<u>חישוביות וסיבוכיות – תרגיל 3</u>

1)

על מנת להוכיח כי $S_1 \cup S_2 \in NPC$ נצטרך להראות 2 דברים:

1) $S_1 \cup S_2 \in NP$
2) $S_1 \cup S_2 \in NPH$

<u>נראה כי $S_1 \cup S_2 \in NP$ - (זאת אומרת כי קיים מוודא בזמן פולינומי)</u>

ידוע כי $S_1, S_2 \in NPC \rightarrow S_1, S_2 \in NP$ זאת אומרת שלשניהם קיים מוודא בזמן פולינומי.
לכן נגדיר את המוודא עבור $S_1 \cup S_2$ כך –

המוודא יקבל (x, y) נשלח למוודא של S_1 אם המוודא מחזיר 1 אזי גם המוודא שלנו יחזיר 1.

אם לא, נשלח למוודא של S_2 אם המוודא יחזיר 1 אזי גם המוודא שלנו יחזיר 1.

אחרת, נחזיר 0.

<u>כעת נראה כי $S_1 \cup S_2 \in NPH$ -</u>

נעשה זאת ע"י רדוקציה מ S_1 זאת אומרת $S_1 \leq_m^p S_1 \cup S_2$.

הגדרת הרדוקציה:

הרדוקציה בודקת עבור הקלט האם הוא שייך ל S_3 -

אם הוא שייך – היא תחזיר את הקלט הזה.

אם הוא **לא** שייך – הרדוקציה תחזיר קלט x כך ש $x \notin S_1 \cup S_2$

הוכחת נכונות:

ראשית בהכרח קיימת מילה x כך ש $x \notin S_1 \cup S_2$ מכיוון שאנו יודעים כי עבור כל העולם בו אנו מתעסקים $S_1 \cup S_2 \neq U$ (האיחוד הוא אינו כל העולם) ולכן בהכרח קיים x שאינו שייך לאיחוד, בנוסף אנו יודעים כי הגודל שלו הוא קבוע ולכן נוכל למצוא אותו בזמן פולינומי.

הרדוקציה תפעל בזמן פולינומי מכיוון שהיא רק בודקת שייכות לקבוצה S_3 וידעו כי $S_3 \in P$ סימן שקיים אלגוריתם פולינומי מכריע, ובנוסף בחירת המילה שאינה שייכת תתבצע גם כן בזמן פולינומי.

כעת נוכיח את נכונות הרדוקציה עצמה –

<u>כיוון ראשון - $x \in S_1 \to x \in S_1 \cup S_2$ -</u>

על פי הגדרת הרדוקציה הקלט x ייבדק האם שייך ל S_3 והוא אכן יהיה שייך לו כי נתון לנו בשאלה כי $S_1 \subseteq S_3$ ולכן הרדוקציה תחזיר לנו את x שאנו אכן כבר יודעים כי הוא שייך לאיחוד (כי הוא שייך לאחת מקבוצות האיחוד)

<u>כיוון שני - $x \notin S_1 \to x \notin S_1 \cup S_2$ -</u>

על פי הגדרת הרדוקציה הקלט x ייבדק האם שייך ל S_3 והוא לא יהיה שייך ל S_3 מכיוון שאנו יודעים שהוא לא שייך ל S_1 ונתון בשאלה כי $S_1 \subseteq S_3$ ולכן הרדוקציה תחזיר פלט כך שאינו שייך ל $S_1 \cup S_2$ וזה גם מה שאנחנו בודקים.

2)

ראינו בתרגול כי קיימת בעיה R_2 שמגודרת באופן הבא:

$$R_2=\{(x,\mathrm{y})\,||\,y|\le g(|x|)\wedge V(x,\mathrm{y})=1\vee V'(x,\mathrm{y})=1\}$$

ואין לה רדוקציה עצמית (מכיוון שבעיה זאת שייכת ל PC אך לא שייכת ל PF ו S_R שייכת ל p ואלו בדיוק התנאים שראינו להגדרה שאומרת שעבור תנאים אלו לבעיה אין רדוקציה עצמית).

