חישוביות - דף נוסחאות

מכונת טיורינג

מכונת טיורינג M היא שביעייה $M = \left(Q, q_0, F, \Gamma, \Sigma, \bar{b}, \delta\right)$.

1. מ"ט M תעצור כשתגיע למצב סופי - אחרת, עלולה לרוץ עד אינסוף.
2. פלט המכונה: הוא מילה $y \in \Gamma$ כך שהחוים עד הסרט שמסמאל לראש.

שפות רגולריות לדוגמה: $\emptyset, \Sigma^*$ או כל שפה סופית.

שפה לא רגולרית לדוגמה: $\{a^n b^n : n \in \mathbb{N}\}$.

קונפיגוראציה c היא שלשה $c = (\alpha, q, i)$ כאשר:
- $\alpha \in \Gamma^*$ הוא מחרוזת תוכן הסרט.
- $q \in Q$ הוא המצב הנוכחי.
- $i \in \mathbb{N}$ הוא מיקום הראש הקורא כותב.

שקילות מודלים: שתי מכונות טיורינג M_1, M_2 יקראו שקולות אם לכל קלט $x \in \Sigma^*$ התוצאה של שתי המכונות זהה. ⇐ ביוון ראשון: ניקח מכונה M_A (כללית) מהמודל הראשון A, ונמיר אותה למכונה שקולה M_B מהמודל השני B. ⇒ ביוון שני: אותו הדבר רק הפוך. (ניקח מכונה מהמודל השני ונמיר למכונה שקולה מהמודל הראשון). הערה: בדרך כלל אחד הכיוונים יהיה קל להוכיח והשני דורש מעט עבודה.

תכונות של מחלקות RE, R, coRE

$L \in RE$: מ"ט המכריעה שפה, בהכרח מקבלת.	$L \in R \subseteq coRE$: מ"ט המכריעה שפה, בהכרח גם דוחה.
• R סגורה למשלים, איחוד, חיתוך, רשור, איטרציה, רוורס.	$R = RE \cap coRE$
• $RE, coRE$ סגורה לאיחוד, חיתוך, רשור, איטרציה, רוורס.	

שפות מוכרות ב-R

$L_2 = \left\{< M_1 > \mid \exists < M_2 > s.t. \left|L(M_1) \cap L(M_2)\right| < 10 \text{ or } \left|L(M_1) \cap L(M_2)\right| > 1000\right\}$

$L_c = \{< M, x > \mid M \text{ halts on } x \text{ within } c \in \mathbb{N} \text{ steps}\}$

$BHP = \{< M, x > \mid M \text{ halts on } x, \text{ and } M \text{ doesn't enter the } (|x|^2+1)\text{'th cell of its tape}\}$

$COMPOSITE = \{n \mid n \text{ is composite}\}$	$L = \{(w_1, w_2, ..., w_n) \mid \exists i \text{ s.t. } w_i = \bar{i}\}$

$L_{M_0 c} = \{< M > \mid L(M) = L(M_0) \text{ and } |< M >| = c\}$

$L = \{< M, x > \mid \exists \text{ a Turing Machine } M', \text{ s.t. } M' \text{ accepts } x \text{ or } M \text{ accepts } < M' >\}$

שפות מוכרות ב-RE

$L_u = \{< M, x > \mid M \text{ accepts } x\}$	$L_D = \{< M > \mid M \text{ accepts } < M >\}$
$L = \{< M > \mid \exists x \text{ s.t. } f_M(x) = x\}$	$HP = \{< M, x > \mid M \text{ halts (stops) on } x\}$
$L = \{< M > : M(001) = 001\}$	$L_\varepsilon = \{< M > \mid M \text{ accepts } \varepsilon\}$

$L_3 = \left\{< M_1 >, < M_2 > \mid \text{s.t. } \left|L(M_1) \cap L(M_2)\right| > 10 \text{ or } \left|L(M_1) \cap L(M_2)\right| > 1000\right\}$

$L = \{< M_1 >, < M_2 > \mid M_1 \text{ and } M_2 \text{ are TM and } L(M_1) \cap L(M_2) \neq \emptyset\}$

$L_3 = \{< M > \mid \exists w \in L(M) \text{ s.t. } M \text{ accepts } w \text{ in less than } |w| \text{ steps}\}$

$L = \{< N, x > \mid N \text{ running on } x \text{ has an accepting path and a rejecting path}\}$

שפות מוכרות ב-coRE

$\overline{HP}, \overline{L_u}, \overline{L_d}$	$L = \{< M > \mid < M > \notin L(M)\}$

$L = \{< M > \mid L(M) = \emptyset\}$

$L_4 = \{< M > \mid M \text{ is a TM that halts on at most one input}\}$

שפות מוכרות שהם לא ב-RE וגם לא ב-coRE כלומר $\overline{coRE} \cup \overline{RE}$

$L_{\Sigma^*} = \{< M > \mid L(M) = \Sigma^*\}$	$L_\infty = \{< M > : |L(M)| = \infty\}$
$L_{=3} = \{< M >: |L(M)| = 3\}$	$L_{eq} = \{< M_1, M_2 > \mid L(M_1) = L(M_2)\}$

$L_1 = \left\{< M_1 >, < M_2 > \mid \text{s.t. } \left|L(M_1) \cap L(M_2)\right| < 10 \text{ or } \left|L(M_1) \cap L(M_2)\right| > 1000\right\}$

$L = \left\{\left(< M_1 >, < M_2 >, x\right) \mid M_1 \text{ stops on } x \text{ and } M_2 \text{ doesn't stop on } x\right\}$

$L_1 = \{< M > \mid M \text{ stops to every input after more than } 42 \text{ steps}\}$

רדוקציות $\leq$ (חישוביות - לא פולינומיות)

הגדרה: תהיינה שפות $L_1, L_2 \subseteq \Sigma^*$, נאמר ש: L_1 ניתנת לרדוקציה ל-L_2 (נסמן $L_1 \leq L_2$) אם ורק אם קיימת פונקציה $f: \Sigma^* \to \Sigma^*$ שהיא: **1)** פונקציה מלאה: פונקציה המוגדרת לכל קלט. **2)** פונקציה הניתנת לחישוב: קיימת מ"ט שיכולה לחשב את הפונקציה הזו. **3)** פונקציה תקפה: $\forall x \in \Sigma^* : x \in L_1 \Leftrightarrow f(x) \in L_2$.

אם $L_1 \leq L_2$ (אם L_1 ניתנת לרדוקציה ל-L_2) אז: • אם $x \in L_2$ אז גם $x \in L_1$. • אם $x \in L_2$ אז גם $x \in RE$. • אם $x \in L_2$ אז גם $x \in coRE$.	אם $L_1 \leq L_2$ (אם L_1 ניתנת לרדוקציה ל-L_2) אז: • אם $x \notin L_1$ אז גם $x \notin L_2$. • אם $x \notin L_1$ אז גם $x \notin RE$. • אם $x \notin L_1$ אז גם $x \notin coRE$.

כדי להוכיח ש: $L \in \overline{RE} \cup \overline{coRE}$, צריך להוכיח ב-2 רדוקציות: $L \notin RE$ וגם $L \notin coRE$.

מקרי קצה חוקיים:
- לכל שפה $L \neq \Sigma^*$ ניתן לרדוקציה $\emptyset \leq L$.
- לכל שפה $\emptyset \neq L$ ניתן לרדוקציה $L \leq \Sigma^*$.

מקרי קצה לא חוקיים: $\Sigma^* \leq \emptyset$ וגם $\emptyset \leq \Sigma^*$ פונקציית הרדוקציה היא תמיד דטרמיניסטית!

כל שפה $L_1 \in R$ ניתנת לרדוקציה לכל שפה אחרת L_2 כלומר $L_1 \leq L_2$ כך ש: $L_2 \neq \Sigma^*$ וגם $L_2 \neq \emptyset$.

כמות הרדוקציות הקיימות בעולם חסומה בכמות המ"ט כיוון שכל רדוקציה ניתנת לחישוב. (בת מניה $\aleph_0$)

שפות שלמות

שפה L היא שלמה ב-RE אם"ם היא: **1)** $L \in RE$ **2)** $\forall L' \in RE : L' \leq L$ (כל L' ניתנת לרדוקציה ל-L)

שפות שלמות של RE שהוכחנו: HP, L_u.	כל השפות ב-R הם שלמות מלבד הטריוויאליות: $\emptyset, \Sigma^*$.

נתונה שפה שלמה $L \in REC$ ונתונה שפה נוספת $L^* \in RE$. אם מתקיים ש: $L \leq L^*$ אז גם $L^* \in REC$.

במחלקה $RE \cup coRE$ אין שפה שלמה

משפט רייס

הגדרה: תכונות לא טרוויאליות ב-RE הן תכונות S כך ש: $S \subseteq RE$ וכן $\emptyset \neq S \neq RE$.

אבחנה: לכל תכונה לא טרוויאלית S קיימת שפה אחת ב-S ולפחות שפה אחת ב-$\backslash RE$.

הגדרה: בהינתן תכונה $S \subseteq RE$, נגדיר את השפה $L_S = \{< M > \mid L(M) \in S\}$.

הגדרה (משפט רייס): לכל תכונה לא טרוויאלית $S \subseteq RE$ מתקיים $\emptyset \neq S \subseteq RE$: $L_S \notin R$.

הגדרה (משפט רייס המורחב): בנוסף, אם $\emptyset \notin S$ אז $L_S \notin coRE$ ואם $\emptyset \in S$ אז $L_S \notin RE$.

אבחנה: אם התכונה היא שלמה לכל מכונה ולא תכונה לשל שפה אם משפט רייס לא עובד.

אם S טריוויאלית - משפט רייס "לא עובד".

מכונת טיורינג אי דטרמיניסטית

מ"ט א"ד שקולה בכוח החישוב שלה לתכונה דטרמיניסטית

אסימטריה של מ"ט א"ד: אם הרצנו מכונה א"ד על קלט x, יש כמה אפשרויות:
1) המכונה קיבלה **2)** המכונה דחתה **3)** המכונה לא עוצרת.

א"ד מוגבל: $\exists c \in \mathbb{N}$. נוח לחשוב על עץ ההרצות הזה בתור עץ בינארי.

מ"ט א"ד N **מקבלת** שפה L אם: 1. לכל $x \in L$ קיים מסלול מקבל בעץ החישוב. 2. לכל $x \notin L$ לא קיים מסלול מקבל בעץ. 3. ב-2 המקרים, יתכן גם מסלולים אינסופיים.	מ"ט א"ד N **מכריעה** שפה L אם: 1. לכל $x \in L$ קיים מסלול מקבל בעץ החישוב. 2. לכל $x \notin L$ כל המסלולים דוחים. 3. ב-2 המקרים, כל המסלולים סופיים.

מחלקת שפות בזמן ריצה

הגדרה - מחלקה של שפות: תהי פונקציה $t: \mathbb{N} \to \mathbb{N}$. נסמן ב-$DTIME(t(n))$ את מחלקת השפות שיש להן מכונת טיורינג דטרמיניסטית מכריעה שזמן הריצה שלה הוא $O(t(n))$.

משפט 1: אם $t_1(n) = O(t_2(n))$ אז $DTIME(t_1(n)) \subseteq DTIME(t_2(n))$.

משפט 2: שפה שניתנת להכרעה בזמן $O(n \cdot \log(n))$ במכונה עם סרט אחד היא בהכרח רגולרית.

מסקנה: זמן הסימולציה של מכונה מרובת סרטיות ע"י מכונה חד-סרטית הוא ריבועי לכל היותר: $O(t(n)^2)$

מכונת טיורינג פולינומית

מכונה דטרמיניסטית פולינומית מכריעה:
1. הוכחת נכונות:
   a. $M(x) = 1 \leftarrow x \in L$
   b. $M(x) = 0 \leftarrow x \notin L$
2. הוכחת סיבוכיות: להוכיח שלכל קלט x, זמן הריצה של המכונה על x חסום ע"י פולינום כלשהו $p(|x|)$.

מכונה א"ד פולינומית מכריעה:
1. הוכחת נכונות:
   a. $x \in L \leftarrow$ אז **קיים** מסלול **מקבל** בעץ החישוב של המכונה על x.
   b. $x \notin L \leftarrow$ אז **כל** המסלולים בעץ החישוב של המכונה על x **דוחים**.
2. הוכחת סיבוכיות: להוכיח שלכל קלט x, ולכל מסלול בעץ החישוב, זמן הריצה של המכונה על x חסום ע"י פולינום כלשהו $p(|x|)$.

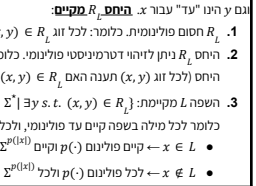
הפולינום $p(n) = n^c$ יקרא **חסם זמן הריצה** של המכונה M.

המחלקות בעולם הסיבוכיות

המחלקה P - בעיות הכרעה (כן או לא) שניתן לפתור אותן (תמיד לעצור) בזמן פולינומי: $O(n^c)$ c - מספר קבוע) האלגוריתם צריך להיות דטרמיניסטי (ללא ניחושים).

המחלקה NP-שלמה (NPC) - בעיות שהן NP-קשות וגם שייכות ל NP.
1. המחלקה L_2 היא שלמה ב-NP אם:
   1. $L_2 \in NP$ (שייכת למחלקה).
   2. לכל שפה $L_1 \in NP$ מתקיים ש: $L_1 \leq_p L_2$.

המחלקה NP-קשה (NPH) - בעיות שקשות יותר מכל הבעיות האחרות ב NP אך הן עצמן לא חייבות להיות ב NP. איך מודדים קושי? ע"י רדוקציה פולינומית: אם L היא NP-קשה אז לכל $L' \in NP$ מתקיים: $L' \leq_p L$.



- P **סגורה** למשלים, איחוד, חיתוך, רשור, איטרציה, רוורס, הפרש, חזקה.

המחלקה NP - בעיות הכרעה שבהינתן פתרון מבחוץ, ניתן לאמת שאכן זהו הפתרון בזמן פולינומי. (איך בפועל מקבלים את הפתרון? ע"י מכונה אי דטרמיניסטית שפשוט מנחשת את הפתרון ומניחים שהיא מנחשת נכון ואז היא מוודאת את הפתרון. אז ע"י יחס NP שמקבל בנוסף ל x הקלט, גם עד y - הפתרון עצמו ואז היחס/האלגוריתם מוודא בצורה דטרמיניסטית את הפתרון).

המחלקה coNP - בעיות ההכרעה שהשלימה שלהן שייכת ל NP. כלומר, בהינתן עד, ניתן להשתמש בו ולוודא בזמן פולינומי אי קיום פתרון (שהקלט לא בשפה). כאן מנחשים את ההוכחה שהקלט לא בשפה.

המחלקה coNP-שלמה - בעיות שהן $coNP$ קשות (קשות יותר מכל הבעיות האחרות ב $coNP$) וגם שייכות בעצמן ל $coNP$.

מה ידוע?:

$P \subseteq NP$	$P \subseteq coNP$
$P \subseteq NP \cap coNP$	$P \neq NPH$
$NPC \subset NPH$	$NP \subseteq R$ וגם $P \subseteq R$

אם תמצאו שפה NPC השייכת ל P אז $P = NP$.

מה לא ידוע?:
- $NP \subseteq P$ (כלומר לא ידוע האם $P = NP$)
- $NP = coNP$
- $P = NP \cap coNP$

- $NP, coNP$ **סגורה** לאיחוד, חיתוך, רשור, איטרציה, רוורס, חזקה.

יחס R_L

הגדרה: שפה $L \in NP$ אם קיים יחס דו-מקומי R_L המכיל זוגות (x, y) כך שמתקיים: $x \in L$ וגם y הינו "עד" עבור x. **היחס R_L מקיים**:
1. R_L חסום פולינומית. כלומר: לכל זוג $(x, y) \in R_L$ קיים פולינום $p(\cdot)$ כך שמתקיים: $|y| \leq p(|x|)$.
2. היחס R_L ניתן לזיהוי דטרמיניסטי פולינומי. כלומר - קיימת מ"ט דטרמיניסטית פולינומית V המכריעה את היחס (לכל זוג (x, y) תענה האם $(x, y) \in R_L$ או $(x, y) \notin R_L$). המכונה V נקרא מאמת.
3. השפה L מקיימת: $L = \{x \in \Sigma^* \mid \exists y \text{ s.t. } (x, y) \in R_L\}$.

כלומר לכל מילה בשפה קיים עד פולינומי, ולכל מילה שלא בשפה לא קיים עד פולינומי.
- $x \in L \leftarrow$ קיים פולינום $p(\cdot)$ וקיים $y \in \Sigma^{p(|x|)}$ כך ש: $(x, y) \in R_L$.
- $x \notin L \leftarrow$ לכל פולינום $p(\cdot)$ ולכל $y \in \Sigma^{p(|x|)}$ כך ש: $(x, y) \notin R_L$.

רדוקציה פולינומית $\leq_p$ (של סיבוכיות)

אם יש רדוקציה בזמן פולינומיאלי של A ל-B מסמנים $A \leq_p B$.

רדוקציה פולינומית: בהינתן שתי שפות L_1, L_2, נאמר ש: L_1 ניתנת לרדוקציה פולינומית ל-L_2 ונסמן $L_1 \leq_p L_2$ אם קיימת פונקציה f כך ש: **1)** f ניתנת לחישוב בזמן פולינומי. **2)** f תקפה, כלומר $x \in L_1 \Leftrightarrow f(x) \in L_2$.

אם $L_1 \leq_p L_2$ אז גם $L_1 \in NP$ ו-$L_2 \in NP$.	אם $L_1 \leq_p L_2$ אז $\overline{L_1} \leq_p \overline{L_2}$.
היחס $\leq_p$ טרנזיטיבי וגם סימטרי. לא ידוע אם היחס $\leq_p$ רפלקסיבי.	אם $L_1 \in P$ ו-L_2 היא שפה כלשהי ששונה מ-$\emptyset$ וגם מ-Σ^*, אז $L_1 \leq_p L_2$.
היחס $\leq$ הוא רפלקסיבי, טרנזיטיבי **ולא** סימטרי.	אם $L_1 \leq L_2$ אז גם $\overline{L_1} \leq \overline{L_2}$.

