)}) = 2^{o(t(n))}$.

הגדרה שונה למחלקה NP: נאמר כי לשפה L יש מוודא פולינומי אם קיים c>1 ומ"ט דטר' V שרצה בזמן פולינומי כך ש:

$L = \{x: \exists y, |y| \leq |x|^c, V(x, y) = accept\}$.

משפט: $L \in NP \Leftrightarrow$ ל- L יש מוודא פולינומי.

דוגמאות לשפות ב- NP:

$HAM\_PATH = \{(G, s, t): s-t \text{ is a hamiltonian path on G}\}$ (לא ברור עם היא ב- P)

$COMPOSITE = \{<M>:$ M פריק$\}$ (m פריק אם"ם קיימים מספרים $x, y \neq 1$ כך ש- $x \cdot y = m$).

$SAT = \{\varphi: \varphi \text{ is satisfied}\}$, $CLIQUE = \{<G, k>:$ G גרף, k מספר, בגרף יש קליקה בגודל k$\}$

$SUBSET\_SUM = \{<s, t>:$ s קבוצת מס' טבעיים, t מס' טבעי וקיימת תת קבוצה של s שסכומה t$\}$

משפט cook-levin: $SAT \in P \Leftrightarrow NP = P$ כלומר SAT וגם 3-SAT הן NP-COMPLETE אחרת NP היא שווה ל- P.

רדוקציות פולינומיאליות:

הגדרה: יהיו A,B שפות (מעל אותו א"ב) נאמר שיש רדוקציה פולינומיאלית מ- A ל- B $(A \le_p B)$ אם קיימת פונקציה f שניתנת לחישוב בזמן פולינומי עם התכונה הבאה: $x \in A \Leftrightarrow f(x) \in B$.

משפט: $A \le_p B$ ו- $B \in P$ אז $A \in P$. נניח $A \le_p B$ ו- $B \in P$ כלומר יש פונק' f הניתנת לחישוב ע"י מ"ט דטר' פולינומיאלית R כך ש- $x \in A \Leftrightarrow f(x) \in B$ נראה מ"ט עבור A: על קלט x נריץ את R על x ונקבל y= f(x) נריץ את מ"ט הדטר' של B על y. אלגוריתם זה מכריע את A והוא פולינומי.

דוגמאות:

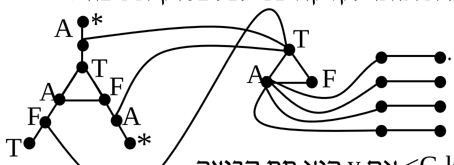
* $3-SAT \le_p CLIQUE$: $\varphi \to <G,k>$

בהינתן נוסחא φ בצורת 3-CNF נבנה גרף: לכל ליטרל (3m) יהיה קדקוד משלו, לכל שני קדקודים בגרף נחבר אותם אלא אם מתקיים: הליטרלים באותה פסוקית, לא מחברים ליטרל ושלילתו. המספר k יהיה m (מספר הפסוקיות).

NP שלמות:

עבור שפה $B \in NP$ נאמר שהיא NP שלמה אם לכל שפה $A \in NP$ מתקיים: $A \le_p B$.

* $CIRCUIT-SAT = \{C : f_c(y) = 1$ -C מעגל וקיים y כך ש $\}$ היא NP שלמה.
* 3-SAT היא NP שלמה.
* 3-COLOR היא NP שלמה. נראה רדוקציה מ- 3-SAT. בהינתן נוסחת 3-CNF נבנה גרף ע"י יצירת משולש F,T,A ובנוסף לכל משתנה בנוסחה יהיו שני קדקודים בקשת(המשתנה ושלילתו). לכל ליטרל תהיה קשת המחברת אותו לקדקוד A לכל פסוקית ניצור: כל צביעה תקינה תגדיר ערכים למשתנים.



* $VC = VERTEX\_COVER = \{<G,k>:$ ב- G יש כיסוי קדקודים בגודל k$\}$ היא NP שלמה.

