שפות NP-שלמות

שם	קלט	הסבר
HAMPATH	$<G>$	G גרף מכוון מכיל מסלול המילטוני.
uHAMPATH	$<G,s.t>$	G גרף לא מכוון מכיל מסלול המילטוני מs ל-t
dHAMPATH	$<G,s.t>$	G גרף מכוון מכיל מסלול המילטוני מs ל-t
CHAMPATH	$<G>$	G גרף מכוון המכיל מעגל המילטוני
3-SAT	$<\varphi>$	φ נוסחא בצורת 3-CNF ספיקה מהצורה $(x_1 \vee x_2 \vee x_3) \wedge (x_4 \vee x_5 \vee x_6)$
3-COL	$<G>$	G גרף לא מכוון 3 צביע
CLIQUE	$<G,k>$	G גרף לא מכוון המכיל קליקה בגודל k
VERTEX-COVER	$<G,k>$	G גרף לא מכוון ויש לו כיסוי בצמתים בגודל k

ניתנת לקבלה	כריעה	שפה
V	X	$ACCEPT=\{<M,w>:$ M מ"ט, w מחרוזת. M מקבלת את w$\}$
X	X	$NOT-ACCEPT=\{<M,w>:$ M מ"ט, w מחרוזת. M לא מקבלת את w$\}$
V	X	$HALT=\{<M,w>:$ M מ"ט, w מחרוזת. M עוצרת על w$\}$
V	X	$NOT-EMPTY=\{<M>: L(M)\neq\varnothing$ .M מ"ט$\}$
X	X	$EMPTY=\{<M>: L(M)=\varnothing$ .M מ"ט$\}$
X	X	$EQUAL=\{<M_1,M_2>: L(M_1)=L(M_2)$ .M_1,M_2 מ"ט$\}$
X	X	$ALL=\{<M>: L(M)=\Sigma^*$ .M מ"ט$\}$

סכמה לפיתרון שפות NP שלמות:

1) נוכיח כי התנאי בשפה הוא מסוג NP ע"י שימוש במוודא פולינומי:

a. נקבע את x קלט לפונקציה , y תשובה ספציפית שצריך לבדוק (לפי תנאי השאלה)

b. "אם השפה L בNP אזי קיים לה מוודה פולינומי. כלומר מ"ט V וקבוע c"

c. נגדיר את המוודא הפולינומי V ע"י אלגוריתם שמראה איך y עונה על x.

d. להגיד שהמוודא הפולינומי אכן פולינומי "זמן הריצה של V פולינומי באורך הקלט"

e. הוכחת זמן ריצה + **להגיד איזה קבוע c בחרנו כדי לקיים את התנאי** $|y| \le |x|^c$

f. **נכונות** - להוכיח כי בשפה ע"י $x \in L$ ו $x \notin L$.

2) להוכיח כי השפה L היא NP שלמה – ע"י רדוקציה:

a. **נמצא רדוקציה מתאימה לפי תנאי השאלה** – בעזרת הטבלה מלעיל.

b. נמצא **הרחבה** לרדוקציה כך שניתן להגיע בקלות להרחבה מהרדוקציה ולחזור בקלות מהנוסחא החדשה לרדוקציה.

c. **הוכחה:**

i. "נשים לב כי המיפוי R רץ בזמן פולינומי כי הוא..."

ii. $<x_{Red}> \in Red$ – נראה כי עבור הקלט x_{Red} מגיעים להוכחה של $<x_L> \in L$.

iii. $<x_L> \in L$ – נראה כי עבור הקלט x_L נוכל להגיע חזרה לרדוקציה ובהנתן אופן הבניה של x_L ניתן להסיק כי מתקיים $<x_{Red}> \in Red$

• מקביל להוכחת $x \in L$ ו $x \notin L$ לכו אם יותר נוח נשתמש בצורה זו.