כל שפה ב-NPC ניתנת לרדוקציה פולינומית לכל שפה ב-NPC. בשני הכיוונים. $L_1 \leq_p L_2 \wedge L_2 \leq_p L$

אם קיימת שפה $L_1 \in NPC$ שניתנת לרדוקציה פולינומית לשפה $L_2 \in P$ כלומר $L_1 \leq_p L_2$ אזי $NP = P$.

פסוקים

הגדרה: פסוק נקרא **ספיק** אם יש לפחות השמה אחת של ערכי אמת למשתנים של הפסוק שבה ערך האמת של הפסוק הוא $true$.

מה זה DNF? - בצורת $(x \wedge y) \vee (z \wedge t)$	**מה זה CNF?** - בצורת $(x \vee y) \wedge (z \vee t)$
זהות CNF שתמיד נכון: $(\bar{x}) \wedge (x)$	**זהות CNF שתמיד נכון:** $(\bar{x} \vee x)$

שפות ב-P

$DNF - SAT = \{< \phi > \mid \phi \text{ is a satisfiable DNF Boolean formula}\}$

$PATH = \{< G, s, t, > \mid G \text{ is a directed graph that has a directed path from } s \text{ to } t\}$

$PRIMES = \{n \mid n \text{ is prime}\}$, $COMPOSITES = \{n \mid n = pq, \text{ for integers } p, q > 1\}$

$11 - CLIQUE = \{< G > \mid \exists C \subseteq V(G) \text{ s.t. } |C| = 11 \text{ and } C \text{ is a clique}\}$

$SP = \{(< G >, k) \mid \text{The shortest path in } G \text{ is of length} < k\}$

$2SAT = \{< \phi > \mid \phi \text{ is a satisfiable 2CNF Boolean formula}\}$

$L_{logn} = \{\phi \mid \phi \text{ has a satisfying assignment } \pi, \text{ and } \exists i \text{ s.t. } \forall_{j \notin [i+1, i+2, ..., i+\log n]} \pi(x_j) = T\}$

$1COL = \{G \mid G \text{ has a 1 coloring}\}$	$2COL = \{G \mid G \text{ has a 2 coloring}\}$
$EC = \{< G > \mid G \text{ has an Euler cycle}\}$	$EP = \{< G > \mid G \text{ has an Euler path}\}$

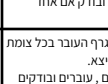
"משפט ארבעת הצבעים" מבטיח שלכל גרף מישורי יש 4-צביעה. כלומר, $4PlanarColor \in P$ כי בעזרת המשפט, אפשר לבנות מ"ט דטרמיניסטית שבהינתן גרף G, מספיק לה לבדוק כי G מישורי, אם כן, אז בהכרח קיים 4-צביעה ל-G.

אם ביקשו ממנו גרף k-צביע כאשר בגרף יש רק n קודקודים כך ש: $k \geq n$ אז קיימים יותר צבעים מקודקודים ולכן אפשר לפתור באופן דטרמיניסטי ובזמן פולינומי מקרים פרטיים כאלה.

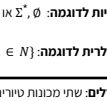
הוכחה: $2SAT \in P$. **מבוא להוכחה:** במקרה של פסוקים שיש בה רק שני ליטרלים, אם ידוע לנו על אחד מהם שהוא F אז השני חייב להיות T כדי שהפסוק יסתפק. מה שאומר שניתן לבנות גרף מכוון שירכז את כל התנאים של כל הפסוקיות ולהשתמש בגרף הנ"ל כדי למצוא השמה מספקת. כך שאם השמה זו לא קיימת, נוכל לזהות זאת ולהחזיר תשובה שלילית.נוכיח ע"י בניית גרף שייצג שקילות לגיית לפסוק. הבנייה תעשה בזמן פולינומי, הפעולות על הגרף יוישעו בזמן פולינומי, הפסוק שנעסוק בו הוא $\phi(x_1, ..., x_n) = C_1 \wedge C_2 \wedge \ ... \ \wedge C_m$ בעל m פסוקיות. לסיכום, בהינתן פסוק $2CNF$ נתאר מכונה/אלגוריתם דטרמיניסטי פולינומי: M_{2SAT} על קלט $< \phi >$ תבצע: **1)** בונה את הגרף הנ"ל. **2)** לכל $v \in V$ תבצע: **2.1)** מבצעת BFS (או DFS) מ-v. **2.2)** אם קיים מסלול מ-v אל $\bar{v}$, מבצעת גם BFS מ-$\bar{v}$, אם נמצא שהמסלול מגיע חזרה אל v - אז דחה. **3)** קבל. נכונות הבנה: נובעת ישירות נכונות הקריטריון שהוכחנו.סיבוכיות זמן ריצה: סיבוכיות של DFS היא $O(n + |E|) = O(n + n^2)$ ובמבצע את ה-DFS למשך $n = |V|$ פעמים. סה"כ נקבל $O(n^3)$ - זמן פולינומי.

תורת הגרפים

כיסוי קודקודים - קבוצת קודקודים שנוגעת בכל צלעות הגרף.
מכונה: מנחש קבוצה בגודל K, ועובר על כל הקודקודים ובדוק אם אחד מהשכנים שלה (או אני) ב-K.



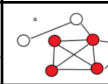
קבוצה שלוטת - קבוצת קודקודים שנוגעים בכל שאר הקודקודים בגרף.
מכונה: מנחש קבוצה בגודל K, ועובר על כל הקודקודים ובדוק אם אחד מהשכנים שלה K-ב.



מעגל המילטון - הוא מסלול בגרף העובר בכל צומת פעם אחת פרט לצומת שממנו יצא.
מכונה: מנחש רשימת קודקודים, ועוברים ובודקים שהם שונים אחד מהשני, עובר אחד אחד ובודק שהם מחוברים בצלע ושהאחרון מחובר לראשון.

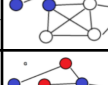
מסלול המילטון - הוא מסלול בגרף מכוון או בלתי מכוון העובר בכל צומת שממנו יצא.
מכונה: מנחש רשימת קודקודים, ועוברים ובודקים שהם שונים אחד מהשני, עובר אחד אחד ובודק שהם מחוברים בצלע.

קליקה - תת גרף שבו כולם מחוברים לכולם בצלע.



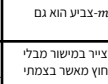
מעגל אוילר - הוא מסלול אוילר מעגלי (מתחיל וגגמר באותו צומת) העובר בכל קשת פעם אחת.
זהות: בגרף **קשיר** (BFS) קיים מעגל אוילר אם ורק אם כל הקודקודים בעלי דרגה זוגית.

קבוצה בלתי תלויה - תת גרף שבו אף אחד לא מחובר לאף אחד בצלע.

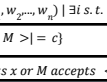


מסלול אוילר - הוא מסלול בגרף העובר בכל קשת בדיוק פעם אחת.
זהות: בגרף **קשיר** (BFS) קיים מסלול אוילר אם ורק אם יש בדיוק 2 או 0 צמתים בעלי דרגה אי זוגית.

גרף k-צביעה - גרף שניתן לצבוע את קודקודיו ב-k צבעים שונים כך שלא יהיו 2 סמוכים עם אותו הצבע.
זהות: אם $n = m$ אז כל גרף m-צביע הוא גם n-צביע



גרף דו צדדי - גרף שבו ניתן לחלק את הקודקודים לשתי קבוצות זרות, כך שלא קיימת קשת בין שני קודקודים השייכים לאותה הקבוצה.
- גרף הוא דו-צדדי אם ורק אם אין בו מעגל אורך אי-זוגי.
- גרף הוא דו-צדדי אם ורק אם הוא 2-צביע.



גרף מישורי - הוא גרף שניתן לצייר במישור מבלי שהקשתות תתחוכנה זו את זו (חוץ מאשר בצמתי הגרף). זהות: כל גרף מישורי הוא 4-צביע.

גרף k PLANAR צביע - גרף מישורי k-צביע.
זהות: כל גרף מישורי הוא 4-צביע.

גרף איזומורפי - (כאלו שיש ביניהן איזומורפיזם) הם זהים זה לזה מכל בחינה תאורטית.

שפות NP-שלמות (NPC) שהוכחנו בהרצאות, תרגולים ומטלות

$SAT = \{< \phi > \mid \phi \text{ is a satisfiable Boolean formula}\} \in NPC$

$CNF - SAT = \{< \phi > \mid \phi \text{ is a satisfiable CNF Boolean formula}\} \in NPC$

איך הוכח?: בעזרת משפט קוק לוין.

$SAT_2 = \{< \phi > \mid \exists \text{ two satisfying assignments to } \phi\}$

איך הוכח?: בדרקוציה $SAT \leq_p SAT_2$ עם $f(\phi) =$ 'φ' וגם $\phi = \phi \wedge (y \vee \bar{y})$ כאשר 'φ'.

$DHL = \{< G > \mid G \text{ is a directed graph with a Hamiltonian path}\}$

איך הוכח?: בדרקוציה $HL \leq_p DHL$ עם $f(G) =$ 'G' - ניקח כל צלע ב-G ונשים במקומה 2 צלעות מכוונות.

$HL = \{< G > \mid G \text{ is an undirected graph with a Hamiltonian path}\}$

איך הוכח?: בדרקוציה $HC \leq_p HL$ עם $f(G) =$ 'G' - ניקח קודקוד v ו"נפצל" אותו לשני קודקודים u, w שיהיו מחוברים לכל השכנים של v. נוסיף גם צלעות שיוצאות מ-w ו-u לקודקודים חדשים.

$VC = \{< G, k > \mid G \text{ is a graph that contains a vertex cover of size } k\}$

איך הוכח?: בדרקוציה $3CNFSAT \leq_p VC$ עם $f(\phi) =< G, k >$ - לכל משתנה x φ-, ניצור 2 קודקודים לו ולמשלים שלו ונחבר ביניהם צלע. כל פסוקית היא שלשה של קודקודים (הליטרלים בפסוקית הזאת) ומחוברים ביניהם וגם מחוברים לקודקודי המשתנים שלהם (בהתאם) שיצרנו לכל משתנה x.

$3 - CNF - SAT = \{< \phi > \mid \phi \text{ is satisfiable } 3 - CNF \text{ Boolean formula}\}$

איך הוכח?: בדרקוציה $3SAT \leq_p SAT$. עם $f(\phi) =$ 'φ' - לכל פסוקית שיש בה 1 או 2 ליטרלים, נבחר אחד מהם ונשכפל אותו בתוך הפסוקיות עד שנגיע ל-3 ליטרלים. לכל פסוקית שיש בה יותר מ-3 ליטרלים, נפצל אותה לכמה פסוקיות בגודל 3, במידה ונשאר לנו שארית להשלים אז נבחר במשתנה במשתני עזר y_i ונשכפל אותם עד שנגיע ל-3 ליטרלים בכל הפסוקיות.

$BALANCED - SAT = \{\phi \mid \exists \text{ balanced satisfying assignments for } \phi\}$

איך הוכח?: בדרקוציה $f(\phi) =$ 'φ' עם $SAT \leq_p BALANCED - SAT$ נבנה את הפסוק 'φ' כך: $(y_1 \vee \bar{y}_1) \wedge \ ... \ \wedge (y_n \vee \bar{y}_n) \wedge \phi = \phi$ 'φ'.

$IS = \{< G, k > \mid G \text{ is an undirected graph that has a } k - \text{node independent set}\}$

איך הוכח?: בדרקוציה $VC \leq_p IS$ עם $f(< G, k >) =< G, n - k >$. **למה**: עבור גרף $G = (V, E)$ קבוצת הקודקודים $S \subseteq V(G)$ היא בלתי תלויה ב-G אם"ם $V \backslash S$ היא כיסוי קודקודים של G.

$CLIQUE = \{< G, k > \mid G \text{ is a graph that contains a clique of size } k\}$

איך הוכח?: בדרקוציה $IS \leq_p CLIQUE$ כאשר $f(< G, k >) =< G', k' >$. **למה**: עבור גרף G, קבוצת הקודקודים $S \in V(G)$ היא קליקה ב-G אם"ם S היא קבוצה ב"ת ב-$\bar{G}$ (כל הלא שכנים של G הם שכנים).

$CliqueIS = \{< G, k_1, k_2 > \mid G \text{ is a graph with a Clique of size } k_1 \text{ OR an IS of size } k_2\}$

איך הוכח?: בדרקוציה $CLIQUE \leq_p CliqueIS$ כאשר $f(< G, k >) =< (< G', k_1, k_2 >)$.

$SUBSET - SUM = \{< S, t > \mid S = \{x_1, .., x_n\}, \exists \{y_1, .., y_k\} \subseteq S, \Sigma y_i = t\}$

איך הוכח?: בדרקוציה $3SAT \leq_p SUBSET - SUM$. (בעזרת בניית טבלה y, z, h, g).

$HamOrClique = \{(G, k) \mid G \text{ has a Hamiltonian path or a Clique of size } k\}$

איך הוכח?: בדרקוציה $CLIQUE \leq_p HamOrClique$ כאשר $f(< G, k >)$. נאלץ את G' לא להיכל אף פעם מסלול המילטוני - זאת בעזרת הוספת קודקוד חדש ובודד לגרף G'.

$HamAndClique = \{(G, k) \mid G \text{ has a Hamiltonian path and a Clique of size } k\}$

איך הוכח?: בדרקוציה $HAMPATH \leq_p HamAndClique$ כאשר $f(< G >) =< G, 1 >$.

$3COLOR = \{< G > \mid G \text{ can be colored with 3 colors}\}$

איך הוכח?: בדרקוציה $3SAT \leq_p 3COLOR$ כאשר ניצור 3 קודקודים T, F, B ונחבר אותם. לכל ליטרל בפסוק, ניצור קודקוד ונחבר אותו ל-B. נחבר בין כל משתנה לשלילתו. לכל שלושה ליטרלים המהווים פסוקיות, נוסיף 'תוספת' בעלת 6 קודקודים ו-13 צלעות.

$EXACT - SUBSET - SUM = \{(x_1, ..., x_n), k, m \mid \exists I \subseteq [n] \text{ s.t. } \Sigma_{i \in I} x_i = k \wedge |I| = m\}$

איך הוכח?: בדרקוציה $SUBSET - SUM \leq_p EXACT - SUBSET - SUM$ כאשר $f(< (x_1, ..., x_n), k >) = (< (x_1, ..., x_n, 0, 0, ..., 0, 0), k, n >)$ (נרפד n אפסים לקבוצה מימין).

השפה $NAE - 3cnfSAT$ זהויי שפה של פסוקיות $3cnf$, שיש לן השמה מספקת, אבל בכל פסוקיות יש ליטרל שמקבל F. **איך הוכח?**: בדרקוציה: $3cnfSAT \leq_p NAE - 3cnfSAT$ עם $f(< \phi >) =$ 'φ' - אז דחה. **3)** קבל. נכונות הבנה: נובעת ישירות נכונות הקריטריון שהוכחנו.סיבוכיות זמן ריצה: סיבוכיות של DFS היא $O(n + |E|) = O(n + n^2)$ ובמבצע את ה-DFS למשך $n = |V|$ פעמים. סה"כ נקבל $O(n^3)$ - זמן פולינומי.

$NAE - 3cnfSAT \leq_p NAE - 4cnfSAT$.

$3 - PLANAR - COLOR = \{G \mid G \text{ is a planar graph and has a valid } 3 - coloring\}$

איך הוכח?: בדרקוציה: $3COLOR \leq_p 3 - PLANAR - COLOR$. בכל פסוקית ניתן בין שתי צלעות, נכניס את הגרף המישורי W (שמופיע בציור בחלק של תורת הגרפים למעלה עבור PLANAR).

נקודות שערן הוסיף בסוף

השפה EXACT-SUBSET SUM - מקבלים קבוצה A של n מספרים עם מספר k ועוד מספר m כך קשיימת קבוצה קבוצה l שהסכום של הקבוצה הוא k והגודל של l הוא m.

השפה BALANCES-SAT - נאמר על ההשמה שהיא מאוזנת אם מספר המשתנים שקיבלו אמת שווה למספר המשתנים שקיבלו שקר.

כאשר נרצה להראות שייכות ל- coRE (מכונה דוחה) ולא ל-R (שפות מוכרות ב-coRE)
כאשר נרצה להראות שייכות ל-RE (מכונה מקבלת) ולא ל-R (שפות מוכרות ב-RE)
אי שייכות ל-RE ולא ל-coRE - רדוקציה לשפה שלא שייכת לשניהם.

תורת הקבוצות וקומבינטוריקה

סימטרי: $L_1 \Delta L_2 = (L_1 \setminus L_2) \cup (L_2 \setminus L_1)$ | $L_1 \setminus L_2 = L_1 \cap \overline{L_2}$

דה מורגן 1: $L_1 \cup L_2 = \overline{\overline{L_1} \cap \overline{L_2}}$ | **דה מורגן 2:** $L_1 \cap L_2 = \overline{\overline{L_1} \cup \overline{L_2}}$

$|\Sigma^*| = \aleph_0$ - אינסופית | $\overline{L_1} = \Sigma^* \setminus L_1$

$L_1 = (L_1 \cup L_2) \setminus (L_2 \setminus (L_1 \cap L_2))$

$\binom{n}{k} = O(n^k)$ | $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

$\binom{n}{n-c} = O(n^c)$ - פולינומי (c הוא קבוע כמו "3") | $\binom{n}{n/2} = O(2^{n/2})$ - אקספוננציאלי.

תורת המספרים

- **מספר פְּרִיק** הוא מספר שלם חיובי שאפשר לכתוב אותו כמכפלה של שני שלמים גדולים מ-1.
- **מספר ראשוני** הוא מספר גבוה גדול מ-1, שלא ניתן להציגו כמכפלה של שני מספרים טבעיים קטנים ממנו, כלומר הוא מתחלק רק ב-1 ובעצמו.
- **מחלק משותף מקסימלי** $\gcd(a,b)$ של שני מספרים שלמים הוא המספר השלם הגדול ביותר שמחלק את שניהם ללא שארית. למשל, המחלק המשותף המרבי של 12 ו-18 הוא 6.
- **להשלים - להסביר פתרון למציאת ראשוני בביצרי: "לחלק בכל הראשוניים עד השורש"**
- **משפט בזו???**

שאלות על מחלקות סיבוכיות

טענה: $L \in NP$ **הוכחה:** אם $P \subseteq coNP$ אז לפי סגירות למשלים גם $\bar{L} \in P$. מאחר ו-$\bar{L} \in NP$ אזי $L = \bar{\bar{L}} \in coNP$ ומכאן **מ.ש.ל.**

משפט: אם $L_1 \in NPC$ וגם L_2 מקיימת את התכונות הבאות: **1)** $L_2 \in NP$ **2)** $L_1 \leq_p L_2$, כלומר L_1 ניתנת לרדוקציה עם L_2. אז גם $L_2 \in NPC$. **הוכחה:** נתון לנו כי $L_2 \in NP$, לכן אנחנו חייבים להראות לכל שפה $L' \in NP$ ניתנת לרדוקציה פולינומית עם L_2. מאחר ש: $L_1 \in NPC$, כל שפה $L' \in NP$ ניתנת לרדוקציה פולינומית $L' \leq_p L_1$, וגם נתון לנו כי $L_1 \leq_p L_2$. לכן, מאחר והיחס $\leq_p$ הוא טרנזיטיבי, אז כל $L' \in NP$ ניתנת לרדוקציה פולינומית עם L_1 וגם L_1 ניתנת לרדוקציה פולינומית עם L_2. לכן, כל שפה $L' \in NP$ ניתנת לרדוקציה פולינומית עם L_2 ומכאן $L_2 \in NPC$.