הוכחה: $INDEPENDENT\_SET \le_p VC$, בהינתן קלט <G,k> יהי n מס' הקדקודים ב- G רשום <G,n-k> על הסרט ועצור. מכיוון שקבוצת קדקודים ב"ת היא VC מתקיים ש- $<G,k> \in IS \Leftrightarrow <G,n-k> \in VC$. נראה כי $VC \in NP$ המוודא הפולינומי V: על קלט <G,k,y> אם y היא תת קבוצה של קדקודים בגודל k המהווה VC ל- G אזי קבל אחרת דחה.

* HAM_PATH היא NP שלמה: $3-SAT \le_p HAM\_PATH$ הוכחה עם הגאג'טים.
* $SSUM = SUBSET\_SUM = \{<S,T>: S = \{x_1,...,x_n\}, x_i \in N, \exists S' \subseteq S : \sum_I x_I = T\}$ היא NP שלמה. מוודא פולינומי: על קלט $<S,T,S'>$ יבדוק האם $S' \subseteq S$ וגם מקיים את הסכום – אם כן יקבל אחרת ידחה. ניתן להראות רדוקציה $3-SAT \le_p SSUM$.

רדוקציות:

הגדרה: יהיו A,B שפות (מעל אותו א"ב) נאמר שיש רדוקציה מ- A ל- B $(A \le_m B)$ אם קיימת מ"ט R שלכל x, R(x) עוצרת ופולטת y כך ש- $x \in A \Leftrightarrow y \in B$.

דוגמאות:

נגדיר: $L_1 = \{<M>: L(M) \ne \Sigma^*\}$ נראה כי $\overline{ACCEPT} \le_m L_1$:

R על קלט <M,w>: אם <M,w> אינו קידוד חוקי של מ"ט ומילה אזי רשום על הסרט קידוד <T> של מ"ט T כך ש- $L(T) = \phi$. אחרת נבנה מ"ט T אשר על קלט x: מסמלצת את M על w, אם M מקבלת אז accept אחרת reject. כתוב את T על הסרט ועצור.

נגדיר: $L_2 = \{<M>: M \text{ on } \varepsilon \text{ writes a}\}$ נראה כי $ACCEPT \le_m L_2$:

R על קלט <M,w>: נבנה מ"ט T אשר על קלט x: אם $x = \varepsilon$ אזי סמלץ את M על w. אם M מקבלת את w אזי כתוב a על הסרט וקבל. אחרת קבל. כתוב את T על הסרט ועצור.

נגדיר: $L_3 = \{<M>: M \text{ always stops}\}$ נראה כי $ACCEPT \le_m L_3$:

R על קלט <M,w>: נבנה מ"ט T אשר על קלט x: סמלץ את M על w, אם M מקבלת את w אז קבל, אחרת כנס ללולאה אינסופית. כתוב את T לסרט ועצור.

היררכיה של זמן:

פונקציה t(n) נקראת פונקצית זמן תקינה אם $t(n) \ge n$ ויש מ"ט שעל קלט 1^n רצה בזמן $O(t(n))$ ומוציאה קידוד בינארי של t(n).

משפט ההירככיה לזמן: לכל פונקצית זמן תקינה t(n) $TIME(t(n)) \subset TIME(t(n^2))$ כלומר קיימת $L \in TIME(t(n^2))$ כך ש- $L \notin TIME(t(n)))$.

$$EXP = \{\bigcup_{k=1}^{\infty} TIME(2^{(n^k)})\}, CO\_NP = \{L : \overline{L} \in NP\}, \quad NP \subset EXP, CO\_NP \subset EXP, P \subset EXP.$$

סיבוכיות זיכרון:

עבור מ"ט M וקלט x נגדיר: $SPACE(M,x) =$ {מה המיקום הכי ימני של הראש הקורא של אחד הסרטים תוך כדי ריצה על x}.

נאמר שמ"ט רצה בזיכרון S(n) אם לכל M x רצה על x (באורך n) $SPACE(M,x) = O(S(n))$.

$SPACE(S(n)) = \{L :$ יש מ"ט דטרמיניסטית שרצה בזיכרון O(S(n)) ומכריעה את L}

$NSPACE(S(n)) = \{L :$ יש מ"ט לא דטרמיניסטית שרצה בזיכרון O(S(n)) ומכריעה את L}

טענה: למ"ט דטרמיניסטית M שרצה בזיכרון S(n) יש לכל היותר $2^{O(S(n))}$ קונפיגורציות שונות.