שפות לא מתקבלות

$\{<M>:$ M מ"ט ומקבלת את כל המילים שמתחילות ב-1$\}$

$DECIDE=\{<M>$ M מ"ט ועוצרת על כל קלט$\}$

$\{<M,k>: |L(M)|<k$ ו M מ"ט$\}$

$\{<M>:$ M א"מ שמקבל את כל המלים מאורך זוגי$\}$

EMPTY→ EQUAL

R(<M>)=<M,M'>

כך ש- M'=מכונה שדוחה כל קלט

L(M)=empty set ⇔ L(M)=L(M')

←: L(M)=empty set ← וגם L(M')=empty set ← L(M)=L(M')

→: L(M)=L(M') ← וגם L(M')=empty set ← L(M)=empty set

כריעה	
✓	$ACCEPT_{DFA}=\{<M,w>: w$ M אס"ד, M מקבלת את w$\}$ פשוט מריצים את האס"ד
✓	$EMPTY_{DFA}=\{<M>: L(M)=\varnothing$ ו- M אס"ד$\}$ בתרגיל, מחפשים מצב מקבל בDFS
✓	$ALL_{DFA}=\{<M>: L(M)=\Sigma^*$ M אס"ד,$\}$ הופכים מצבים ובודקים $EMPTY_{DFA}$
✓	$ACCEPT_{NDFA}=\{<M,w>: w$ M אסל"ד, M מקבלת את w$\}$ הופכים לאס"ד
✓	$EMPTY_{NDFA}=\{<M>: L(M)=\varnothing$ M אסל"ד,$\}$ הופכים לאס"ד
✓	$ALL_{NDFA}=\{<M>: L(M)=\Sigma^*$ M אסל"ד,$\}$ הופכים לאס"ד
✓	$ACCEPT_{CFG}=\{<G,w>: w\in L(G)$ G דח"ה,$\}$ בתרגיל, אלגוריתם שבודק שמילה ניתנת לגזירה. זמן הריצה שלו אקספוננציאלי. ישנם היום אלגוריתמים יעילים מאד שעושים זאת. תראו בקומפיילרים ובעיבוד שפות טבעיות.
✓	$EMPTY_{CFG}=\{<G>: L(G)=\varnothing$ G דח"ה,$\}$ מסמנים טרמינלים ואז משתנים שגוזרים רק דברים מסומנים...
×	$ALL_{CFG}=\{<G>: L(G)=\Sigma^*$ G דח"ה,$\}$ זה מאד מאד מפתיע! השפה גם לא ניתנת לקבלה.

רדוקציה: ACCEPT → NOT_REGULAR / NOT_CFG

R(<M,w>)=<M'>

הגדרת M': בהנתן קלט x:

הרץ את M על w. אם M דוחה- דחה. (יתכן שזה לא יעצור)

הרץ את T על x ונהג כמוה.

R לא נכנסת ללולאה אינסופית- להסביר

T היא מ"ט כך ש- $L(T)=L=\{a^nb^n: n>0\}$. L לא רגולרית ולכן

<T>∈NOT_REGULAR

←: M מקבלת את w ← לכל קלט x: M' מריצה את T על x ונוהגת כמוה ← L(M')=L(T) ← השפה של M' לא רגולרית

→: M לא מקבלת את w ← או ש-M דוחה את w ← לכל x: M' דוחה את x, כלומר L(M')=empty-set. או ש-M נכנסת ללולאה אינסופית על w ואז לכל x L(M')=empty-set

משפט: בכדי להוכיח ששפה L היא NP שלמה:

1. השפה L היא ב-NP

2. לכל שפה L' שהיא NP שלמה ויש רדוקציה פולינומיאלית: $L' <_{p} L$. במילים: רדוקציה משפה NP שלמה לשפה שלנו

3-SAT → CLIQUE

בונים גרף G בעל 3m קודקודים: קודקוד לכל מופע של ליטרל בנוסחה. בגרף יהיו כל הצלעות האפשריות למעט: 1. לא שמים צלע בין שני קודקודים מאותה שורה-פסוקית. 2. לא שמים צלע בין ליטרל לשלילתו. נבחר k=m. Rרצה זמן פולינומי

←: יש השמה v שמספקת את d ← בכל פסוקית יש ליטרל שמסתפק ← כל הליטרלים הללו מחוברים אחד לשני כי: 1. הם לא באותה שורה. 2. לא יכול להיות משתנה ושלילתו, כי השמה לא יכולה לספק ליטרל ושלילתו בו זמנית. ← הראינו קליקה בגודל k=m