הוכח/הפרך: אם $P \neq NP$ ו-$NPC \cap NP = \emptyset$ **הוכחה:** יהי $L \in NPC$. הוכחנו כי $L \in NP$, ונותר להראות ש: $L \notin P$. יהי $L' \in NP$, אז, מאחר ש: $L \in NPC$, נובע ש: $L' \leq_p L$. מאחר ש: $L \in P$ ולפי משפט הרדוקציה, נקבל שגם $L' \in P$.

הוכח/הפרך: אם $NP \subseteq coNP$ אז $NP = coNP$. **הוכחה:** נראה ש: $coNP \subseteq NP$. יהי $L \in coNP$. אז $\bar{L} \in NP$ ומאחר ש: $NP \subseteq coNP$, נובע שגם $\bar{L} \in coNP$. לכן $L = \bar{\bar{L}} \in NP$.

שאלות שייכות ל-NPC

הרכבת פונקציות: נדגיר את השפה $COLOR = \{(<G>, k) \mid G \text{ can be colored with } k \text{ colors}\}$. הראו רדוקציה $CNF - SAT \leq_p COLOR$. **פתרון:** נסמן ב-h את פונקציית הרדוקציה של $CNF - SAT \leq_p 3_CNF_SAT$. נסמן ב-$g$ את פונקציית הרדוקציה של $3_CNF_SAT \leq_p 3COLOR$.
פונקציית הרדוקציה: $f(<\phi>) = (g(h(\phi)), 3)$. **תקפות: כיוון א':** $\phi \in CNF - SAT \Rightarrow f(<\phi>) \in 3COLOR$ ← מהתקפות של h ← $h(<\phi>) \in 3 - CNF - SAT$ ← לפי התקפות של g ← $g(h(<\phi>)) \in 3COLOR$. **כיוון ב':** $(g(h(<\phi>)), 3) \in COLOR \Rightarrow \phi \in CNF - SAT$ ← לפי התקפות של h נקבל כי $h(<\phi>) \in 3 - CNF - SAT$. **מ.ש.ל.**

כלל אצבע להוכחת NP לשפות עם OR ו-AND:
1. אם כתוב לנו $L = \{A \text{ OR } B\}$ זה נאלץ בה"כ את B להיות תמיד F ונעשה רדוקציה עם הקרוב אל A.
2. אם כתוב לנו $L = \{A \text{ AND } B\}$ זה נאלץ בה"כ את B להיות תמיד T ונעשה רדוקציה עם הקרוב אל A.

הוכחה: $HamOrClique = \{(G,k) \mid G \text{ has a Hamiltonian path or a Clique of size } k\} \in NPC$
פתרון: (להראות שייכות ל-NP). נראה עכשיו פתרון ל-HP. נראה רדוקציה $CLIQUE \leq_p HamOrClique$.
פונקציית הרדוקציה: $f(<G,k>) = (<G',k>)$. **הסבר:** אנחנו נראה שאם G לא קיימת קליקה אז G' לא קיימת קליקה ולא קיים מסלול המילטוני. כדי להבטיח את זה, נאלץ את G' לא להכיל אף פעם מסלול המילטוני - זאת בעזרת הוספת קודקוד חדש ובודד לגרף G'. <u>הפונקציה מלאה ניתנת לחישוב בזמן פולינומיאלי</u>: בניית G' על ידי העתקת גרף G עם תוספת קודקוד בודד אחד בזמן קבוע $O(1)$.
הקבוצה: $HamOrClique \leq_p CLIQUE$. **כיוון א':** $HamOrClique \in G,k \Rightarrow CLIQUE \in G,k$ ← קיים בגרף G קליקה בגודל k ← גרף G' הנתון של G עם קודקוד מבודד נוסף שלא פוגע בהגדרת הקליקה ← קיים ב-G' קליקה בגודל k ← $HamOrClique \in G',k \Rightarrow CLIQUE \in G',k$. **כיוון ב':** $CLIQUE \in G',k \Rightarrow HamOrClique \in G',k$ ← קיים בגרף G' קליקה בגודל k או מסלול המילטוני ← לא יתכן כי קיים מסלול המילטוני כי קיים קליקה מבודד ב-G' ולכן קיים רק קליקה בגודל k ← מאחר ו-G' הוא העתק של G אך עם קודקוד מבודד נוסף, בהסרת הקודקוד הזה נקבל את G ← קיים ב-G קליקה בגודל k ← $CLIQUE \in G,k \Rightarrow HamOrClique \in G,k$.

תרגיל: $ExactSubsetSum = \{(x_1,..,x_n), k, m \mid \exists I \subseteq [n] \text{ s.t. } \Sigma_{i \in I} x_i = k \wedge |I| = m\} \in NPC$.
פתרון: (להראות שייכות ל-NP). נראה עכשיו פתרון ל-NPH. נסמן $ESS = ExactSubsetSum$.
וגם נסמן $SS = SubsetSum$ נראה רדוקציה $ESS \leq_p SS$. **פונקציית הרדוקציה:**
תקפות: כיוון א': $ESS \in (<(x_1,...,x_n), k>) = (<(x_1,...,x_n,0,...,0), k, n>) = f(<(x_1,...,x_n), k>)$. הסבר: נרפד n אפסים בקבוצה הימנית. ← יש תת קבוצה המסתכמת ב-k, בגודל r כך ש: $r \leq n$ ← $(x_1,...,x_n), k \in SS$ ← אם נוסיף לקבוצה $n-r$ אפסים, נקבל קבוצה שעדיין מסתכמת ב-k ובגודלה את n. ← $(x_1,...,x_n,0,...,0), k, n \in ESS$. **כיוון ב':** $(x_1,...,x_n,0,...,0), k, n \in ESS \Rightarrow (x_1,...,x_n), k \in SS$ ← יש תת קבוצה המסתכמת ב-k ובגודלה הוא n ← אותה קבוצה בלי האפסים עדיין מסתכמת ב-k ← זו תהיה תת הקבוצה $(x_1,...,x_n), k \in SS \Rightarrow (x_1,...,x_n) \in ESS$.

הוכיחו: $SAT_2 = \{<\phi> \mid \exists \text{ two satisfying assignments to } \phi\} \in NPC$.
פתרון - חלק א': נוכיח $SAT_2 \in NP$. המכונה N_2 על קלט $<\phi>$ תפעל: **1)** נחש השמה π_1 ונחש השמה נוספת כאשר $\pi_2 \neq \pi_1$. **2)** בדוק ש-π_1 השמה מספקת, כלומר בדוק ש: $\phi(\pi_1) = true$. **3)** בדוק ש-π_2 השמה מספקת, כלומר בדוק ש: $\phi(\pi_2) = true$. **4)** אם π_1 וגם π_2 השמות מספקות עבור ϕ - קבל. אחרת, דחה. **סיבוכיות זמן הריצה:** נסמן ב-n את מספר המשתנים ב-ϕ. שלב 1: כגודל הניחוש, שה"כ $O(2n)$. שלב 2-3: בבדיקת ההשמה נצבע הצבה בפסוק, זה יקח לנו כגודל ϕ, כלומר $O(|\phi|)$. סה"כ $O(|\phi| + n)$ - פולינומי. **הוכחת נכונות בניית המכונה:** (להשלים).
פתרון - חלק ב': נוכיח ש-SAT_2 נוכיח הרדוקציה פולינומית $SAT_2 \leq_p SAT$.
פונקצית הרדוקציה: $f(\phi) = \phi' \wedge (y \vee \bar{y})$ כאשר ϕ' הוא אי-זהות. אין צורך לתאר את האלגוריתם מכיוון שהפונקציה מתארת היטב את הפעולה הנדרשת. הוכחת נכונות פונקצית הרדוקציה הפולינומית: **1)** הפונקציה f ניתנת לחישוב בזמן פולינומי, כי צריך בסה"כ להוסיף מחרוזת קבועה. **2)** תקפות הפונקציה: **כיוון א':** $\phi \in SAT \Rightarrow \phi' \in SAT$ ← קיימת השמה מספקת π לפסוק ϕ ← ההשמה $\pi_1 = \pi \cdot 0$ וגם $\pi_2 = \pi \cdot 1$ מספקות את ϕ' כיוון שקיימת בו פסוקית טאוטולוגית (תמיד נכונה) ← יש ל-ϕ' לפחות שתי השמות מספקות ← $\phi' \in SAT_2$. **כיוון ב':** $\phi' \in SAT_2 \Rightarrow \phi \in SAT$ ← קיימות שני השמות מספקות שונות π_1, π_2 לפסוק ϕ' ← נבחר בה"כ את ההשמה המספקת π_1 ← ההשמה π_1 בפרט מספקת את הפסוק ϕ ← $\phi \in SAT$.

נאמר על השמה שהיא מאוזנת אם מספר המשתנים שקיבלו T שווה למספר המשתנים שקיבלו F.
נתונה השפה: $BALANCED - SAT = \{\phi \mid \exists \text{ balanced satisfying assignments for } \phi\}$
הוכיחו: $BALANCED - SAT \in NPC$. **פתרון - שלב א':** נוכיח כי $BALANCED - SAT \in NP$.
נבנה N מ"ט אי"ד פולינומית המכריעה את השפה $BALANCED - SAT$. המכונה N על קלט $<\phi>$ תבצע: **1)** אם מספר המשתנים ב-ϕ הוא אי-זוגי - דחה. **2)** נחש השמה π. **3)** בדוק שההשמה מאוזנת - אם לא, דחה. **4)** בדוק שמתקיים $\phi(\pi) = true$. **5)** אם כן, קבל. אחרת, דחה. **סיבוכיות זמן הריצה:** (להשלים). **הוכחת נכונות הבניה:** (להשלים). **פתרון - שלב ב':** נוכיח כי $BALANCED - SAT \in NPH$ בעזרת רדוקציה $SAT \leq_p BALANCED - SAT$. **פונקצית הרדוקציה:** $f(<\phi>) = (<\phi>)$. כאשר ϕ פסוק רגיל ו-ϕ' פסוק עם מספר משתנים זוגי. **ביצוע:** נבנה את הפסוק ϕ' כך שהוא מכיל את הפסוק ϕ ויחד איתו מחוברים n פסוקיות (ב-AND) טאוטולוגיות (תמיד נכונות).
כלומר $\phi' = \phi \wedge (y_1 \vee \bar{y}_1) \wedge \ldots \wedge (y_n \vee \bar{y}_n)$. **הפונקצית פולינומית:** מוסיפים מספר קבוע של פסוקיות טאוטולוגיות - פולינומי. **הפונקצית תקפה:** להשלים.

משפט Cook-Levin

משפט קוק לוין: $SAT \in NPC$. כלומר, השפה SAT היא NP-שלמה. **רעיון ההוכחה:** צריך להוכיח שני דברים:
חלק 1) $SAT \in NP$. **חלק 2)** לכל שפה $L \in NP$ מתקיים ש: $L \leq_p SAT$.

הערות להוכחת חלק 2:
1. מטריצת tableau: נשתמש בטבלה הזאת (קונפסטואלית) כדי לייצר פסוק (לא כחלק מהבניה).
2. השורה הראשונה מתאימה לקונפיגוראציה ההתחלתית.
3. המטריצה תקרא מקבלת, אם אחת השורות שלה היא קונפיגוראציה מקבלת.
4. הרדוקציה תבנה m-ש פסוק שערכו יהיה $true$ אם"ם יש מטריצה מקבלת של N על w.
5. $tableau[i][j] == s$ אם"ם $x_{i,j,s} = true$ מתקיים ש: $s \in C$ ולכל סימן $1 \leq i,j \leq n^k + 1$.
6. הרדוקציה תבנה m-ש את הפסוק ϕ שהוא קוניונקציה (AND) של ארבעה פסוקים:
$\phi = \phi_{cell} \wedge \phi_{start} \wedge \phi_{move} \wedge \phi_{accept}$

- ϕ_{cell} - וידוא שבכל תא במטריצה יכול להיות בדיוק תו אחד מתוך C.
- ϕ_{start} - וידוא שהשורה הראשונה של המטריצה היא קונפיגוראציה ההתחלתית של N על w. בכל תא בשורה הראשונה במטריצה מופיע הסמל הנכון של הקונפיגוראציה ההתחלתית.
- ϕ_{move} - לוודא שכל שורה (קונפיגוראציה) מאפשרת לעבור לשורה הבאה (קונפיגוראציה הבאה) דרך פונקציית המעברים δ של N.
- ϕ_{accept} - בודק שהקונפיגוראציה הסופית הוא מקבל, יספיק לוודא מצב מקבל רק בשורה האחרונה.

<u>הערה עבור</u> ϕ_{move}: ההבדל בין שתי קונפיגוראציות עוקבות מתבטאת בלכל היותר בשלושה תאים רצופים (מיקום הראש, והתאים שלימינו ולשמאלו) וכל השאר זהה. לכן מספיק לוודא שכל "חלון" מסדר 2×3 הוא חוקי לפי N.
<u>טענה</u>: אם השורה הראשונה במטריצה היא הקונפיגוראציה ההתחלתית של N על w, וכל חלון מסדר 2×3 במטריצה הוא חלון חוקי לפי N, אז כל שורה בטבלה היא קונפיגוראציה עוקבת לקונפיגוראציה של השורה שלפניה, בחישוב של N על w.
<u>מסקנה</u>: הגודל של ϕ הוא $O(n^{2k})$ כלומר פולינומי ביחס לגודל הקלט.

שקיפות מחלקות (נגדיר מחלקות A, B כלשהן)

אם צ"ל $A \subseteq B$ אז תהי שפה $L \in A$ נראה ש-L שייכת גם ל-B כלומר $L \in B$. לשפה L יש מכונה M_A, נבנה מכונה M_B על x ובתוכה נסמלץ את M_A על x ונענה כמוה. בכך נקבל $L(M_B) = L$ ולכן $L \in B$.

דוגמה לשקילות מחלקות: עבור מ"ט אי"ד נגדיר:
$L_4(M) = \{x \in \Sigma^* \mid M \text{ has at least } 4 \text{ different accepting paths when running on } x\}$
זוהי שפת כל המילים ש-M מקבלת לפחות 4 מסלולים שונים. נגדיר את השפה הבאה: $NP_4 = \{L \mid There\ exists\ a\ non-deterministic\ polynomial\ time\ M\ s.t\ L_4(M) = L\}$.
הוכיחו: $NP_4 \leq_p NP$. **פתרון:** תהי $L \in NP_4$. צריך להוכיח כי $L \in NP$. מאחר ש $L \in NP$ ולכן קיימת M_L מ"ט אי"ד פולינומית המכריעה את השפה L. בניית המכונה: נבנה את M'_L מ"ט אי"ד חדשה. המכונה M'_L על קלט x תבצע: **1)** מריצה את M_L על x. **2)** אם דחתה - דחה. **3)** אם M_L קיבלה את x: **4)** מנחשת ביט. **5)** מנחשת ביט. **6)** מקבלת. <u>**סיבוכיות זמן הריצה**</u>: קל לראות ש: M'_L פולינומית. הרצה של M_L על x היא פולינומית כי $NP \in L$, ושאר הניחושים של M'_L הם בזמן קבוע. **הוכחת נכונות הבניה:** עבור שפה $L \in NP$ ושפה $L_{4,M'_L} \in NP_4$, נוכיח כי $L_{4,M'_L} = L$. **כיוון א':** $x \notin L \Rightarrow M_L \leftarrow x \notin L_{4,M'_L}$ תעצור ותדחה בכל מסלול חישוב (לפי הגדרה של מ"ט אי"ד מכריעה) ← M'_L תעצור ותדחה בכל מסלול חישוב ← $x \notin L_{4,M'_L}$. **כיוון ב':** $x \in L \Rightarrow$ קיים מסלול חישוב מקבל שבו M_L תעצור ותקבל ← ל- M'_L פולינומית. הרצה של M_L על x היא פולינומית כי L_{4,M'_L}, ← 00,01,10,11 ← $x \in L_{4,M'_L}$ ← הנחכנו כי $L_{4,M'_L} = L$ ומאחר ו-$L_{4,M'_L} \in NP_4$ אז גם $L \in NP_4$. ומכאן $NP \subseteq NP_4$ כנדרש.

הוכחת שקילות מודלים

שאלה ממטלה 2: מ"ט דטר' לעומת מ"ט אי"ד בה מילה מתקבלת אך ורק אם קיימים לפחות שני מסלולים מקבלים. **פתרון: כיוון 1:** בהיגתן מכונה מהמודל החדש, נראה מכונה דטרמיניסטית שקולה. המכונה הדטרמיניסטית תקבל קלט x ותסמלץ את המכונה מהמודל החדש ע"י סריקת BFS של עץ הבחירות האי דטרמיניסטיות בדומה להוכחת השקילות של המכונה הדטרמיניסטית לאי דטרמיניסטית הרגילה. ברגע שמצאנו לפחות 2 מסלולים המסתיימים בקבלה - נקבל. אם המסתיימה סריקת כל המסלולים ומצאנו לכל היותר מסלול אחד מקבל - נדחה. **כיוון 2:** בהיגתן מכונה מהמודל הדטרמיניסטי הרגיל, נראה מכונה שקולה מהמודל החדש. המכונה תקבל קלט x, תגריל ביט (0 או 1), אם יצא 0 היא תקבל ואם יצא 1 אז היא תסמלץ את ריצת המכונה הדטרמיניסטית שלה ע"י ותענה בהתאם וכך קיבלנו שאם המכונה המקורית קיבלה את ישנם 2 מסלולי חישוב מקבלים עבור x במודל החדש ואחרת יהיה רק מסלול חישוב אחד מקבל.