הוכחה: $(|\Sigma|^{S(n)})^3 \cdot |Q| \cdot (S(n))^3 \le (2^{\log|\Sigma|})^{3S(n)} \cdot O(1) \cdot 2^{S(n)} \le 2^{O(S(n))}$ (בחזקת 3 בגלל 3 סרטים)

משפט: $SPACE(S(n)) \subseteq TIME(2^{O(S(n))})$

הוכחה: תהי מ"ט המכריעה שפה $L \in SPACE(S(n))$ נשים לב שבפרט M עוצרת על כל קלט. נניח בשלילה ש- M על קלט מסוים x רצה יותר זמן ממספר הקונפיגורציות שלה, מעקרון "שובך השפנים" M עוברת באותה קונפיגורציה פעמיים אבל אז M איננה עוצרת על x, סתירה.

משפט: $NSPACE(S(n)) \subseteq TIME(2^{O(S(n))})$

הוכחה: נגדיר גרף מכוון שנקרא גרף הקונפיגורציות עבור מ"ט M שרצה בזיכרון S(n) וקלט x. קדקודים יהיו הקונפיגורציות האפשריות $2^{O(S(n))}$. קשתות: $C_1 \to C_2 \Leftrightarrow C_1 \underset{M}{\vdash} C_2$. M מקבלת את x אס"ם קיים מסלול על הגרף מהקונפיגורציה ההתחלתית עד למקבלת.

כדי לסמלץ את M נבנה את גרף הקונפיגורציות של M על x (זמן $2^{O(S(n))}$), נריץ אלגוריתם לפתרון בעית הקשירות (למשל BFS) (זמן ליניארי ב- $2^{O(S(n))}$) ולכן סה"כ: $2^{O(S(n))}$.

משפט savich: $NSPACE(S(n)) \subseteq SPACE(S(n)^2)$

הוכחה: נתונה מ"ט לא דטר' M שרצה בזיכרון S(n) וקלט x ורוצים לדעת האם M מקבלת את x.

נגדיר: $REACH(C_1,C_2,t)=\{C_1,C_2$ בין t האם יש מסלול באורך לכל היותר} , נרצה לפתור את $REACH(C_0,C_a,T)$ כאשר $T=2^{O(S(n))}$:

1. נבקש זיכרון לאחסן את המשתנים.
2. נבדוק האם הקונפיגורציות זהות, אם כן נחזיר "כן".
3. נבדוק האם ניתן לעבור בין הקונפיגורציות במעבר יחיד, אם כן נחזיר "כן".
4. אחרת: נעבור בלולאה על כל הקונפיגורציות האפשריות T...1.
5. נקרא ל- $REACH(C_1,C\ ,\frac{T}{2})$
6. נקרא ל- $REACH(C\ ,C_2,\frac{T}{2})$
7. אם כן נחזיר "כן". אחרת "לא".

נחשב את כמות הזיכרון של REACH כאשר הוא מקבל את t:

$$A(t)=O(S(n))+O(S(n))+O(S(n))+O(S(n))+A(\frac{t}{2})=O(S(n)\log t)\le O(S(n)^2).$$

מה צריך להראות כדי להוכיח ש:

$L\in DFA$ - להראות אוטומט דטרמיניסטי המכריע את L.

$L\in NFA$ - להראות אוטומט לא דטרמיניסטי המכריע את L.

$L\in PDA$, $L\in CFL$ - להראות דקדוק ח"ה או אוטומט מחסנית המכריע את L.

$L\notin CFL$, $L\notin REG$ - שימוש בלמת הניפוח.

שפה כריעה – להראות מ"ט עבורה.

שפה לא כריעה – להראות רדוקציה משפה אחרת לא כריעה או שימוש במשפט RICE.

$L\in P$ - להראות מ"ט הרצה בשמן פולינומי המכריעה אותה.

$L\in NP$ - להראות מוודא פולינומי עבורה או להראות מ"ט לא דטר' עבורה.

$L\in NP-COMPLETE$ - להראות ש- $L\in NP$ ורדוקציה משפה שהיא NP שלמה או שלכל שפה ב- NP יש רדוקציה ל- L.