→: יש קליקה S בגודל k=m ← נגדיר פונקציית השמה לכל משתנה 1. אם Xi מופע בחיוב בS אזי ההשמה תיתן לו ערך אמת T. 2. אם Xi מופיע בשלילה ב-T אז קבל ערך אמת F. 3. אם Xi לא מופיע ב-T ניתן לו ערך אמת T (לא משנה). ← הבנייה שלנו מוגדרת היטב וכן כי לא יתכן שאותו משתנה Xi מופיע גם בחיוב וגם בשלילה ב-S. כיS קליקה ובG ליטרל ושלילתו לא מחוברים. בכל פסוקית ישנו ליטרל שנמצא בS. ליטרל זה מסתפק ע"י ההשמה שבחרנו. לכן הפסוקית מסתפקת

3-SAT → 3-COLOR: 1. רכיב השמה: כל ליטרל ושלילתו, 2. Gadget: 9 קודקודים,3 מכל סוג(קצה,ביניים,פנימיים) 3. רכיב משולש: מכיל {T,F,A} קשתות מק"ק ביניים ל-T. קשתות מרכיב משתנים(קודקודי קצה) השמה ל-A. צביעה תקינה ורלוונטית אם קצה: {T,F} וביניים: {F,A}. לא תקין: {F,F,F}

3-COLOR → 4-COLOR

פשוט מוסיפים קודקוד אחד ומחברים אותו לכל הקודקודים בG.

3-COLOR → 10-COLOR

נוסיף לגרף קליקה בגודל 7 שכל אחד מקודקודיה מחובר לכל אחד מקודקודי G

מבוא לסיבוכיות: $P=\cup_{c=1}^{\infty} DTime\in(n^c)$

היא שפה המוכלת ב- $NP=\cup_{c=1}^{\infty} NTime\in(n^c)$

וזוהי שפה המוכלת ב- $EXP=\cup_{c=1}^{\infty} DTime\in(2^{n^c})$

האם $P\neq NP$? לא ידוע, אבל חושבים שכן.

האם $NP\neq EXP$? גם לא ידוע וחושבים שכן.

האם $P\neq EXP$? כן.

מסקנה: $P\neq NP$ או $NP\neq EXP$ או

שפות רגולאריות

$L_1=\{w\in\{a,b\}^*:$ זוגי $|w|\}$

$L_1=\{w\in\{0,1\}^* \mid \#_w1\%3==0\}$

$L_2=\{w\in\{0,1\}^* \mid |w|\%2==1\}$

$L=\{w\in\Sigma^*$ מופיעה ב-w בדיוק פעמיים $\sigma\}$

שפות חסרות הקשר

$L=\{a^nb^n \mid n\geqslant 0\}$

$L_3=\{a^ib^j: i\neq j \wedge 2i\neq j\}$

$L=\{w=u_1\bigcirc u_2 \mid u_1=u_2^R, |u_1|=|u_2|\}$

$L=\{w=u_1\bigcirc u_2 \mid u_1\neq u_2, |u_1|=|u_2|\}$

$L=\{w=u_1\bigcirc u_2 \mid u_1=u_2 |u_1|=|u_2|\}$

$L=\{a^nb^m: m\geqslant n\}$

$L_1=\{a^nb^nc^m: n,m\geqslant 0\}$

שפות מתקבלות

$L=\{<M>: w^R$ M מ"ט וקיימת מילה w כך ש- M מקבלת את w וגם $\}$

$<M>:$ M מ"ט וקיימים ∞ קלטים עליהם היא עוצרת ו- ∞ קלטים עליהם היא לא עוצרת$\}$

$\{<M_1,M_2>:$ M_2,M_1 מ"ט, M_1 מקבלת $<M_2>\}$

שפות כריעות

$INFINITE_{DFA}=\{<A>$ A אס"ד, $L(A)$ אינסופית$\}$

$EVEN_{CFG}=\{<G>:$ G דח"ה וקיימת מילה באורך זוגי בשפה של G$\}$

$\{<G>:$ G דח"ה ויש ב L(G) לפחות שלוש מילים$\}$

שפות תלויות הקשר

$L=\{1^{2^i-1+i}: i\in\mathbb{N}\}$

$L_2=\{a^nb^m:$ $n,m\geq 0$ ומתקיים $n+m$ מספר ראשוני$\}$

שפות לא רגולריות

$L=\{w\in\{a,b,\ldots,z\}^*:$ קיימת אות $\sigma\in\Sigma$ כך ש-σ מופיעה ב-w לפחות $\frac{|w|}{2}$ פעמים$\}$

דף עזר זה נכתב ע"י נציגי סטודנטים. רונן אינו אחראי לחומר שכתוב בו, ואינו אחראי אם נפלו בו טעויות. הדף נועד כדף עזר, ומותר להסתמך כמוכח רק על חומר שנלמד בכיתה או בתרגיל

הגדרה פורמלית לאס"ד- אס"ד מוגדר ע"י חמישיה סדורה (Q,Σ,δ,q_0,F)

- Q- קבוצה סופית של מצבים
- Σ- א"ב
- $\delta: Q\times\Sigma\to Q$ -פונקציית מעבר.
- q_0- מצב התחלתי.
- $F\subseteq Q$-קבוצת המצבים המקבלים.