סיבוכיות זמן ריצה

אלגוריתם חיפוש BFS (למשל עבור מסלול קצר ביותר) עם מטר' שכנויות בזמן ולכן $O(n^2)$ בזמן.
במ"ט אי"ד עבור NP, גודל ניחוש של קבוצה בגודל k הוא $O(k \log(n))$ כאשר $\log(n)$ הוא עבור קידוד מספר לביצרי כאשר המספר הוא בין 1 ל-n.

עבור כל שפה שהקלט שלה הוא קידוד של מספר $< n >$, זמן הריצה צריך להיות פולינומיאלי בכמות הספרות המייצגות את המספר n. נשים לב ש: $|< n >| = \log(n)$ ולכן נתעניין כאן במ"ט שרצות בזמן פולינומי ב-$\log(n)$.

סגירות ל-NP - דוגמה לשרשור

טענה: אם $L_1, L_2 \in NP$ אזי גם $L_1 \cdot L_2 \in NP$. **הוכחה:** מכיוון ש: $L_1, L_2 \in NP$ אזי קיימות להן מ"ט אי"ד פולינומיות מכריעות M_1, M_2. נבנה את M' מ"ט אי"ד פולינומית המכריעה את השפה $L_1 \cdot L_2$. המכונה M' על קלט x תבצע: **1.** תנחש פירוק של x מהצורה $x = wu$. **2.** תסמלץ את M_1 על w. **3.** תסמלץ את M_2 על u. **4.** אם שתיהן קיבלו, <u>קבל</u>. אחרת, אם לפחות אחת מהן דחתה, <u>דחה</u>. **הוכחת נכונות הבניה:** נוכיח כי $L_1 \cdot L_2 = L(M')$. **כיוון א':** $L_1 \cdot L_2 \Rightarrow x \in L_1 \cdot L_2 \Rightarrow$ קיים פירוק $x = wu$ כך ש: $w \in L_1 \wedge u \in L_2$ ← כזה $M_1(w) = 1 \wedge M_2(u) = 1$ ← תקבל $x \in L(M') \Rightarrow M'$ ← לכל פירוק $x = wu$ כך ש: $w \notin L_1 \vee u \notin L_2$ ← לכל ניחוש, $M_1(w) = 0 \vee M_2(u) = 0$ ← תדחה $x \notin L(M')$. **סיבוכיות:** המכונות M_1, M_2 פולינומיות ולכן גם M' פולינומית.

דוגמה לשימוש במשפט רייס

דוגמה: $L_3 = \{<M>: L(M) \in coRE\}$ **1) הגדרת החתכה:** נגדיר את $S = \{L \in RE: L \in coRE\}$
ומכאן: $L_3 = S_3$. **2) הוכחת אי טריוויאליות:** נוכיח ש S אינה טריוויאלית: $L_u \notin S$ כי $L_u \in RE \backslash coRE$ ולכן $S \neq RE$. מצד שני, S כי $L \in RE \cap coRE$ ולכן: $\Phi \neq S$. לכן S אינה טריוויאלית.
3) מסקנה: ולכן לפי משפט רייס, $L_3 \notin R$.

דוגמה: $L_1 = \{<M>: |L(M)| > 10\}$ **1) הגדרת החתכה:** נגדיר את $S = \{L \in RE: |L| > 10\}$
ומכאן: $L_1 = S_1$. **2) הוכחת אי טריוויאליות:** נוכיח ש S אינה טריוויאלית: $S \notin$ כי $|\Phi| = 0 \leq 10$ ולכן $S \neq RE$. מצד שני, S כי $L = \{0, 0^2, ..., 0^{11}\} \in RE$ ולכן S אינה טריוויאלית.
3) מסקנה: לכן לפי משפט רייס, $L_1 \notin R$.

תרגיל: בשאלה זו נוכיח מקרה פרטי של משפט רייס. תהי S תכונת השפות: $S = \{L \mid \Sigma^{107} \subseteq L\}$.
ותהי: $L_s = \{<M> \mid L(M) \in S\}$ **a)** הוכיחו כי $L_s \in RE$ **b)** הוכיחו כי $L_s \notin R$.
הוכיחו כי $L_s \notin R$. (יש להוכיח את משפט רייס, לא להשתמש בו). **פתרון:** **a)** אלגוריתם: על קלט $<M>$:
1) עבור על כל המילים $w \in \Sigma^{107}$ **1.1)** הרץ את M על w. אם דחתה - דחה. **2)** קבל. **נכונות:** (להשלים).
פתרון ב: נראה רדוקציה: $HP \leq_s L_s$ ע"י: $f(<M, w>) =<M'>$ כאשר: **1)** על קלט x: **1)** הרץ את M על w. ואז **2)** $|x|$ קבל. **3)** אחרת - דחה. **תקפות:** (להשלים).

בעיות חיפוש מול בעיות הכרעה

בשאלות מהסגנון הזה נותנים לנו נתון שידוע פתרון פולינומי <u>דטרמיניסטי</u> לבעיית ההכרעה וצריך למצוא פתרון לבעיית החיפוש (להחזיר את הפתרון עצמו ולא רק כן או לא)
סד"י=: בדרך כלל מסמנים את המכונה המכריעה הקיימת ב-M.
באלגוריתם החיפוש A שמקבל קלט $Object$:
1. תחילה מריצים את M על כל הקלט ואם היא דחתה אז מחזירים ש-"אין פתרון".
2. אם היא קיבלה, מנסים למצוא את מרכיבי הפתרון ע"י מעבר אינרטיבי אלמנט אחרי אלמנט ובדיקה (ע"י קריאה שוב ושוב למכונה M עבור הקלט ללא המרכיב שבודקים) האם הוא שייך לפתרון או להיפך. אם כן - נשמור אותו, אחרת - נזרוק אותו.
3. לבסוף, נחזיר את הפתרון.

- HC - לכל צלע e, בדוק האם ב-$G \backslash \{e\}$ יש עדיין מעגל המילטוני אז $G = G'$ אחרת $G = G$.
- DHC - לכל צלע e, בדוק האם ב-$G \backslash \{e\}$ יש עדיין מעגל המילטוני אז $G = G'$ אחרת $G = G$.
- HP - לכל צלע e, בדוק האם ב-$G \backslash \{e\}$ יש עדיין מסלול המילטוני אז $G = G'$ אחרת $G = G$.
- IS - לכל קודקוד v, בדוק האם ב-$G \backslash \{v\}$ יש עדיין קבוצה ב"ת, אם כן $G = G'$ אחרת $G = G$.
- $CLIQUE$ - לכל קודקוד v, בדוק האם ב-$G \backslash \{v\}$ יש קליקה אם כן אז $G = G'$ אחרת $G = G$.
- VC - לכל קודקוד v, בדוק האם ב-$G \backslash \{v\}$ יש כיסוי קודקודים בגודל $k - 1$, אם לא אז $G = G'$ אם כן, אז $G = G$.

דוגמה עבור מציאת קליקה מקסימלית: נניח ש: $P = NP$. תארו אלגוריתם (יעיל) עבור מציאת קליקה מקסימלית. אין צורך להוכיח את נכונות האלגוריתם. כיוון ש: $CLIQUE \in NP$ לפי ההנחה $CLIQUE \in P$. יהי A אלגוריתם יעיל אלגוריתם שמכריע את $CLIQUE$. **אלגוריתם ראשון:** נבנה קודם כל אלגוריתם עבור מציאת קליקה בגודל נתון k בגרף. B על קלט $<G, k>$ תבצע: **1)** נריץ את $A(G, k)$. אם דחה, נחזיר "אין פתרון". **2)** עבור כל קודקוד v בגרף: **2a)** נריץ את B מהגרף ונקבל גרף חדש G'. **2b)** נריץ את $A(G')$. אם קיבל, $G' = G$ ומשיך לקודקוד הבא. **2c)** אם דחה, נמשיך לקודקוד הבא עם G. **3)** נחזיר את הקודקודים שנשארו. **אלגוריתם שני:** כעת נתאר אלגוריתם עבור מציאת קליקה מקסימלית. C על קלט $<G>$ **1:** עבור $i = 0$ עד i אינסופי: **1a)** נריץ את $A(G, i)$. **1b)** אם קיבל, $++i$. **1c)** אם דחה, נריץ את $B(G, i - 1)$ **1d)** נחזיר את הפתרון שהתקבל.

דוגמה עבור בוקבוצה ב"ת: ניח ש: $P = NP$. תארו במילים מימוש של מ"ט דטר' פולינומית שבהינתן קלט $<G, k>$ מחזירה קבוצה ב"ת ב-G שגודלה k, או מחזירה "לא קיים" אם לא קיים כזאת. אין צורך להוכיח נכונות, אך חשבו את סיבוכיות זמן של המכונה. **פתרון:** לפי ההנחה ש $P = NP$, קיימת מ"ט דטר' פולינומית M_{IS} העובדת בזמן $O(p(n))$ המכריעה את IS. נראה את האלגוריתם המבוקש: על קלט $<G, k>$ כאשר G - גרף, k - מספר שלם חיובי: **1)** הרץ את M_{IS} על $<G, k>$. אם דחתה - החזר "לא קיים". **2)** עבור $v \in V(G)$ **2a:** הורד את v ואת הצלעות המחוברות אליו ב G ושמור את הגרף המתקבל ב H. **2b)** הרץ את M_{IS} על $<H, k>$ **2c)** אם קיבלה את קבע את G ל הנשוא H (המשך ללא ש קודקוד).
2c) אם דחתה, החזר את v (המשך בכל מי שהיה). **3)** החזר את קודקודי G שנשארו. **סיבוכיות:** נסמן ב n את גודל הקלט. **1.** הרצת M_{IS} בפעם הראשונה: $O(p(N))$. **2.** לולאה ראשית מבצעת $O(n)$ איטרציות כאשר $N \leq n$ מייצג את כמות הקודקודים. **3.** בכל איטרציה, מורידים קודקוד בסיבוכיות $O(N)$ ואז מרצים שוב את M_{IS} על הגרף הנותר בזמן $O(p(N))$. **4.** לבסוף עוברים על מה שנשאר ומחזירים את הקודקודים הנותרים: $O(N)$. **סה"כ:** $O(p(N) + N) + n(N + p(N))$ החסום ב $O(Np(N) + N^2)$ פולינומי בגודל הקלט.

בעיית חיפוש מסלול המילוטן: האלגוריתם: על קלט $<G>$ **1)** הרץ את $M_{HamPath}$ על $<G>$.
אם דחתה - החזר "לא קיים מסלול המילוטני" **2)** עבור $e \in E(G)$ **2a:** הורד את הצלע e מהגרף וסמן ב H את הגרף המתקבל. **2b)** הרץ את $M_{HamPath}$ על $<H>$ **2c.** אם דחתה - החזר את e לגרף. **2d)** אם קיבלה - קבע $G = H$ (המשך עם H במקום G, ללא הצלע) **3)** סרוק את הגרף הנותר ומצא את אחד הקצוות של המסלול. **4)** בצע מעבר על המסלול והחזר את סדרת הקודקודים המתקבלת.

בעיית חיפוש PARTITION: מכיוון ש: $P = NP$ אזי $SubsetSetSum \in NP$ כי $SubsetSum \in NP$ ומכאן: קיימת מ"ט דטרמיניסטית פולינומית M_{SS} המכריעה את $SubsetSetSum$ וגם קיימת מ"ט דטרמיניסטית פולינומית M_p המכריעה את $PARTITION$. נגדיר את המכונה היעילה הבאה $SearchPartition$ המוצאת את הקבוצה עבור $PARTITION$: האלגוריתם $SearchPartition$ על קלט $S = (x_1, x_2, ..., x_n)$ תבצע: **1)** הרץ את M_p על S $<.$ אם דחתה - החזר "לא קיים". **2)** סכום $sum = \Sigma_{x \in S} x$ (סכום כל הקבוצה S). **3)** צור קבוצה ריקה $S' =$ **4)** הגדר $k = sum/2$ **4.1)** עבור כל i 1-ו עד n בצע: **4.1)** הרץ את M_{SS} על $(x_{i+1}, x_{i+2}, ..., x_n, k - x_i)$. **4.1.1)** עבור כל i 1-ו עד n בצע: **4.1.1)** הוסף את x_i ל-S' והגדר $k = k - x_i$ **4.1.1.2)** אם $k = 0$ החזר את S' הקבוצות S, S'. **להשלים:** (הוכחת נכונות וסיבוכיות בזמן פולינומי).

בעיית חיפוש SUBSET-SUM: מכיוון ש: $P = NP$ אזי $SubsetSum \in NP$ כי $SubsetSum \in P$.
מכאן: קיימת מ"ט דטרמיניסטית פולינומית M_{SS} המכריעה את $SubsetSum$. נגדיר את המכונה היעילה הבאה המוצאת את תת הקבוצה: M על הקלט $(x_1, x_2, ..., x_n, k)$ כאשר $x_1, x_2, ..., x_n$ הם מספרים שלמים. **1)** הרץ את M_{SS} על $(x_1, x_2, ..., x_n, k)$. אם דחתה - החזר "לא קיים". **2)** הגדר: $I = \emptyset$ (קבוצת אינדקסים). **3)** אם $k = 0$ החזר את I. **4)** עבור i 1-ו עד t בצע: **4.1)** הרץ את M_{SS} על $(x_{i+1}, x_{i+2}, ..., x_n, k - x_i)$. **4.1.1)** אם ענתה כן, **4.1.1.1)** הוסף את i ל-I והגדר $k = k - x_i$ **4.1.1.2)** אם $k = 0$ החזר את I.

<u>**כיסוי קודקודים (החזרת מספר כ קטן ביותר)**</u>: מהו הגודל **המינימלי k** הדרוש לכיסוי קודקודים לגרף נתון? **פתרון:** נניח ש $P = NP$ ומכאן קיימת מ"ט דטרמיניסטית פולינומית M_{VC} המכריעה את VC בזמן פולינומי. האלגוריתם: על קלט $<G>$ **1:** עבור k מ 1 עד $|V|$: **1.1:** הרץ את $M_{VC}(<G, k>)$ אם קיבלה - החזר את k (בצורת מספר). **2)** החזר $|V|$. **סיבוכיות:** פולינומית: $O(|V| \cdot p(|<G, |V|>|))$ כאשר p הוא הפולינום של זמן הריצה של M_{VC}.

בעיית חיפוש CNF-SAT: מכיוון ש: $P = NP$ אזי $SAT \in NP$ כי $SAT \in P$. מכאן: קיימת מ"ט דטרמיניסטית פולינומית M_{SAT} המכריעה את SAT. נגדיר את המכונה היעילה הבאה המוצאת את ההשמה: המכונה M על קלט ϕ כאשר ϕ היא נוסחת CNF תבצע: **1)** הגדר π להיות כמות המשתנים ב-ϕ **2)** הרץ את M_{SAT} על ϕ. אם דחתה - החזר "לא קיים". **3)** הגדר $z = \pi$. **4)** עבור i מ-1 ועד π תבצע: **4.1)** הגדר ϕ_0 - אותה הנוסחה ϕ עם השמה $x_i = 0$. **4.2)** הגדר ϕ_1 - אותה הנוסחה ϕ עם השמה $x_i = 1$. **4.3)** הרץ את M_{SAT} על ϕ_0. **4.3.1)** אם קיבלה: הגדר ϕ_0 ← ϕ ושרשר את 0 ל-z: $z0$. **4.3.2)** אחרת: הגדר ϕ_1 ← ϕ ושרשר את 1 ל-z: $z1$. **5.2)** החזר את z. **להשלים:** (נכונות וסיבוכיות).

<u>**כיסוי קודקודים (לא פורמלי)**</u>: **1)** בדוק $M(<G, k>)$. אם דחה, החזר "לא קיים". **2)** צור קבוצה ריקה $H = \{\}$ **3)** עבור $v \in V$ בצע: **3.1)** הורד $G' = G \backslash \{v\}$ **3.2)** בדוק $M(G', i - 1)$ **3.3)** אם קיבל, אז $G = G'$ ומוסיף $H = H \cup \{v\}$ **3.4)** אם $G = G'$ אם דחה, המשך לקודקוד הבא. **4)** החזר את H.

שאלות שייכות NP

תרגיל 1: הוכיחו: $SP = \{(<G>, k) \m

שאלות שייכות ל-NPC

תרגיל: $L = \{(G,5k) \mid G \text{ has a VC of size } 5k, \text{ and } k \in N\} \in NPC$. **פתרון:** (להשלים עבור NP), נראה גם ש: $L \in NPH$: בעזרת הרדוקציה $VC \leq_p L$. נבנה את הגרף החדש G' כך: $G' = G \cup G \cup G \cup G \cup G$. **סיבוכיות:** בנית G' הוא פולינומי $O(n^5)$. **תקפות:** (להשלים).

תרגיל: $L = \{<G,k> \mid <G,k> \in CLIQUE \text{ and } k \leq |V(G)|/3\} \in NPC$. **פתרון:** (להשלים עבור NP). נראה גם ש: $L \in NPH$ נראה רדוקציה $CLIQUE \leq_p L$. כך: $f(<G,k>) = <G',k'>$.
נראה פונקציה מפוצלת: **1)** $k' = |V(G)|/3$ ו $G' = G$ אז $k \leq |V(G)|/3$ ו **2)** $k' = |V(G)|/3$ אז נבנה את G' להיות G בתוספת $2 \cdot |V(G)|$ קודקודים חדשים ומבודדים. וגם $k' = k$. **סיבוכיות ותקפות**-להשלים.

תרגיל: $L = \{<G,k> \mid G \text{ has an odd number of vertices OR } G \text{ contains a Clique of } k\} \in NPC$. **פתרון:** (להשלים שייכות ל-NP). נראה שייכות ל-NPH: נראה רדוקציה $CLIQUE \leq_p L$ ע"י: $f(<G,k>) = <G',k'>$ כאשר: **1)** $G' = G$ אם יש ב G כמות קודקודים זוגית. **2)** G' יהיה G עם תוספת קודקוד בודד ש G בכמות קודקודים אי זוגית. **סיבוכיות ותקפות** - להשלים.

תרגיל: $L = \{(G,k) \mid G \text{ has two disjoint Cliques } C_1 \text{ of } k \text{ and } C_2 \text{ of } 2k. \text{ and } |V| \geq 3k+10\} \in NPC$. **פתרון:** (להשלים שייכות ל-NP). שייכות ל-NPH: נראה רדוקציה: $CLIQUE \leq_p L$ ע"י: $f(<G,k>) = <G',k'>$ כאשר: G' יכיל את G, רכיב נוסף שהוא קליקה בגודל $2k$ ועוד 10 קודקודים בודדים. $k' = k$. **תקפות-להוכיח ע"י:** **1)** אם יש קליקה בגודל k אז ב G קליקה k קודקודים ולכן ב G' יהיו לפחות $2k + 10 = 3k + 10$ קודקודים. בנוסף, ב G' תהיה קליקה בגודל k ו G' ועוד קליקה בגודל $2k$ (מה שהוספנו) ולכן: $<G',k'> \in L_1$. **כיוון ב':** אם ב G אין קליקה בגודל k אז ב G' תהיה רק קליקה אחת בגודל $2k$ ולכן $<G',k'> \notin L_1$. **סיבוכיות:** (להשלים).

הכיוון - $L = \{\phi \mid \phi \text{ is a CNF that has at least 7 satisfiable assignments}\} \in NPC$.
פתרון: השפה שייכת ל NPC. שייכות ל NP: ע"י מ"ט אי"ד: על קלט ϕ :1) נחש ל השמות למשתני הנוסחה: $z_1, z_2, ..., z_7$ **2)** בדוק שכל 7 מהן שונות זו מזו. אם לא - דחה. **3)** הצב כל אחת מההשמות בנוסחא ובדוק האם היא מתקיימת, אם לא - דחה. **4)** קבל. **סיבוכיות:** גודל כל השמה הוא $O(n)$ - וקטור של n ערכי אמת. ולכן סה"כ נקבל שהאורך הכולל של כל ההשמות יחד הוא: $O(n)$. בדיקה שההשמות שונות: $O(n^2)$.
בדיקה שכל אחת מההשמות מספקת את כל הנוסחא: $O(n)$. סה"כ: $O(N^2)$ - פולינומי בגודל הקלט.
נכונות: אם $\phi \in L_1$ אז קיים ניחוש בו נחשש את 7 ההשמות המספקות הנ"ל (השונות), נציב, נבדוק ונקבל. אם $\phi \notin L_1$ אז לא קיימות 7 השמות מספקות ולכן לכל ניחוש שנמצא בהכרח יייתכן לפחות השמה אחת שאינה מספקת ולכן נדחה. **הוכחת קושי:** ע"י רדוקציה: $SAT \leq L_1$ ע"י:
$f(<\phi>) = <\phi \wedge (y_1 \vee y_2 \vee y_3) \wedge (y_1 \vee y_2 \vee y_3) \wedge (y_1 \vee y_2 \vee y_3)>$ כאשר: ϕ (נוסחת CNF תקינה) **סיבוכיות:** התעתקת הנוסחא + תוספת של פסוקים אחת. סה"כ: $O(n)$. **תקפות:** לפסוקית $(y_1 \vee y_2 \vee y_3)$ יש 7 השמות מספקות (כל קומבינציה חוץ מ FFF) ולכן אם לפ ϕ הייתה לפחות השמה אחת מספקת אזי ל ϕ יהיו לפחות 7 השמות מספקות, ואם ל ϕ אין השמה מספקת אז גם ל ϕ אין השמה מספקת.

הוכיחו: אם $L = \{x \cdot 1^{|x|} \mid x \in IS\} \leq_p \{x \cdot 1^{|x|} \mid x \in IS\} \in P$. **פתרון:** נראה ש: $P = NP$ אזי $NP \leq_p L$. ומכיוון שנתון: $L = \{x \cdot 1^{|x|} \mid x \in IS\} \leq_p \{x \cdot 1^{|x|} \mid x \in IS\} \in P$ ולפי משפט: אם יש שפה ב-P שהיא NPC אזי $P = NP$ נובעת הטענה. בעזרת את המכונה הדטר' הבאה המכריעה את $\{x \cdot 1^{|x|} \mid x \in IS\}$:
המכונה M על קלט w כאשר w מהצורה: $w = x \cdot 1^{|x|}$. ובדוק שהיא אכן $1^{|x|}$. **2)** הגדר: $<G,k> =: x$. **3)** עבור על כל תתי הקבוצות של קודקודים בגודל k מתוך n קודקודי הגרף: **3.1)** בדוק עבור כל זוג קודקודים בקבוצה שהם אינם מחוברים בצלע. **3.2)** אם נמצאו שניים מחוברים - המשך לתת הקבוצה הבאה. **3.3)** אחרת - קבל. **ניתנת לחישוב זמן פולינומי:** חישוב $|x|$ הוא $O(2^{|x|})$ הנראה אקספוננציאלי בגודל x אבל פולינומי בגודל הקלט כי גודל הקלט הוא $|x \cdot 2^{|x|}|$. כמות תתי הקבוצות היא לכל היותר $O(2^n)$ ובדיקה בין כל שניים שיש צלע: $n^2 = O(n^2)$. סה"כ פולינומי בגודל הקלט. **נכונות:** (השלימו).

הוכיחו: $L = \{<G,k> \mid G \text{ contains a Clique of size } k \text{ OR an IS of size } k\} \in NPC$.
הוכחה: להראות ש $L \in NPH$. נוכיח ב $L \in NPC$ נראה $IS \leq_p L$ ע"י
$f(<G,k>) = <G',n+k>$ כאשר G' מוגדר באופן הבא: ניקח את הגרף G ונוסיף לו n קודקודים בודדים. כעת, לא תיתכן קליקה בגרף בגודל $n+k$ כי הקודקודים שהוספנו לא מחוברים לאף קודקוד אחר ולכן לא יכולים להצרף לקליקה גדולה ולכן הקליקה הגדולה ביותר שיכולה להיות היא בגודל k. מאידך, אם קיימת קבוצה ב"ת ב-G בגודל k אזי n הקודקודים שהוספנו מצטרפים ומיצרים ביחד קבוצה ב"ת בגרף G' בגודל $n+k$. הרדוקציה מלאה וניתנת לחישוב זמן פולינומי: .... **תקפות:** .....

שאלות כלליות מבמבנים ותרגולים

בהינתן מכונת טיורינג אי-דטרמיניסטית M, נגדיר: המכונה ההופכית של M, הינה מכונה זהה בפעולתה לפעולת M, למעט החלפת המצב המקבל והמצב דהודחה אחד בשני. נסמן את המכונה ההופכית ב-$M_{inverse}$.
סעיף א': מוכיחו אם הפריכו: $L(M) = L(M_{inverse})$ (השפה ההופכית של שפת המכונה M, שווה לשפת המכונה ההופכית). **סעיף ב':** האם קיימת מכונה M, כך שמתקיים: $L(M) = L(M_{inverse})$? אם כן, תנו דוגמא, אם לא, הוכיחו. **פתרון א':** הפרכה: ניקח מכונה M שלא עוצרת על אף קלט. מכאן: $L(M) = \Phi$. $L(M_{inverse}) = \Phi$. וזו הפרכה כי $L(\bar{M}) = \Sigma^*$. **פתרון ב':** כן. ניקח מכונה M שלא עוצרת על אף קלט. מכאן: $L(M) = \Phi$. $L(M_{inverse}) = \Phi$.

נתונה השפה:
$L_{logn} = \{\phi \mid \phi \text{ has a satisfying assignment } \pi, \text{ and } \exists i \text{ s.t. } \forall_{j \in \{i+1, i+2, ..., i+\log n\}} \pi(x_j) = T\}$
בשפת בני אנוש: קיימת ל-ϕ השמה מספקת, כך שכל המשתנים מקבלים T חוץ מרצף של $\log(n)$ משתנים שיכולים לקבל מה שבא להם T או F. **הסבר לפתרון:** אם יש לנו $\log_2(n)$ משתנים שאפשר לשחק איתם איך שבא לנו, אז יש לנו $2^{\log_2(n)}$ אופציות, כי לכל אחד מה-$\log_2(n)$-ים יש 2 אפשרויות: $\{T,F\}$. בדרך כלל אמרנו שאנחנו לא יכולים לבדוק השמה מספקת כי יש לנו לעבור על 2^n אופציות שזה אקספוננציאלי, אבל עכשיו יש לנו $2^{\log_2(n)}$ אופציות, ולפי חוקי לוג $n = a^{\log_a(n)}$ בלומר יש לנו n אופציות וזה אכן פולינומי!. לכן, $L_{logn} \in P$.
פתרון: $L_{logn} \in P$. נבנה מ"ט דטרמיניסטית מכריעה עבור L_{logn}. M על קלט ϕ תבצע: **1)** עבור $i = 1 \leq i \leq n - \log(n)$ **1.1)** אם ההשמה הנוכחית + כל שאר המשתנים קיבלו T - קבל. **1.2)** דחה. סיבוכיות זמן ריצה: עבור כל i, **1.1.1)** אם ההשמה האפשרית הוא n $2^{\log(n)} =$ סה"כ נבדוק $O(n \cdot n)$ השמות ← בדיקה של השמה אחת $O(n)$ ← זמן הריצה של המכונה הוא $O(n^3)$ - פולינומי. נכונות הבניה: נובעת ישירות מהבנייה.

הגדרה: השפה $NAE - Not\ All\ Equal - SAT$ (כאשר $NAE - K - CNF - SAT$ זוהי שפה של פסוקיות $CNF - K$, אך לכל השמה מספקת, אבל בכל פסוקית יש ליטרל שמקבל F.
תרגיל: הוכיח ש: $NAE - 3 - CNF - SAT \in NPC$.
פתרון: תחילה נוכיח ה $NAE - 3 - CNF - SAT \in NPH$. נבנה מ"ט אי"ד N שתכריע את השפה $NAE - 3 - CNF - SAT$. המכונה M על קלט ϕ :1) נחש לה ϕ פסוקן, תבצע: **1)** תנחש את ה. **2)** בדוק השמה זו על ϕ: **2.1)** לכל פסוקית ϕ p בצע השמה זו ובדוק שאכן קיים ליטרל אחד שהוא F - אחרת, דחה. **3)** אם ה מספקת אם אז קבל. אחרת - דחה. המכונה ניתנת לחישוב זמן פולינומי: גודל הניחוש $O(|\pi|)$, בדיקת השמה היא $O(|\phi|)$ ולכן פולינומי. נכונות הבנייה: ...
כעת נותר להראות ש $NAE - 3 - CNF - SAT \in NPH$ על ידי שתי רדוקציות:
$3 - CNF - SAT \leq_p NAE - 3 - CNF - SAT \leq_p NAE - 4 - CNF - SAT$
רדוקיה ראשונה: $3 - CNF - SAT \leq_p NAE - 4 - CNF - SAT$. נגדיר פונקציה כלשהי g שמקבלת פסוקית $\varphi_i = (x \vee y \vee y \vee z)$ ומרחיבה אותה במשנה החדש w. כלומר: לכל פסוקית φ_i, נגדיר משתנה חדש w בצורה הבאה: $g(x \vee y \vee z) = (x \vee y \vee z \vee w)$. אבחנה: אם השמה π היא NAE ומספקת, אז גם $\bar{\pi}$ היא NAE ומספקת. מספקת הרדוקציה: $f(\phi) = \phi'$ כך ש:
$\phi' = \bigwedge_{m=1}^{m} g(\varphi_m)$ לכל φ_m ... $\wedge \bigwedge_{1}^{m} g(\varphi_1)$.
הפוקציה ניתנת לחישוב זמן פולינומי: להוסיף כמות קבועה של משתנה חדש $O(1)$. הפונקציה תקפה: ....
רדוקיה שניה: $NAE - 3 - CNF - SAT \leq_p NAE - 4 - CNF - SAT$. נפעל בדומה להרחבות שעשינו לרדוקציה של $CNF - SAT \leq_p 3 - CNF - SAT$. נגדיר פונקציה כלשהי g שמקבלת פסוקית $\varphi_i = (x_1 \vee x_2 \vee x_3 \vee x_4)$ ומפרקת אותה בעזרת המשנה החדש w, לצורה של $3CNF$. כלומר: לכל פסוקית φ_i, נגדיר משתנה חדש w: $g(x_1 \vee x_2 \vee x_3 \vee x_4) = (x_1 \vee x_2 \vee w_i) \wedge (\bar{w}_i \vee x_3 \vee x_4)$
פונקצית הרדוקציה: $f(\phi) = \phi'$ כך ש $\phi' = \bigwedge_{m=1}^{m} g(\varphi_m)$ לכל φ_m ... $\wedge \bigwedge_{1}^{m} g(\varphi_1)$.
הפוקציה ניתנת לחישוב זמן פולינומי: להוסיף כמות קבועה של משתנה חדש $O(1)$ ולפצל לפסוקיות. הפונקציה תקפה: ....

שאלות שייכות ל-RE,R,CORE

תרגיל - $L_1 = \{<M> \mid M \text{ stops to every input after more than } 42 \text{ steps}\} \in \overline{coRE} \cup \overline{RE}$. לא ניתן להשתמש במשפט רייס מכיוון שהתכונה היא לא של שפות מכונות.
פתרון: הפיוזה: $\overline{HP} \leq_p L_1$ ו $HP \leq_p L_1$ נתחיל עם $\overline{HP} \leq_p L_1$: פונקצית הרדוקציה:
נוכיח ב-2 רדוקציות $f(<M,x>) = <M'>$ כאשר: M' על קלט w תבצע: **1)** ממלץ את M על x. **2)** רוץ 42 צעדים ואז קבל.
נכונות פונקצית הרדוקציה: **1)** הפונקציה מלאה - מוגדרת לכל קלט, M, x קיים M'. **2)** הפונקציה ניתנת לחישוב - פעולת קומפיליצה פשוטה, לכל מ"ט קיים קידוד. **3)** הפונקציה תקפה - להשלים.
רדוקיה שנייה $HP \leq_p L_1$: פונקצית הרדוקציה: $f(<M,x>) = <M'>$. M' על קלט w תבצע: **1)** ממלץ את M על x למשך $|w|$ צעדים. **2)** אם M עצרה - רוץ לאינסוף. **3)** אם לא עצרה - רוץ 42 צעדים ואז קבל.
נכונות פונקצית הרדוקציה: **1)** הפונקציה מלאה - מוגדרת לכל קלט, M, x קיים M'. **2)** הפונקציה ניתנת לחישוב - פעולת קומפיליצה פשוטה, לכל מ"ט קיים קידוד. **3)** הפונקציה תקפה - להשלים.

- כדי להוכיח שייכות ל-$coRE$ אפשר לתאר מ"ט לשפה המשלימה $\bar{L} \in RE$.

תרגיל: נתונה השפה: $COMPOSITE = \{n \mid n \text{ is composite}\}$. הוכיחו: $COMPOSITE \in R$.
פתרון: נתאר מ"ט אי"ד M המכריעה את השפה $COMPOSITE$. אלגוריתם: M על קלט n (או שניתן לסמן $M(n)$) תבצע: **1)** נחש מספר k כך ש: $1 < k < n$ **2)** אם $k\%n == 0$ אז M תקבל. **3)** אחרת - תדחה.

תרגיל: $L_{M_0,c} = \{<M> \mid L(M) = L(M_0) \text{ and } |<M>| = c\}$. **פתרון:** כיוון ש: c קבוע, יש כמות מכונות סופית בגודל c, והשפה סופית ולכן השפה שייכת ל-R.

הוכיחו: $L = \{<N,x> \mid N \text{ on } x \text{ has an accepting path and a rejecting path}\} \notin R$.
פתרון: נראה רדוקציה $HP \leq_p L$. פונקציית הרדוקציה: $f(<M,x>) = <N,y>$.
N על קלט y תפעל: **1)** תמחק את M על x. **2)** מגרילה ביט b. **3)** אם $b = 0$ אז N דוחה. **4)** אם $b = 1$ אז N מקבלת.

תרגיל: $L = \{<M_1, M_2>: \left|L(M_1) \cap L(M_2)\right| > 10 \text{ or } \left|L(M_1) \cap L(M_2)\right| > 1000\} \in RE/R$
פתרון: (להשלים איי שייכות ל-R ברדוקציה). כעת נוכיח שהיא שייכת ל-RE בשימוש **הרצה מבוקרת**: נסדר את כל המילים ב-Σ^* בסדר לקסיקוגרפי, ונבצע את האלגוריתם הבא: **1)** עבור איטרציה $i = 1, 2, ...$: **1.1)** אחתל מונה $c = 0$. **1.2)** עבור איטרציה $j = 1, 2, ..., i$ **1.2.1)** הרץ את M_1, M_2 על המילים $w_1, ..., w_j$ למשך j צעדים. לכל מילה שהתקבלה קדם את c באחד. אם $c > 10$ אז החזר $true$. **נכונות** (להשלים).

דוגמה (לא פתרון מלא): $L_2 = \{<M> : |L(M)| \leq 2\} \in RE$ אם נתון שהמילה בשפה: כדי להוכיח זאת צריך לרוץ על כל המילים ולהראות שהיא לא מקבלת יותר מ 2. לכן: $\bar{L}_2 \notin RE$. אם נתון שהמילה לא בשפה: כדי להוכיח זאת נרוץ כמו מקודם ונבדוק שהמכונה מקבלת 3 מילים לפחות ונדע נסתור. לכן: $L_2 \in coRE$.

הוכיחו: $L = \{<M> \mid M \text{ halts on at least one input}\} \in RE \backslash R$. נגדיר את המ"ט הא"ד הבאה: המכונה M על קלט $<M>$ תבצע: **1)** נחש מילה w באורך כלשהו. **2)** הרץ את M על w וקבל. ניתנת לחישוב: פעולת הניחוש: כתיבת 0 או 1 והתקבלה לניחוש הנו הבא או עצירה. וסמלץ. נכונות: להשלים. **חלק 2:** נוכיח כי $L \notin R$ ברדוקציה $L_u \leq L$ ע"י: $f(<M,w>) = <M'>$. המכונה M' על קלט x תבצע: **1)** אם $x = \varepsilon$ אז: **1.1)** הרץ את M על w, אם קיבלה - קבל. **1.2)** אחרת, היכנס לוללאה אינסופית. **2)** אחרת, היכנס לוללאה אינסופית. הרדוקציה מלאה וניתנת לחישוב: כתיבת תיאור מכונה. תקפות: (השלם).