- **הוכחת נכונות באס"ד הוא באמצעות אינדוקציה על תנאי השאלה.** (מהחוברת)
- בעבור שאלות בהן צריך למנות מספר הופעות של אות במילה ואם ידוע לנו מספר אותיות גדול וסופי בשפה ניתן לכתוב וקטור כללי למילה בשפה באורך מספר האותיות בשפה ולמנות את מספר ההופעות לפי מיקום האות בא"ב בשפה, ונמנה אותיות רק עד גבול מסויים רלוונטי לתנאי השאלה . (מהחוברת)

למת הניפוח לשפות רגולריות- לכל שפה רגולרית L קיים מספר טבעי $n_0\geq 1$ ומתקיים: לכל מילה $w\in L$ כך ש$|w|\geq n_0$ קיימת חלוקה $w=xyz$ שמקיימת:

1. $|y|\geq 1$
2. $xy^kz\in L$ לכל $k\geq 0$.
3. $|xy|\leq n_0$

סכמה לשימוש בלמת הניפוח:

- נניח בשלילה כי השפה היא רגולרית. לכן למת הניפוח מתקיימת.
- בוחרים מילה ארוכה מספיק בשפה כפונקציה של n_0 (אומרים שקיימת לפי הלמה)
- נראה שבכל חלוקה אפשרית של המילה שבחרנו תנאים 1,2,3 לא יכולים להתקיים בוזמנית.
- קיום של מילה כזאת בשפה סותר נכונות של למת הניפוח (שהוכחה כנכונה).
- מסקנה: הנחה לא נכונה. כלומר. שפה לא רגולרית.

תכונות הסגור לשפות רגולריות- אם L_1,L_2 רגולריות אז גם השפות הבאות רגולריות.

$L_1\cup L_2$	$L_1\cap L_2$	$L_1\circ L_2$	$\overline{L_1}$	L_1^*	L_1^R

אלגוריתם ליצירת אוטומט מכפלה:

אם נקבל ביטוי המורכב מ2 שפות או מ2 חלקים שניתן לחלקם ע"י הקשרים $\{\cap,\cup\}$ נקוץ על האוטומט במקביל בצורה הבאה:

1) נקבע את q_0 בתור הזוג הסדור המתאר את תנאי ההתחלה בL_1,L_2 , (q_0,p_0).
2) ניצור קודקודים לאוטומט החדש המורכבמזוג סדוק של כל האפשרויות להתקדם בין 2 האוטומטים.
3) כל אפשרות להתקדמות לפי δ נגוע עם מצביעים על 2 האוטומטים וננמתח קשת בין 2 צמתים אם בעבור בחירת איבר מסויים נגיע למצב זהה ב2 האוטומטים המקוריים L_1,L_2 .
4) נקבע ממצב מקבל בהתאם לקשר המחבר בין השפות.

- בעבור $\cap$ נקבע מצב מקבל **אם כל הצמתים** בזוג הסדור הם צמתים מקבלים באוטומט המקורי.
- בעבור $\cup$ המצב המקבל קורה רק **אם צומת אחד לפחות** בזוג הסדור הוא מצב מקבל באוטומטים המקוריים.

משפט Myhill-Nerode – L היא שפה רגולרית אמ"מ מספר מחלקות השקילות שלה הוא סופי. באס"ד מינימאלי מספר המצבים שווה למספר מחלקות השקילות.