$L = \{M \mid M \text{ on } 20 \text{ s.t. the first } n \text{ words in lexi order at least } \frac{n}{4} \text{ are accepted}\} \in RE$
הוכחה: נגדיר מ"ט א"ד הבאה: N על הקלט $<M>$ תבצע: **1)** נחש מספר שלם וחיובי n. **2)** אם $n < 20$ דחה. **3)** חשב $m = roof(n/4)$ **4)** נחש m מילים $w_1, ..., w_m$ מתוך n המילים הראשונות בסדר הלקסי'. **4)** בדוק שכולן שונות זו מזו. **5)** עבור i מ-1 ועד m בצע: **5.1)** הרץ אצ M על w_i. אם דחתה - דחה. קבל. ניתנת לחישוב. הרדוקציה. נכונות: להשלים.

הוכיחו: $L = \{<M_1, M_2>: \left|L(M_1)\right|, \left|L(M_2)\right| \text{ are both finite, and } \left|L(M_1)\right| \text{ divides } \left|L(M_2)\right|\} \notin RE$
הוכחה: נוכיח $\bar{L}_u \leq L$ ע"י: $f(<M,w>) = <M',M'>$. המכונה M' על קלט x תבצע: **1)** אם $x = \varepsilon$ אז קבל. **2)** אחרת, הרץ את M על w ועונה כמוה. הרדוקציה מלאה וניתנת לחישוב: כתיבת תיאור של מכונה. תקפות: (להשלים).

הוכיחו: $L = \{<M_1, M_2> \mid \exists x \in \Sigma^* \text{ s.t. } M_1 \text{ accepts } x \text{ and } M_2 \text{ rejects } x\} \in RE \backslash R$.
פתרון: שייכות ל RE: ע"י מ"ט אי"ד: על קלט $<M_1, M_2>$ ע"י: **1)** נחש מילה x כלשהי. **2)** הרץ את M_1 על x. אם דחתה - דחה. **3)** הרץ את M_2 על x. אם קיבלה - דחה. אם דחתה - קבל. נכונות: ....
אי שייכות ל R: ע"י רדוקציה: $HP \leq L_1$ ע"י: $f(<M,w>) = <M_1, M_2>$ כאשר: M_1: על קלט x: **1)** הרץ את M על w. **2)** קבל. M_2: על קלט x: **1)** דחה. תקפות:...

הוכיחו: $L = \{<M> \mid \exists x \in \Sigma^{24} \text{ s.t. } M \text{ doesn't enter the } |x| \text{'s cell of tape}\} \in R$.
פתרון: השפה שייכת ל R. נראה אלגוריתם מכריע: על קלט $<M>$:1) נחש מילה x באורך 24. בצע **2)** הרץ את M על x ועקוב אחר כל הקונפיגורציות שהמכונה עוברת בהן. **3)** אם M נכנסה לתא 24 - דחה. **4)** אם M חזרה על אותה קונפיגורציה שכבר הייתה בה - קבל. **5)** אם M עצרה ללא כניסה לתא 24 - קבל. נכונות: ....

הוכיחו: $L = \{<M_1, M_2, M_3> \mid \exists x \in \Sigma^* \text{ s.t. } M_1 \text{ accepts } x, M_2 \text{ rejects } x \text{ and } M_3 \infty \text{ on } x\} \notin RE$
פתרון: ע"י רדוקיה $\overline{HP} \leq_p L_3$ ע"י: $f(<M,w>) = <M_1, M_2, M_3>$ כאשר M_1: על קלט x: **1)** קבל. M_2: על קלט x: **1)** דחה. M_3: על קלט x: **1)** הרץ את M על w ועונה כמוה. תקפות: ...

הוכיחו: $L = \{<M> \mid \exists L \in RE \backslash R \text{ and } \exists L' \in coRE \backslash R \text{ s.t. } L \cap L' \subseteq L(M)\} \in R$
הוכחה: תמיד נקלוף $L = HP \in RE \backslash R$, $L' = \overline{HP} \in coRE \backslash R$ ואז החיתוך יצא שפה ריקה שמוכלת בכל שפה ולכן אין צורך לבדוק מה זה עושה אלא ניתן לקבל מייד. ולכן $L_3 \in R$.

שאלת סייווג ל-$\overline{RE} \cup \overline{coRE}$

$L = \{<M_1, M_2>: \left|L(M_1) \cap L(M_2)\right| < 10 \text{ or } \left|L(M_1) \cap L(M_2)\right| > 1000\} \in \overline{RE} \cup \overline{coRE}$
פתרון: נוכיח זאת ב 2 שלבים ועל סמך משפט הרדוקציה: **1)** ע"י רדוקיה: $HP \leq L_1$ וזה יוכיח ש $L_1 \notin \{RE, RE\}$ וזה יוכיח ש $\overline{HP} \leq L_1$: **2)** ע"י רדוקיה: $HP \notin \{R, coRE\}$ כי $L_1 \notin \{R, coRE\}$ ו $\overline{HP} \notin \{R, RE\}$. **שלב ראשון:** $f(<M,w>) = <M_1, M_2>$ כך ש: M_1 מקבל הכל. M_2 מקבלת את המילים: $\{1, 11, 111, ..., 1^{11}\}$ (11 מילים שונות) ועבור שאר המילים היא מריצה את M על w ומקבלת לאחר עצירת M. הרדוקיה מלאה (אין קלט שהיא לא מוגדרת עליו) הרדוקיה ניתנת לחישוב - כתיבת תיאור של 2 מ"ט תקינות. הרדוקיה תקפה: (להשלים).
שלב שני: $f(<M,w>) = <M_1, M_2>$ כך ש: M_1 מקבל הכל. M_2 מריצה אם M על w ולאחר עצירת M מקבלת את המילים: $\{1, 11, 111, ..., 1^{11}\}$ (11 מילים שונות) ועבור שאר המילים היא דוחה. הרדוקיה מלאה הרדוקיה ניתנת לחישוב - כתיבת תיאור של 2 מ"ט תקינות. הרדוקיה תקפה: (להשלים).

תרגיל: $L = \{<M> \mid M \text{ stops to every input after more than } 42 \text{ steps}\} \in \overline{RE} \cup \overline{coRE}$.
פתרון: רדוקיה: $HP \leq L_1$ (ויכיח ש $L_1 \notin coRE$ ו ופפרט $L_1 \notin R$) הרדוקיה: $f(<M,x>) = <M'>$ כאשר: M' - על קלט w: **1)** ממלץ את M על x. **2)** בצע עוד 42 צעדים ימינה וקבל. (מוגדרת על כל קלט) וניתנת לחישוב. **תקפות**: (להשלים). רדוקיה: $\overline{HP} \leq L_1$ (ויכיח ש $L_1 \notin RE$ ו ופפרט $L_1 \notin R$) הרדוקיה: $f(<M,x>) = <M'>$ כאשר: M' - על קלט w: **1)** ממלץ את M על x למשך $|w|$ צעדים. **2)** אם M לא עצרה בזמן המוקצב אז בצע עוד 42 צעדים ימינה וקבל. **3)** אחרת, בצע לוולאה אינסופית. הרדוקציה מלאה (מוגדרת על כל קלט) וניתנת לחישוב. **תקפות**: (להשלים).

דוגמה (לא פתרון מלא): $L_3 = \{<M> : |L(M)| = 2\} \in RE$ אם נתון שהמילה בשפה: כדי להוכיח זאת צריך לרוץ על כל המילים ולהראות שהיא לא מקבלת יותר מ 2 ופחות. לכן: $\bar{L}_3 \notin RE$. אם נתון שהמילה לא בשפה: ייתכן שהמכונה לא מקבלת כלום ואז נצטרך לרוץ על כל המילים. לכן: $\bar{L}_3 \notin coRE$.

הבעיה הבאה אינה ב RE ואינה ב coRE.
$L = \{<M> \mid M \text{ halts on any input in less than } 10 \text{ step or more than } 20 \text{ steps}\}$
הוכחה: אינה ב coRE ע"י רדוקיה: $HP \leq L$. ע"י: $f(<M,w>) = <M'>$ כאשר: M': על קלט x: **1)** הרץ את M על w. עבור **2)** בצע עוד 20 צעדי סרק וקבל.
אינה ב RE ע"י רדוקיה: $\overline{HP} \leq L$ ע"י: $f(<M,w>) = <M'>$ כאשר: M': על קלט x: **1)** הרץ את M על w למשך $|x|$ צעדים. **2)** אם M עצרה בזמן המוקצב - היכנס לוללאה אינסופית. **3)** אחרת בצע עוד 20 צעדי סרק וקבל.
נכונות: אם M לא עוצרת על w אז קבל x, המכונה M לא תעצור בזמן המוקצב ולכן על כל קלט נבצע עוד 20 צעדים ונקבל (תנאי L מתקיים).

שאלות שייכות ל-P

הוכיחו - $L = \{G \mid G \text{ has a VC of size } 5k, \text{ for some } k \in N\} \in P$. **פתרון:** נראה מ"ט M_1 דטרמיניסטית פולינומית עבור השפה L_1. נשים לב שנוכל לבדוק האם יש VC בגודל $n - t$ כאשר $t = n \bmod 5$. $t = n \bmod 5$. המכונה M_1 על הקלט G כאשר G הוא גרף, תבצע: **1)** עבור $t = n \bmod 5$ **1.1)** עבור על כל תתי-קבוצות של $V(G)$ בגודל $n - t$. **1.1.1)** בדוק האם הא מהווה VC. אם כן, קבל. **2)** דחה. **סיבוכיות**: לעבור על כל התתי קבוצות בגודל $n - t$ (יש 5 סוגי שאריות מ-0 עד 4) ולכן $O(n^4)$ וזה פולינומי. **נכונות**: (השלימו).

הוכיחו - $L = \{\phi \mid \phi \text{ is a DNF that has at least 8 satisfiable assignments}\} \in P$.
פתרון: נראה אלגוריתם פולינומי דטרמיניסטי עבור השפה. M: על קלט $<\phi>$:1) עבור על הנוסחא ומחק פסוקיות שיש בהן משתנה ושלילתו ומחק כפילויות. **2)** אם לא נותרו פסוקיות - דחה. **3)** הגדר מונה $c = 0$. **4)** עבור כל פסוקית, חשב כמה משתנים לא מופיעים בה (k) והוסף למונה $c = c + 2^k$. **5)** אם $c \geq 8$ קבל ואחרת דחה. **סיבוכיות**: (להשלים). **נכונות**: (להשלים).

הוכיחו: $L = \{\phi \mid \phi \text{ is CNF that has a satise assignmt with a FALSE to 7 variables}\} \in P$
פתרון: נראה אלגוריתם פולינומי דטרמיניסטי: על קלט $<\phi>$:1) עבור על כל תתי הקבוצות בגודל 7 משתני הנוסחא. **1.1)** הצב במשתנים אלו FALSE ובדוק האחרונים TRUE ובדוק הנה הנוסחא מסתפקת. אם כן - קבל. **2)** דחה. **סיבוכיות**: מספר תתי הקבוצות בגודל 7 של משתנים היא: $\binom{n}{7} = O(n^7)$ ועבור כל קבוצה כזו צריך להציב בנוסחא ולבדוק שהיא מתקיימת: $O(N)$. סה"כ חסום: $O(N^7)$.
כאשר N מייצג את אורך הקלט, n מייצג את כמות המשתנים בנוסחא.

הוכיחו: $L = \{<G,k> \mid \forall v \in V: d(v) < 100 \text{ and } G \text{ contains a Clique of size } k\} \in P$.
פתרון: אלגוריתם פולינומי דטרמיניסטי: על קלט $<G,k>$:1) עבור על כל קודקודי הגרף ובדוק לפי מסריצת השכנויות שכל אחד מהם בדרגה קטנה ממש מ 100. אם לא - דחה. **2)** בדוק שכל זוג קודקודים **3)** עבור על כל תתי הקבוצות של קודקודים בגודל k ועבור כל קבוצה: **3.1)** בדוק שזוג קודקודים בקבוצה מחוברים בצלע. אם כן - קבל. **4)** דחה. **סיבוכיות**: מעבר על כל הקודקודים ובדיקת הדרגה היא ב $O(2^n)$ חסום בגודל הקלט. בדיקת $k - 100$ - חסום בגודל הקלט. מעבר על כל תתי קבוצות בגודל k הלא כל היותר $\binom{n}{100} = O(n^{100})$ וכל זוג ≤ 100. ובדיקה של חיבור בצלעות עוד כל קבוצה כזו: $O(n^4)$.
סה"כ: $O(n^{104})$ החסום ב $O(N^{104})$ - פולינומי בגודל הקלט.

הגדרה של SET COVER
הוכיחו שהבא: $SC = \{(n,k,S_1,...,S_t) \mid n.k \in N, \forall i \in [t]\ S_i \subseteq [n], \exists I \subseteq [t] \text{ s.t. } |I| = k \text{ and } \bigcup_{i \in I} S_i = [n]\}$
הוכיחו: $L = \{(n,S_1,....S_t) \mid \exists \text{ an even } k \in N \text{ s.t. } (n,k,S_1,....,S_t) \in SC\} \in P$.
הוכחה: השפה שייכת ל P. כי בהינתן הקלט: $n, S_1, ..., S_t$ אז $k = t$ זוגי. נבחר: $k = t$ ואז אם האיחוד שלן מכסה את $\{1,2,...,n\}$ אז מצאנו את ה k המבוקש ולכן נקבל. ואחרת נבדוקה כי אם האיחוד של כולן לא כיסה את הכל אז גם נאחד חלק מקבוצות, לא נצליח לכסות את הכל. אם t אי זוגי אז נבחר: $k = t - 1$ ואז יש לעבור על $O(t) = \binom{t}{1} = \binom{t}{t-1}$ אפשרויות לבחור את $t - 1$ הקבוצות מתוך ה t, לאחד אותן ולבדוק הנם האיחוד בגודה $\{1,2,...,n\}$. אם מצאנו - נקבל. אם לא מצאנו בכלל - נדחה כי לא ייתכן שכמות קטנה יותר תכסה הכל. סיבוכיות: פולינומית בגודל הקלט.

שאלה 2022 מועד ב' סמסטר א'

בהינתן מ"ט א"ד M, מילה w תקרא רב מסלולית ב-N אם יש ל-w (במכונה N) לפחות מסלול חישוב מקבל אחד, לפחות מסלול חישוב דוחה אחד ולפחות מסלול חישוב אחד שלא עוצר.
השפה הרב מסלולית של המכונה הא"ד M היא קבוצת המילים שהן רב מסלוליות ב-N.
סעיף א' הוכיחו או הפריכו: $L \in RE$ אזי קיימת מ"ט א"ד M שהשפה הרב מסלולית שלה שווה ל-L.
סעיף ב' הוכיחו או הפריכו: קיימת מ"ט א"ד M שהשפה הרב מסלולית שלה היא השפה הבאה:
$L = \{<M,w> \mid M \text{ is a TM that doesn't accept } w\}$.
פתרון א': הוכחה: אם $L \in RE$ אזי קיימת מ"ט M המזהה את L. נגדיר את המכונה הא"ד הבאה: N: על קלט x: **1)** נחש מספר שלם בין 1 ל 3. **2)** אם יצא 2 - דחה. **4)** אם יצא 3, הרץ את M על x ועונה כמוה. **נכונות**: אם x בשפה אז יהיה לו מסלול חישוב אחד מקבל ואחד דוחה ואחד לא עוצר. אם x לא בשפה אז לא יהיו לו מסלולים מקבלים בכלל.
פתרון ב': הוכחה: נגדיר את המכונה הבאה: N: על קלט $<M,w>$:1) נחש מספר שלם בין 1 ל 3. **2)** אם יצא 1 - הרץ את M על w: עובר **2.1)** אם דחתה - תיכנס לוללאה אינסופית **2.2)** אם קיבלה - קבל. **3)** אם יצא 2 - קבל. **4)** אם יצא 3 - דחה.

שאלות שייכות ל-NPH (לא ל-NP)

תרגיל: $L_{1/8} = \{\phi \mid \phi \text{ is 3CNF and } \exists \text{ a satisfying assignment to } \phi, \text{ and at least } \frac{1}{8} \text{ of the possible assignments are not satisfying}\}$
הוכיחו ש: $L_{1/8} \in NPH$. **פתרון:** נוכיח ברדוקציה $3SAT \leq_p L_{1/8}$. **פונקצית הרדוקציה**:
1.1) עבור על כל תתי-קבוצות של $V(G)$ בגודל $n - t$. **1.1.1)** בדוק האם הא מהווה VC. אם כן, קבל. **2)** דחה. **סיבוכיות**: לעבור על כל התתי קבוצות בגודל $n - t$ (יש 5 סוגי שאריות מ-0 עד 4) ולכן $O(n^4)$ וזה פולינומי. **נכונות**: (השלימו

מטלה 3

דוגמה פרקטית מעבר מ-CNF ל-3CNF: נמיר לצורת $3CNF$ כך:

$$\phi = (B \vee \bar{C} \vee \bar{D} \vee \bar{F} \vee G) \wedge (E \vee \bar{G}) \wedge (A \vee \bar{B} \vee E)$$

$$\phi = (\bar{B} \vee \bar{F} \vee z_1) \wedge (\bar{z}_1 \vee \bar{D} \vee z_2) \wedge (\bar{z}_2 \vee \bar{F} \vee G) \wedge (E \vee \bar{G} \vee E) \wedge (A \vee \bar{B} \vee E)$$

אם הפסוקית בגודל 3, לא נשנה כלום. אם הפסוקית בגודל 2, נבחר שרירותית באחד מהמשתנים להשלמה.

הוכחה: $CNF - IS = \{G, k, \phi \mid G \text{ has a size } k \text{ IS OR } \phi \text{ is satisfiable } CNF\} \in NPC$.

פתרון: נוכיח כי $CNF - IS \in NP$. המכונה M על הקלט $\langle G, k, \phi \rangle$ תבצע: **1)** מנחשת קבוצת קודקודים בגודל k והשמה בגודל n. **2)** בודקת האם קבוצת הקודקודים אכן IS. אם כן, מקבלת. **3)** מציבה את ההשמה בפסוקית ϕ ומוודאת שערך הנוסחה הוא T. אם כן, מקבלת. אחרת, דוחה. **סיבוכיות:** המכונה רצה בזמן בפולינומי בגודל הקלט: **1.** ניחוש קבוצת הקודקודים חסומה ב-$|V(G)|$. **2.** ניחוש השמה באורך n. **3.** וידוא IS - מעבר על מטר השכנויות ווידוא כי אין צלעות $|V(G)|^2 \geq k^2$. וידוא ספיקות הנוסחה: $|\phi| = O(m)$. **נכונות:** להשלים. **שלב 2:** $CNF - IS \in NPH$. נראה רדוקציה $SAT \leq_p CNF - IS$. הפונקציה: $f(\phi) = \langle G = (\{v_1, v_2\}, \{v_1, v_2\}), 2, \phi \rangle$. הרדוקציה מחושבת בזמן פולינומי בקלט: העתקה של הנוסחה, וייצור גרף בעל שני קודקודים וצלע אחת. **תקפות:** (השלימו).

תרגיל PARTITION: הוכיחו $PARTITION = \{S \mid \exists S' \subset S \text{ s.t. } \sum_{x \in S'} x = \sum_{x \notin S'} x\} \in NPC$.

פתרון: נוכיח כי $PARTITION \in NP$. המכונה M על הקלט S תבצע: **1)** תנחש תת קבוצה של ספרים T. **2)** תבדוק האם $\sum_{x \in T} x = \sum_{x \in S \setminus T} x$. אם כן, קבל. אחרת, דחה. **סיבוכיות:** ניחוש תת קבוצה של ספרים חסום בכמות הספרים בקלט, וסכימת אירבי שתי הקבוצות מתבצעת בזמן פולינומי בכמות המספרים בקבוצה. **נכונות:** (להשלים). **חלק 2:** נוכיח כי $PARTITION \in NPH$. נראה רדוקציה $SubsetSum \leq_p Partition$. הפונקציה: $f(\langle S, t \rangle) = \langle S' \rangle$. יהי $\sum_{y \in S} y = x$. הקבוצה S' תכיל את כל הספרים המקוריים מקבוצה S וגם את האיבר החדש $x - 2t$. **הרדוקציה פולינומית:** חישוב סכום כל איברי הקבוצה פולינומי בכמות האיברים. חישוב $x - 2t$ מתבצע ב-$O(1)$. **תקפות:** (להשלים).

הוכיחו $DS = \{\langle G, k \rangle \mid G \text{ with a size } k \text{ dominating set}\} \in NPC$.

פתרון: נוכיח $DS \in NP$ (הוכחה נמצאת בחלק של "שאלות שייכות ל-NP"). **חלק 2:** נוכיח $DS \in NPH$. נראה רדוקציה $VC \leq_p DS$. הפונקציה: $f(\langle G, k \rangle) = \langle G', k \rangle$. לכל צלע $\{uv\} \in E(G)$ נוסיף קודקוד חדש w. את הקודקוד נחבר גם ל-u וגם ל-v. הפרמטר k נשאר זהה. **סיבוכיות:** הרדוקציה פולינומית: עברנו על $|E(G)|$ צלעות, לכל אחת הוספנו קודקוד ושתי צלעות. **תקפות:** (השלימו).

הוכיחו $DoubleHC = \{\langle G \rangle \mid G \text{ with two different Hamiltonian cycles}\} \in NPC$.

פתרון: להוכיח שייכות ל-NP. **חלק 2:** נוכיח $DoubleHC \in NPH$ ברדוקציה $HC \leq_p DoubleHC$. הפונקציה: $f(\langle G \rangle) = \langle G' \rangle$. אם $|V(G)| \leq 2$ - לא לשנות. אחרת, פונקציית הרדוקציה תייצר גרף G' המכיל שלושה קודקודים חדשים. יהי קודקוד $v \in V(G)$ ונשמור שלושה קודקודים חדשים v', u_1, u_2. ניצור קליקה $\{v, v', u_1, u_2\}$ ונחבר את כל השכנים של v גם אל v'. **הרדוקציה פולינומית:** העתקת גרף, הוספת $O(1)$ קודקודים וצלעות. **תקפות:** (להשלים).

הוכיחו: אם $L_1 \leq_p L_2$ וגם $L_2 \in NP$ אזי $L_1 \in NP$. **פתרון:** נתון כי $L_2 \in NP$ ולכן קיימת מכונה א"ד M_2 המכריעה אותה בזמן פולינומי. היות ומתקיים $L_1 \leq_p L_2$, קיימת מכונה לחישוב הרדוקציה f הרצה בזמן פולינומי. נבנה בעזרתן מ"ט א"ד המכריעה את השפה L_1 בזמן פולינומי: המכונה M_1 על קלט x תבצע: **1)** מריצה את $f(x)$ ומקבלת פלט y. **2)** מריצה את M_2 על הקלט y וענה כמוה. **סיבוכיות:** המכונה פולינומית, שכן M_f, M_2 פולינומיות. כנוכנות נובעת מתקפות הרדוקציה ומכונות M_2. בנינו מ"ט א"ד פולינומית לשפה $L_1 \in NP$.

הוכיחו: אם $L_1 \leq_p L_2$ וגם $L_2 \in NPH$ אזי $L_1 \in NPH$. **פתרון:** נתון כי $L_1 \leq_p L_2$ ולכן קיימת מ"ט לחישוב הרדוקציה M_f הרצה בזמן פולינומי. נתון בנוסף כי $L_2 \in NPH$ ולכן לכל שפה $L \in NP$ מתקיים $L \leq_p L_1$. במילים אחרות, לכל שפה $L \in NP$ קיימת מכונה M_{fL} פולינומית לרדוקציה ממנה אל L_1. לכן, לכל שפה $L \in NP$ קיימת רדוקציה לשפה L_2: הרדוקציה תהיה $M_f(M_{fL})$. ומכאן ש: $L_2 \in NPH$ לפי ההגדרה.

הוכיחו: תהי $L_1 \in NPC$. אזי $P = NP \Leftrightarrow L_1 \in P$. **פתרון כיוון א':** היות ו-$L_1 \in NPC$ אזי גם $L_1 \in NP$. אך $P = NP$ ולכן $L_1 \in P$. **פתרון כיוון ב':** מהגדרת NPC, לכל $L' \in NP$ מתקיים $L' \leq_p L_1$. לכן, ממשפט הרדוקציה נקבל $L' \in P$, ולכן $P = NP$.

מטלה 2

תהי $L = \{\langle M \rangle \mid \exists w_1, w_2 \in \Sigma^* \text{ s.t. } M \text{ accepts } w_1 \text{ within } |w_2|^{steps} \text{ and } M \text{ accepts } w_2 \text{ within } |w_1|^{steps}\}$ בנו לשפה L מכונה דטרמיניסטית ומכונה א"ד. **פתרון:**

מכונה דטרמיניסטית: על קלט $\langle M \rangle$: **1)** נמצא i מ-1 עד אינסוף בצעד: **2)** עבור j מ-1 עד i בצעד: **3)** עבור k מ-1 עד i בצעד: **3.1)** הרץ את M על w_j למשך $|w_k|$ צעדים. (כאשר w_t מייצג את המילה ה-t ב-Σ^* לפי סדר לקסיקוגרפי) **3.2)** הרץ את M על w_k למשך $|w_j|$ צעדים. **3.3)** אם ב-2 ההרצות M הספיקה לעצור ולקבל - קבל. **הסבר:** נשים לב שמכיוון ש i הוא רץ עד אינסוף אזי למעשה נעבור על כל זוג מילים אפשריות ונצליב את הרצת M על כל אחת מהן לפי כמות הצעדים הנדרשת ולכן מכונה זו מזהה את השפה. **מכונה א"ד:** על קלט $\langle M \rangle$: **1)** נחש 2 מילים: w_1, w_2. **2)** הרץ את M על w_1 למשך $|w_2|$ צעדים. **3)** הרץ את M על w_2 למשך $|w_1|$ צעדים. **4)** אם ב 2 ההרצות M הספיקה לעצור ולקבל - קבל. אחרת - דחה.

הוכיחו: $\overline{REG} \cup coRE = \{\langle M \rangle \mid L(M) \text{ is a CFL and not regular}\}$. **פתרון:** (שלב לא נחוץ אך טוב לדוגמה): נראה כי $L \notin R$ בעזרת משפט רייס. נגדיר את תכונה $S = \{L \in RE \mid L \text{ is a CFL but not Regular}\}$. נוכיח שהתכונה לא טריוויאלית: $S \neq \emptyset$ כי $\{a^n b^n\} \in S$ (השפה הריקה רגולרית). $S \neq \Sigma^*$ כי זו שפה חסרת הקשר שאינה רגולרית. לכן, לפי משפט רייס $L \notin R$. **שלב 2** נראה כי $L \notin RE$ בעזרת רדוקציה מ-$\overline{L_u}$. הפונקציה: $f(\langle M, x \rangle) = \langle M_x \rangle$. המכונה M_x על הקלט y תבצע: **1)** אם $y = 0^n 1^n$ עבור n טבעי אז קבל. **2)** הרץ את M על w וענה כמוה. **הרדוקציה** מוגדרת לכל קלט וניתנת לחישוב. **תקפות:** (להשלים). **שלב 3:** נראה כי $L \notin coRE$ בעזרת רדוקציה מ-L_u עם הפונקציה: $f(\langle M, x \rangle) = \langle M_x \rangle$. המכונה M_x על קלט y תבצע: **1)** אם $y = 0^n 1^n$ עבור n טבעי, קבל. **2)** נחש משפט k. **3)** הרץ את M על x למשך k צעדים וענה הפוך. אם לא עצרה - קבל. **הרדוקציה** מוגדרת לכל קלט וניתנת לחישוב. **תקפות:** (להשלים).

הוכיחו: $L_n = \{\langle M_1, M_2, ... M_n \rangle \mid \text{no word of length smaller than } n \text{ is in } L(M_1) \cap ... \cap L(M_n)\} \in NPC$.

הוכיחו: $L_n \in coRE \setminus R$. **פתרון:** נראה רדוקציה מ-$\overline{L_u}$ עם פונקציה: $f(\langle M, w \rangle) = \langle M', ... M' \rangle$. כל ה-$n$ מכונות זהות. המכונה M' על הקלט y תבצע: **1)** הרץ את M וענה כמוה. **תקפות:** (להשלים). נראה כי $L \in coRE$ ע"י בניית מ"ט הוכחה. **1)** עבור $i = 1, ..$ עבור $j = 1, ..., |\Sigma^*|^{n-1}$ **2.1)** אתחל מונה $c = 0$. **2.2)** עבור $k = 1, ..., n$ בצע: **2.2.1)** הרץ את המילה ה-j למשך i צעדים על המכונה M_k. אם קיבלה את c. **2.3)** אם $c = n$ אז דחה. **נכונות** (להשלים).

הוכיחו: $L = \{\langle M \rangle \mid M \text{ stops to every input after more than } 42^{steps}\} \in \overline{RE} \cup coRE$.

פתרון: ידוע לנו ש: $L_{\Sigma^*} = \{\langle M \rangle : |L(M)| = \Sigma^*\} \in \overline{RE} \cup coRE$. הרדוקציה $L_{\Sigma^*} \leq L$ תהיה באופן הבא: $f(\langle M \rangle) = \langle U \rangle$. המכונה U על הקלט y תבצע: **1)** בצע 42 צעדים במקום. **2)** סמלץ את M על y - אם דחה כנס לוולוקה אינסופית. הרדוקציה מלאה... הרדוקציה ניתנת לחישוב.. **תקפות** (להשלים).

הוכיחו: $L = \{G \mid G \text{ is 3COLOR except for at most 2 nodes that requires a 4th color}\} \in NPH$. נוסיף ל-$G$ עוד שני קודקודים ונחבר לכל יתר קודקודי הגרף מלבד זה לזה. הרדוקציה פולינומית משום שהוספת 2 קודקודים ו-$2n$ צלעות מצריכה זמן ליניארי. הרדוקציה מלאה כיוון שהיא מוגדרת לכל גרף וניתנת לחישוב מפני שאת הגרף G' ניתן לקודד.

הוכיחו: $EP = \{G \mid G \text{ contains Euler path}\} \in P$. **הוכחה:** מ"ט M על קלט $\langle G \rangle$ תבצע: **1)** הרץ BFS לוודא כי הגרף קשיר. **2)** אתחל מונה $c = 0$. **3)** עבור $i = 1, ..., |V(G)|$ בצע: **3.1)** אם $deg(v_i)$ הוא אי זוגי אז קבע $c = c + 1$. **4)** אם $c > 2$ אז החזר "אין מסלול אוילר". אחרת החזר "יש מסלול אוילר". האלגוריתם פולינומי BFS רץ ב-$O(|V| + |E|)$.

הוכיחו: $L = \{G \mid G \text{ has 3 foreign domination sets}\} \in NP$. **הוכחה:** המכונה N על הקלט $\langle G \rangle$ תבצע: **1)** מנחשת שלוש קבוצות של קודקודים S_1, S_2, S_3. **2)** לכל קבוצה S_i מוודאת כי שכני כל הקודקודים ב-S_i מכסים את כל הקודקודים $V(G) \setminus S_i$. אחרת דוחה. **3)** לכל $i \neq j$ מוודאת כי $S_i \cap S_j$. אחרת, דוחה. **4)** מקבלת.

מטלה 2

הוכיחו: $Subset - Sum = \{(S, k) \mid S \text{ is a set of numbers. } \exists S' \subseteq S \text{ s.t. } \sum_{s \in S'} s = k\} \in NP$.

פתרון: נוכיח ע"י הגדרת יחס R_L היחס: $(x, y) \in R_L$ אם ורק אם $x = (S, k)$ כאשר S היא קבוצת מספרים, k הוא מספר שלם. $(S') \subseteq S$ כאשר $S' \subseteq S$ וגם $\sum_{x \in S'} = k$. היחס חסום פולינומית כי $|y| \leq |(S)| \leq |x|$. מתקיים: $L \in x$ אם ורק אם קיימת $S' \subseteq S$ כך ש $\sum_{x \in S'} = k$. ולכן נבחר את y להיות (S').

הוכיחו: $CliqueK = \{\langle G, k_1, k_2 \rangle \mid G \text{ has a clique in size } k, \text{ and } k_1 \leq k \leq k_2\} \in NP$.

פתרון: בערת מכונה המוודאת יחס: **סיבוכיות העד:** העד y יהיה מחרוזת ביוארית באורך $|V(G)|$, שיצב (באופן שכבר הסברנו) קבוצת קודקודים כלשהי. האידיאל הוא שהקבוצה שתיצב היא קליקה בגודל המתאים. המכונה V על הקלט $\langle y, (G, k_1, k_2) \rangle$ תבצע: **1)** וודא שגודל הקבוצה המיוצגת הוא לפחות k_1 ולכל היותר k_2 - אם לא, דחה. **2)** בדוק האם כל שני קודקודים בקבוצה יש צלע - אם לא דחה. **3)** קבל. **זמן הריצה:** וידוא גודל הוא ליניארי (השוואת תווים). בדיקה האם בין כל שני קודקודים בקבוצה יש צלע הוא $O(V(G)^2)$ ולכן פולינומי בגודל הקלט. נכונות: (להשלים).

שאלה על איחוד סימטרי Δ

תהיינה L_1, L_2. ההפרש הסימטרי של L_1, L_2 הוא השפה: $L_1 \Delta L_2 = (L_1 \setminus L_2) \cup (L_2 \setminus L_1)$. הוכיחו או הפריכו או הראו שזו איננה פתוחה: **א)** אם $L_1, L_2 \in NP$ אז $L_1 \Delta L_2 \in NP$. **ב)** אם $L_1, L_2 \in NP \cap coNP$ אז $L_1 \Delta L_2 \in NP$. **פתרון א':** הבעיה פתוחה. נראה שהפתרון תלוי בשאלה האם $coNP = NP$. **מצד אחד:** אם $P = NP$ אזי מנתוני השאלה ש: $L_1, L_2 \in NP$ נובע ש: $L_1 \Delta L_2 = (L_1 \setminus L_2) \cup (L_2 \setminus L_1) = (L_1 \cap \bar{L}_2) \cup (L_2 \cap \bar{L}_1)$ ומכאן: $\bar{L}_1, \bar{L}_2 \in NP$ ולכן גם $\bar{L}_1, \bar{L}_2 \in coNP$. **מצד שני:** אם $NP \neq coNP$ אזי תהי השפה $\bar{L} \notin NP$. מהגדרת $coNP$ אז $\bar{L} \in coNP$. כעת, נפריך את הטענה בדוגמה הבאה: $L_1 = L_2 = \Sigma^*$. מתקיים ש: $L_1 \Delta L_2 = (L_1 \setminus L_2) \cup (L_2 \setminus L_1) = \emptyset$. אבל $\bar{L}_1, \bar{L}_2 \notin NP$. כלומר הטענה לא נכונה. ומכיוון ש: $NP = coNP$ היא בעיה פתוחה אז גם הבעיה שלנו פתוחה. **פתרון ב':** הטענה נכונה. תהיינה $L_1, L_2 \in NP \cap coNP$ ולכן $L_1, L_2 \in NP$ וגם $\bar{L}_1, \bar{L}_2 \in NP$ לפי הגדרת $coNP$. מכאן השפה הפתרון הוא בדומה לצד אחד מסעיף א'.

מבחן 2022 מועד א' סמסטר א'

נניח כי הוכח ש: $P \neq NP$. **הפריכו:** תהי שפה $L_1 \in NPC$, ותהי L_2 כך ש: $L_1 \leq_p L_2$. אז $L_2 \in NPC$.

הפרכה: הטענה לא נכונה. דוגמא נגדית: $L_1 = CLIQUE \in NPC$ אזי $L_2 = \Sigma^*$. $L_1 \leq L_2$ אבל $L_2 \in P$ ולכן $L_2 \in NPC$ אזי ייתקיים: $NP = P$ בסתירה להנחה.

הוכיחו: הראו רדוקציה $4COLOR \leq_p 3COLOR$. **הוכחה:** פונקציית הרדוקציה: $f(\langle G \rangle) = \langle H \rangle$ כאשר H הוא G עם תוספת של קודקוד אחד חדש שמחובר לכל שאר הקודקודים שהוא G. **סיבוכיות:** תוספת של קודקוד בודד + כל הצלעות שמחוברות אליו - $O(N)$. **תקפות:** (קלט שייך לשפה השמאלית אם ורק אם הפלט של הרדוקציה שייך לשפה הימנית) **צד א':** אם G הוא 3 צביע אז H הוא 4 צביע כי את קודקוד G נצבע ב 3 צבעים הנתונים ואת הקודקוד החדש נצבע בצבע רביעי לכן צביעה זו תקינה. **צד ב':** אם G אינו 3 צביע אז לא יתיכן ש H יהיה 4 צביע כי בוודאות הקודקוד החדש לבדו צבוע בצבע הרביעי (כי הוא מחובר לכולם) ולכן שאר קודקודי G צבועים ב 3 צבעים - **סתירה**.