בהינתן שפה L מעל א"ב Σ נגדיר שני יחסים על מילים ב- Σ^*

יחס ההסכמה של L-

$$w_1\sim w_2\Leftrightarrow(w_1,w_2\in L)\cup(w_1,w_2\notin L)$$

יחס השקילות של L-

$$w_1\equiv w_2\Leftrightarrow\forall z\in\Sigma^*:\quad w_1z\sim_L w_2z$$

אוטומט מחסנית (א"מ)- $M=(Q,\Sigma,\Gamma,q_0,\delta,F)$

כאשר;

- Q- קבוצה סופית (של מצבים) $F\subseteq Q$- קבוצת המצבים המקבלים.
- Σ- א"ב הקלט
- Γ- א"ב המחסנית
- $q_0\in Q$- המצב ההתחלתי

ופונקציית המעבר- $\delta(q,\sigma,\gamma_1)\to(q_2,\gamma_2)$

$\delta: Q\times\Sigma_\epsilon\times\Gamma_\epsilon\to P(Q\times\Gamma_\epsilon)$

אלגוריתם להפיכת אסל"ד לאס"ד- בהינתן אסל"ד (Q,Σ,δ,q_0,F):

1) כל תת-קבוצה של Q נייצג ע"י מצב באס"ד. כלומר, מספר מצבים באס"ד יהיה כמספר תתי-הקבוצות של Q . בגודל $2^{|Q|}$
2) מצב התחלתי באס"ד – מצב שמייצג קבוצת המצבים באסל"ד שניתן להגיע אליהם מq_0 באמצעות מעברי ε (כולל q_0).
3) מצבים מקבלים – כל מצב שמייצג תת קבוצה של Q שמכילה לפחות מצב אחד מF.
4) כאשר נמצאים במצב שמייצג קבוצה A ומקבלים כקלט אות $\alpha\in\Sigma$ עוברים למצב שמייצג קבוצת כל מצבים שניתן להגיע אליהם כאשר מקבלים קלט α ונמצאים באחד המצבים של A.

תכונות סגור לשפות חסרות הקשר- אם L_1,L_2 חסרות הקשר אז גם השפות הבאות חסרות הקשר.

$L_1\cup L_2$	$L_1\cap R$, R רגולרית	$L_1\circ L_2$	L_1^*	L_1^R

למת הניפוח לשפות חסרות הקשר- לכל שפה ח"ה L קיים מספר טבעי $n_0\geq 1$ ומתקיים: לכל מילה $w\in L$ כך ש-$|w|\geq n_0$ קיימת חלוקה $w=uvxyz$ שמקיימת:

1) $|vy|\geq 1$
2) $uv^kxy^kz\in L$ לכל $k\geq 0$
3) $|vxy|\leq n_0$

דקדוק חסר הקשר (דח"ה) –

- קבוצה סופית V של נונטרמינלים (משתנים) שמסמנים אותם בד"כ באותיות לטיניות גדולות.
  - נונטרמינל אחד מוגדר כ-"נונטרמינל התחלתי" ובד"כ מסומן ב – S.
- קבוצה סופית Σ של טרמינלים (אותיות).
- קבוצה סופית R של כללי גזירה. כל כלל גזירה הוא מהצורה:
  - סדרה סופית של טרמינלים ונונטרמינלים או $Non-terminal\to\varepsilon$

בצורה נורמאלית של חומסקי – דקדוק חסר הקשר (V,Σ,R,S) אם מתקיים:

1. כל כלל גזירה מהצורה $A\to BC$ או $A\to\alpha$ כאשר $A,B,C\in V,B,C\neq S,\alpha\in\Sigma$.
2. ε יכול להיגזר רק מהנונטרמינל התחלתי. כלומר, $S\to\varepsilon$.

- לכל דקדוק חסר הקשר קיים דקדוק חסר הקשר בצורה הנורמאלית של חומסקי .
- **אם רוצים להוכיח ששפה המתקבלת ע"י אס"ד היא אינסופית צריך להוכיח שקיים לו לולאה** (מהחוברת)

מכונת טיורינג (מ"ט)-

הגדרה פורמלית למ"ט – מ"ט מוגדר ע"י שביעיה סדורה$M=(Q,q_0,F,\Gamma,\Sigma,\#,\delta)$ ה:

- Q- קבוצה ופית שאיבריה הם איברי המכונה.
- $q_0\in Q$ – מצב התחלתי של המכונה.
- $F\subseteq Q$ – קבוצת מצבים סופיים $\{Accept,Reject\}$.
- Γ – הא"ב של הסרט.
- Σ -א"ב של הקלט.
- $\#\in\Gamma\backslash\Sigma$ – תו ריק שמסמן שהתא שבו נמצא בסרט לא כולל תוכן (שייך רק לא"ב של הסרט).
- $\delta:(Q\backslash F)\times\Gamma\to Q\times\Gamma\times\{L,S,R\}$ – פונקציית המעברים של המכונה.

- כל אלגוריתם שאפשר לכתוב ע"י שפת C אפשר להגדיר מכונת טיורינג שמקבלת את אותה השפה.

טענה: אם L, $\overline{L}$ ניתנות לקבלה אז L כריעה.

בנוסף, אם R_1,R_2 ביטויים רגולריים אזי גם:

מכונת טיורינג אוניברסלית- מ

1) בדיקה שהקלט מהצורה $<M,w>$ כאשר $<M>$ קידוד חוקי של מ"ט ו w מחרוזת מעל א"ב הקלט של M. אם לא, נדחה.
2) ביצוע סימולציית ריצה של מ"ט M על מחרוזת הקלט w:
   - אם M מקבלת w – נקבל.
   - אם M דוחה w – נדחה.
- אם M לא עוצרת על w אזי גם U לא עוצרת על קלט $<M,w>$

הגדרה: עבור שתי שפות L_1,L_2 אומרים ש- L_1 ניתנת לרדוקציית מיפוי ע"י L_2, ומסמנים זאת $L_1\leqslant_m L_2$ אם קיימת מ"ט R (שמקבלת מחרוזת ומחזירה מחרוזת) כך שמתקיים: 1. לכל $x\in\Sigma^*$, R עוצרת על x.

2. לכל $x\in\Sigma^*$, $x\in L_1\Leftrightarrow R(x)\in L_2$

שפה כריעה – אם מתקיים $L(M)=L$ והיא **עוצרת על כל קלט**.כלומר:

- עבור כל מילה ששיכת לשפה $(x\in L)$, מסלול החישוב שלה יסתיים במצב מקבל (q_{accept}).
- עבור כל מילה שאינה שייכת לשפה $(x\notin L)$, מסלול החישוב שלה יסתיים במצב דוחה (q_{reject}).

תכונות סגור של שפות כריעות:

$L_1\cup L_2$	$L_1\cap R$ R ביטוי רגולרי	$L1\circ L2$	L_1^*	$\overline{L_1}$

משפט רייס- אם שפה L מקיימת:

1) $L\subseteq TM=\{<M>: M \text{ מ"ט}\}$
2) L לא טריוויאלית. כלומר $L\neq\emptyset,TM$.
3) לכל שתי מ"ט M_1,M_2 כך ש-$L(M1)=L(M2)$ מתקיים: $<M1>\in L\Leftrightarrow<M2>\in L$

אזי L לא כריעה. (כלומר לכל 2 מכונות אותה השפה).

מילה מקבלת :

- עבור כל מילה השייכת לשפה $(x\in L)$, מסלול החישוב שלה יסתיים במצב מקבל (q_{accept}).
- עבור כל מילה שאינה שייכת לשפה $(x\notin L)$, מסלול החישוב יסתיים במצב דוחה (q_{reject}) או במצב לא מקבל (כלומר לולאה אינסופית)

תכונות סגור של שפות ניתנות לקבלה:

$L_1\cup L_2$	$L_1\cap R$ R ביטוי רגולרי	$L1\circ L2$	L_1^*

- **כל שפה כריעה גם ניתנת לקבלה (ההפך לא בהכרח נכון). לכן אם שפה אינה ניתנת לקבלה היא גם לא ניתנת להכרעה.**

מבוא לסיבוכיות (שפות NP / P):

מכונת טיורינג לא דטרמיניסטית – מודל תיאורטי בו מאפשרים למכונה לבחור צעד חישוב הבא שלה מתוך קבוצה סופית של אפשרויות. קלט מתקבל ע"י מ"ט לא דטרמיניסטית אם קיים לפחות מסלול ריצה מקבל אחד.