תרגיל: הוכיחו ש $RE \setminus R$ סגורה לפעולת ההיפוך. כלומר הוכיחו כי אם $L \in RE \setminus R$ אז $L^R \in RE \setminus R$.

הוכחה: תהי $L \in RE \setminus R$. מכאן: $L \in RE$ וגם $L \notin R$. לפי סגירות של RE להיפוך נקבל ש $L^R \in RE$. נניח בשלילה ש $L^R \in R$. אזי מסגירות של R להיפוך נקבל ש $(L^R)^R \in R$. כלומר: $L \in R$ (סתירה) לכן: $L^R \notin R$. קיבלנו ש $L^R \in RE, L^R \notin R$ ולכן: $L^R \in RE \setminus R$.

תרגיל: נניח שפה: $L = \{\langle M \rangle \mid \exists n > 0 \text{ s.t. } \forall w \in \Sigma^n, M \text{ accepts } w\}$. **א)** הוכיחו $L \in RE$. **ב)** הראו כי $L \leq HP$ ע"י הפונקציה: $f(\langle M, w \rangle) = \langle M' \rangle$ כאשר: M' על קלט x: **1)** הרץ את M על w. **2)** אם $x = 1$ אז x. קבל. **3)** אחרת - דחה. **תקפות:** אם M עוצרת על w אז M' תקבל את כל המילים באורך 1 ולכן תהיה בשפה L. אם M לא עוצרת על w אז M' לא מקבלת כלום.

פתרון א': הוכחה: $L \in RE$ כי $L \in \Sigma^*$. לכן קיימת מ"ט M_L המכריעה עבור L: המכונה M_L': על קלט x: **1)** הרץ את M_L על x. **2)** אם קיבלה - קבל. **3)** אם דחתה - היכנס לוולוקה אינסופית. נשים לב שכל מילה שתקבלת ב M_L (אינה ב L) אז המכונה הנ"ל לא עוצרת עליה. הסיבה שיש מילה שלא מתקבלת היא רק כי $L \neq \Sigma^*$.

מבחן 2022 מועד ב' סמסטר א'

תהי DP קבוצת כל השפות L שעבור מתקיים $L_1 \in NP$ וגם $L_2 \in coNP$ כך ש: $L_1 \cap L_2 = L$. נתונה השפה: $L = \{\langle G, k \rangle : G \text{ is an undirected graph that has IS of size } k \text{ and doesn't have an IS of size } k + 1\}$ והוכיחו כי $L \in DP$. **פתרון:** נגדיר: $L_1 = IS \in NP$ = שפת כל קידודי $\langle G, k \rangle$ כך שיש ב G קבוצה בלתי תלויה בגודל k. $L_2 = coNPk$ = שפת כל קידודי $\langle G, k \rangle$ כך שאין ב G קבוצה בלתי תלויה בגודל k+1. (כי המשלימה שייכת ל NP) ומכאן: $L = L_1 \cap L_2$.

הוכיחו או הפריכו: $NP \subseteq coNP$ אז $NP = coNP$. **פתרון:** הוכחה: לפי הנתון: $NP \subseteq coNP$. ולכן כדי להוכיחה שווין, מספיק להוכיח ש $coNP \subseteq NP$. תהי $L \in coNP$ ומכאן: $\bar{L} \in NP$. ולפי הנתונים: $\bar{L} \in coNP$ ולכן: $L \in NP$.

נגדיר את השפה הבאה:

$$L = \{\langle \phi \rangle : \phi \text{ is a Boolean formula that has at most one satisfying assignment}\}$$

הוכיחו או הפריכו: $L \in coNP$. **פתרון:** אינטואיציה: כדי לאמת שהקלט הוא בשפה, לא מספיק להראות רק השמה אחת מספקת אלא בנוסף צריך לעבור על כל האחרות ולהראות שהן לא מספקות (וזה לא פולינומי) לכן הנחה ל coNP. כי כדי לאמת שהקלט לא בשפה צריך להראות רק 2 השמות מספקות. נראה כי מ"ט א"ד לשפה המשלימה: N: על קלט $\langle \phi \rangle$: **1)** נחש 2 השמות z_1, z_2 למשתני ϕ. **2)** הצב את כל אחת מהשמות בנוסחא ובדוק האם הנוסחא מספקת. **3)** אם 2 ההשמות מספקות - קבל. **4)** אחרת - דחה.

נכונות: **כיוון א':** אם $\bar{L} \in coNP$ אז קיימות לפחות 2 השמות מספקות ולכן קיים מסלול חישוב בו נחשב בדיוק את 2 ההשמות הללו, נציב בנדוון ונקבל. **כיוון ב':** אם $\bar{L} \notin coNP$ אז לא קיימות 2 השמות מספקות ולכן לכל נחוש שניקח, בהכרח לפחות השמה אחת לא תהיה מספקת ונדחה.

סיבוכיות: גודל ההשמה הוא $O(n)$ ולכן זמן הניחוש הוא פולינומי בגודל הקלט. זמן ההצבה ובדיקת הנוסחא הוא $O(N)$. סה"כ: פולינומי בגודל הקלט..

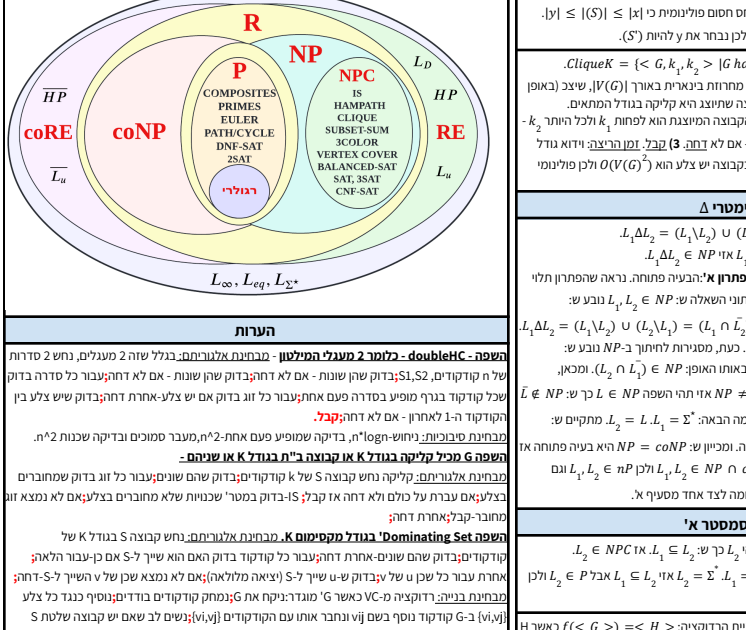
בהינתן גרף לא מכוון G, נסמן ב-$w(G)$ את גודל הקליקה הגדולה ביותר בגרף G. נגדיר את השפה:

$$L = \{\langle G_1, G_2 \rangle \mid G_1, G_2 \text{ are undirected graphs and } w(G_1) \geq w(G_2)\}$$

הראו רדוקציה פולינומית ל-$CLIQUE$ ל-L. (הוכיחו את השוואתכם). **פתרון:** נראה $CLIQUE \leq_p L$. כאשר הפונקציה: $f(\langle G, k \rangle) = \langle G, H \rangle$ כאשר H הוא בדיוק קליקה שלמה בגודל k. **סיבוכיות:** העתקת הגרף + יצירה של קליקה בגודל k בזמן: $O(N)$. **תקפות:** מכיוון שאנו מעתיקים את G ומייצרים G_2 הוא קליקה בגודל k אזי יש ב G קליקה בגודל k אם ורק אם $\omega(G) \geq \omega(H)$ אם ורק אם $\langle G, k \rangle \in CLIQUE$. כלומר: **צד א':** אם $\omega(G_1) \geq \omega(G_2)$ אז יש ב G קליקה בגודל k (לפחות) ולכן ב G מתקיים: $\omega(G_1) \geq k$ ואילו $\omega(G_2) = k$ כי G_2 הוא בדיוק קליקה בגודל k ולכן: $\langle G_1, G_2 \rangle \in L$. **צד ב':** אם $\langle G_1, G_2 \rangle \in L$ אז מכיוון ש G_2 הוא בדיוק קליקה בגודל k ומתקיים: $\omega(G_1) \geq \omega(G_2) = k$ אז זה בדיוק אומר שיש ב G_1 קליקה בגודל לפחות k אך לפי הבנייה: $G_1 = G$ ולכן יש ב G קליקה בגודל k ולכן: $\langle G, k \rangle \in CLIQUE$.

הוכיחו את ההרחבה הבאה של משפט רייס: אם S היא תכונה לא טריוויאלית של שפות RE כך ש: $S \notin RE$ אז $L_S \notin RE$ (רמז: הראו רדוקציה מהשפה $\overline{HP}$). **פתרון:** צש"ל: $L_S \notin RE$. מכיוון ש S אינה טריוויאלית אזי ישנה שפה $A \in S$ ולכן יש מכונה M_A עבור A. נראה רדוקציה: $\overline{HP} \leq L_S$. כאשר: $f(\langle M, w \rangle) = \langle M' \rangle$ כאשר: M': על קלט x: **1)** הרץ את M על w ואת M_A על x במבקיבל. **2)** אם M_A עצרה ודחתה, המתן ל M. **3)** אם M_A עצרה וקיבלה - קבל. **4)** אם M עצרה על w - קבל

$NP \neq P$



הערות

השפה - doubleHC - כלומר 2 מעגלי המילטון - מבחינת אלגוריתם: בגלל שצוי 2 מעגלים, נחש 2 סדרות של n קודקודים, S1,S2;בדוק שיון שונות - אם לא דחה;בדוק שהן שונות - אם לא דחה;עבור כל סדרה בדוק שכל קודקוד בגרף מופיע בסדרה פעם אחת;עבור כל זוג בדוק אם יש צלע-אחרת דחה;בדוק שיש צלע בין הקודקוד ה-1 לאחרון - אם לא דחה;**קבל.**

מבחינת סיבוכיות: ניחוש n*, בדיקה שמופיע פעם אחת-n^2,מעבר סמוכים ובדיקה שכנות n^2.

השפה G מכיל קליקה בגודל k או קבוצה ב"ת בגודל k אי שניהם -

מבחינת אלגוריתם: קליקה נחש קבוצה S של k קודקודים;בדוק שהם שונים;עבור כל זוג בדוק שמחוברים בצלע;אם עברת על כולם ולא דחה אז קבל; IS-בדוק במטר' שכנויות שלא מחוברים בצלע;אם לא נמצא זוג מחובר-קבל;אחרת דחה;

השפה Dominating Set' בגודל מקסימום K. מבחינת אלגוריתם: נחש קבוצה S בגודל K של קודקודים;בדוק שהם שונים-אחרת דחה;עבור כל קודקוד בדוק האם הוא שייך S-S אם כן-עבור הלאה; אחרת עבור כל שכן u של v;בדוק ש-u שייך S-S (יציאה מלולאה);אם לא נמצא שכן של v השייך S-S-דחה; מבחינת בנייה- דוגמה: נתון גרף G מוגדר:ניקח את G;נמחק קודקודים בודדים;נוסיף כנגד כל צלע {vi,vj} ל-G קודקוד נוסף בשם vij ונחבר אותו עם הקודקודים {vi,vj};נשים לב שאם יש קבוצה שלטת S בגודל K בגרף G' אזי לפי הגדרת קבוצה שלטת, כל קודקוד של G' נמצא בקבוצה או שכן שכן של קודקוד בקבוצה;

מבחינת סיבוכיות: בניית גרף חדש - העתקה של הגרף הקודם (גודל הקלט) + הוספה של n^2 קודקודים וצלעות לכל היותר ולכן חסומה בגודל הקלט.

השפה IS בגודל 5 לפחות מבחינת אלגוריתם: עבור על כל תת קבוצה של 5 קודקודים בגרף;(לולאה) בדוק עבור כל זוג שלא מחוברים בצלע;אם נמצאו שנים מחוברים-המשך לקבוצה הבאה;אחרת קבל.

השפה Almost IS - מבחינת אלגוריתם: נחש קבוצה קודקודים S בגודל K;בדוק שכולם שונים-אחרת דחה;הגדר מונה 0-0;עבור כל זוג קודקודים ב-S בדוק שלא מחוברים בצלע;(כניסה ללולאה);אם מחוברים-עלה מונה ב-1;אם c>2 דחה; מבחינת בנייה: כאשר 'G ויש כמו G עם תוספת של 2 קודקודים חדשים המחוברים רק ביניהם.

השפה היא פסוק של CNF שיותר מ-3\4 ההשמות לפסוק מספקות נקודות לפני:

- כאשר נתן לנו רק CNF לא ידוע לנו כמה משתנים יש בכל פסוקית או בכללי.
- נתון לנו CNF לא ידוע כמה משתנים יש אבל אנחנו יודעים שיש לנו 3 ליורלים בכל פסוקית.
- כדי שבעיה תהיה ב-NP יש להראות שלכל קלט x יש ע"ד y שמקיים את התנאי.
- סך האפשריות להשמה ה-n משתנים זה 2 בחזקת n אפשריות השמה.
- במקרה שלנו העד הוא 3\4 לכן זה יהיה 2 בחזקת n כפול 3\4 ולכן אקספו' בגודל הקלט ולכן לא ניתן לתת עד המעיד על שייכות ל-x. כלומר -NPH.

בניית רדוקציה:

- הפסוק בנוי מורכב מ-m פסוקיות, אז לכל פסוקית נוסף 2 משתנים. כלומר עכשיו יש לכל הפסוק 2 בחזקת 2+n. משמע גם מספר ההשמות האפשרי.
- מתוכן ההשמות האלו בהכרח 2 * 3 בחזקת m מספקות כי 4 מתוך 3 האפשריות שלי ייספקו את הפסוקי. ולשאר ה המשתנים שיהיה כל קומבינציה אפשרית. סה"כ קיבלנו ש: 3 * 2 בחזקת m מההשמות מספקות מתוך 2*4 בחזקת n ולכן בדיוק 3\4 מכלל ההשמות הן מספקות.

השפה היא ש-G מורכב מרכיבי קשירות זרים שכולם בגודל k לפחות שייך ל-P;מצא את כל רכיבי הקשירות באמצעות BFS;אם קיים רכיב שיש בו פחות מ-k קודקודים-דחה;עבור כל רכיב C(לולאה) בדוק עבור כל זוג קודקודים ב-C שהם מחוברים בצלע; אם נמצאו שנים שאינם מחוברים-דחה;(יציאה מלולאה);קבל

השפה היא ש-G שיש קליקה בגודל k וגם IS בגודל 2k שייך ל-NPC;נחש קבוצה C בגודל K של קודקודים;בדוק שכל הקודקודים שונים;עבור כל זוג בדוק שמחוברים בצלע;אם יש שנים שלא-דחה;נחש קבוצה S בגודל 2K;בדוק שהם שונים;עבור כל זוג ב-S בדוק שלא מחוברים בצלע;אם יש שנים מחוברים-דחה; מבחינת בנייה:נראה רדוקציה מקליקה מוגדרת ע"י כאשר 'G הוא גרף הזהה ל-G עם עוד 2k קודקודים בודדים;

נתון G ו-k1 ו-k2 כך ש-G יש לפחות k2 קליקות בגודל k1 שייכת ל-NPH;ולא ל-NP;נימוק למה לא ב-NP- כדי לנחש אז לקבל על המעיד על שייכות לשפה יש לתת עד או לנחש k2 קליקות בגודל k1;כמות הקליקות בגודל k1 בגרף יכולה להיות n בחזקת k1 מה שיכול להיות אקספו';נוכיח שהיא שקשה, רדוקציה מקליקה מוגדרת על ידי $\langle G, K, 1 \rangle$;תקפות: $\langle G, K \rangle$ שייך לקליקה אם"ם קיימת ב-G לפחות קליקה 1 בגודל k אם"ם $\langle G, K, 1 \rangle$ שייך ל-L3;

השפה: $\langle G, K \rangle$ כך - G לא מכוון יש קליקה בגודל k וגם כל השאר n-k הקודקודים הם בודדים.

שייכת ל-P-אלגו';חשב את מספר הקוד';הגדר מונה ל-0;עבור כל הקוד'(לולאה) בדוק מספר שכנים;אם הם שווים ל-0 מונה++;אחרת אם מספר השכנים אינו k-1 דחה(יציאה מלולאה) אם c הוא n-k קבל;אחרת דחה;

השפה $\langle G, K, m \rangle$ גרף לא מכוון יש בו קליקה בגודל k ובנו דרגת כל קודקוד היא לכל היותר m.

מניחים ש: NP !=P;זו בעיה פתוחה נראה ששיכות השפה ל-P גוררת P=NP;נראה שהשפה היא NPC נראה ש"ד; עבור על כל הקודקודים ובדוק שדרגתם היא מקסימום m-אם לא-דחה;נחש קבוצת קוד' S בגודל k;בדוק שכל הקודקודים בקבוצה שונים-אם לא-דחה;עבור על כל זוג קודקודים ב-S ובדוק שהם מחוברים בצלע-אם לא-דחה;קבל; **בנייה:כאשר** $\langle G, k, n \rangle$ כאשר m מספר הקוד' ב-G.

השפה n1,n2> כך שיש לפחות common prime factors

נזכיר כי קיים אלגוריתם A הבודק האם מספר ראשוני בסיבוכיות פולינומית, נראה שהשפה ב-NP. נגדיר אי"ד, על קלט <n1,n2>, אלגו', נחש 2 מספרים p1'p2 סיבוכ'-log1 בין 1 ל-n1 ובדוק שהם שונים log^2 p2 אם לא - דחה, הפעל את אלגוריתם A על p1 אם דחה - דחה, הפעל את אלגוריתם A על p2 אם דחה - דחה, בדוק האם n1 מתחלק ב-p1 ללא שארית והאם n1 מתחלק ב-p2 ללא שארית אם לא-דחה,בדוק האם n2 מתחלק ב-p1 ללא שארית והאם n2 מתחלק ב-p2 ללא שארית-אם לא-דחה, קבל.

סדר"פ הוכחת סיווג R,coRE:

1. אם מוכיחים $L \notin R$ לבנות את הרצה מבוקרת ולהראות $L \notin RE$