שפה P:

- $TIME(t(n))=\{L: O(t(n))$ מתקבלת ע"י מ"ט דטרמיניסטית שזמן ריצה שלה $L\}$
- $P=\bigcup_{c\geq0}TIME(n^c)=\{$ מתקבלת ע"י מ"ט דטרמיניסטית שזמן ריצה שלה פולינומיאלי $L\}$

שפה NP:

- $NTIME(t(n))=\{L: O(t(n))$ מתקבלת ע"י מ"ט לא דטרמיניסטית שזמן ריצה שלה $L\}$
- $NP=\bigcup_{c\geq0}NTIME(n^c)=\{$ מתקבלת ע"י מ"ט לא דטרמיניסטית שזמן ריצה שלה פולינומיאלי $L\}$

מוודא פולינומי- בעבור x = **בעיה כל שהי** , y = **פתרון אפשרי לבעיה** ואם קיים קבוע c ומ"ט דטרמניסטית ופולינומית V כך שמתקיים:

- $x\in L\Rightarrow\exists y|y|<|x|^c: V(x,y)=1$

כלומר אם עבור בעיה x קיים y הרץ בזמן פולינומי ביחס לקלט x נחזיר 1.

- $x\notin L\Rightarrow\forall y: V(x,y)=0$ **כלומר אם עבור כל פיתרון y נחזיר 0.**

- **אינטואיצה: מקבלים קלט ותשובה אפשרית ורק צריך לראות אם בזמן פולינומי ניתן לקבוע אם התשובה נכונה או לא.**
- $L\in NP\Leftrightarrow L$ *ל מוודה פולינומי.*

רדוקציה פולינומית- משפה A לשפה B (סימון $A\leq_p B$) אם קיימת מ"ט דטרמיניסטית ופולינומית R ומתקיים $x\in A\Leftrightarrow R(x)\in B$ ($R(x)$= פלט של R על x)

הלכסון של קנטור משפט: אין פונקציה על $f:N\to P(N)$

$P(N)$ היא כמובן קבוצת כל תתי הקבוצות של N)

טכניקת ההוכחה: בשלילה, נניח שיש פונקציה F כזו שהיא על. נחשוב על F כעל מערך דו־מימדי אינסופי (של $(v,x$

במקום ה־ i,j נשאל האם $j\in f(i)$!

אם כן, אז נשמור במקום זה v ואחרת x.

מה מייצגת השורה ה־ i במערך! ־ היא מייצגת את הקבוצה $S=f(i)$. צריכים להראות שיש קבוצה $S^*\subseteq N$ כך שאין $i\in N$ כך ש־ $f(i)=S^*$. כלומר, צריכים להוכיח שקיימת תת־קבוצה של N שאינה מופיעה במערך כשורה.

הרעיון הטכני של קנטור הולך כך;
נסתכל באלכסון ונחשוב עליו כשורה. נהפוך בשורה זו כל v ל־ x ולהיפך. נגלה ש־ "ההיפך מהאלכסון אינו מופיע כשורה במערך" מכיוון שלכל שורה במערך (למשל השורה ה־ i) ההיפך מהאלכסון והשורה לא מסכימים על האיבר ה־ i.
ולכן הקבוצה S^* שמיוצגת ע"י ההיפך מהאלכסון לא מופיעה בשורה, ולא קיים i כך ש־ $f(i)=S^*$. קיבלנו סתירה לכך ש־ F על.

חזרה על אלגברה בוליאנית:

נתון א"ב Σ . נגדיר קבוצת ביטויים רגולריים באופן הבא

- $\varnothing$ • ε • a כאשר $a\in\Sigma$

נוסחא: $(x_1\vee\neg x_2)\wedge(x_3\vee\neg x_1\vee x_2)\wedge x_1\wedge\neg x_4$

משתנים: x_1,x_2,x_3,x_4

סדר פעולות

קשרים: $\vee,\wedge,\neg$ (שמורה: $(\neg,\wedge,\vee)$.

Syntax: ליטרל: $x_1,\neg x_1$

פסוקית: $(l_1\vee l_2....\vee l_t)$ כאשר $l_1...l_t$ ליטרלים לעומת $(x_1\vee\wedge\neg x_2x_1)\wedge\vee$ שזה לא בסינטקס

סמנטיקה:

השמה היא פונקציה α המתאימה לכל משתנה x_i ערך אמת.

x_1	T
x_2	T
x_3	F
x_4	T

בהינתן נוסחה φ והשמה α אפשר "להציב" את α ב- φ ומקבלים ערך אמת. למשל $\neg(T\wedge F)=T$

בהינתן נוסחה φ נאמר ש- φ ספיקה אם קיימת השמה α שכאשר מציבים את α ב- φ מקבלים T.

$3-SAT=\{\varphi:$ נוסחא בצורת $3\text{-}CNF$ ספיקה $\varphi\}$

$SAT=\{\varphi:$ נוסחא ספיקה $\varphi\}$