כעת נגדיר בעיה נוספת R_1 באופן הבא:

$$R_1=\{(x,\mathrm{y})\,|\,x\in S\wedge y=1\}$$

נגדיר את הרדוקציה העצמית כך –

$S_{R_1}\in P$ ולכן קיים אלגוריתם מכריע בזמן פולינומי, שבהינתן קלט x ל R_1 ניגש לאורקל ובודק האם כן או לא.

אם כן – אז הרדוקציה תחזיר $(x,1)$

אם לא – אז הרדוקציה תחזיר $(x,0)$

<u>הוכחת נכונות –</u>

אם $x\in R_1$ אזי $x\in S\wedge y=1$ ולכן אם $x\in s$ אזי הרדוקציה תחזיר $f(x)\in S_R\leftarrow(x,1)$

אם $x\notin R_1$ אזי $x\notin S\vee y\neq 1$ ולכן לא קיים אלגוריתם שמכריע והרדוקציה תחזיר $(x,0)$

כעת נשאר להוכיח כי R_1,R_2 הן בעלות אותה בעיית הכרעה, למדנו כי בעיות הכרעה זה בעצם קבוצת קלטים של בעיות חיפוש, ולכן אם קבוצות הקלטים של 2 בעיות שוות אזי הן אותה בעיית הכרעה.

ועל פי ההגדרות שלנו אכן קבוצות הקלטים זהות ועבור אותה מילה שניהם יחזירו 0 או שניהם יחזירו 1 אזי הם אכן שייכים לאותה בעיית הכרעה.

(3

על מנת להראות כי אכן $AlwaysSAT \in CONP - C$ נוכיח 2 דברים:

1) $AlwaysSAT \in CONP$

2) $\overline{AlwaysSAT} \in NPC \rightarrow AlwaysSAT \in CONP - H$

ראשית נוכיח כי $AlwaysSAT \in CONP$ -

על פי הגדרה של CONP פשוט נראה כי $\overline{AlwaysSAT}$ שייך לNP

בעצם $\overline{AlwaysSAT}$ אומר כי עובר הנוסחה המתקבלת קיימת השמה שלא מספקת אותה.

הגדרת מוודא עבור $\overline{AlwaysSAT}$:

המוודא יקבל את הנוסחה והשמה, אם ההשמה לא מספקת הוא יחזיר 1, ואם היא מספקת הוא יחזיר 1.

כעת נוכיח כי $\overline{AlwaysSAT} \in NPC$ -

נבצע רדוקציה מSAT (שאנו כמובן יודעים שהיא NPC)

הגדרת הרדוקציה:

הרדוקציה תקבל נוסחה x ותחזיר $\overline{x}$

(הרדוקציה פועלת בזמן פולינומי מכיוון שהיא רק מחזיר את השלילה של הנוסחה)

הוכחת נכונות לרדוקציה: נוכיח את 2 הכיוונים

כיוון ראשון $x \in SAT \rightarrow f(x) \in \overline{AlwaysSAT}$ -

נתון כי קיימת השמה מספקת עבור x כעת לאחר הרדוקציה נקבל את $\overline{x}$ וכעת אנו יודעים כי עבור אותה השמה בהכרח היא לא מספקת, זאת אומרת שקיימת השמה לא מספקת וזה בדיוק $f(x) \in \overline{AlwaysSAT}$

כיוון שני $x \notin SAT \rightarrow f(x) \notin \overline{AlwaysSAT}$ -

נתון כי לא קיימת השמה מספקת, כלומר עבור כל השמה נקבל בחזרה 0. לאחר הרדוקציה נקבל $\overline{x}$ ולכן נקבל עבור כל השמה בחזרה 1. ולכן לא תהיה קיימת השמה שתחזיר 0 ולכן $f(x) \notin \overline{AlwaysSAT}$.

4)א(

*נגדיר מראש לסעיף זה כי הפונקציה של רדוקציית קארפ היא h והפונקציה של רדוקציית קארפ החלשה היא f

הוכחה, יהיו S,S' בעיות הכרעה, נניח כי קיימת רדוקציית קארפ מ S' ל S זאת אומרת $x\in S'\leftrightarrow h\left(x\right)\in S$.

<u>הגדרת הרדוקציה החלשה:</u>

הרדוקציה תפעיל את רדוקציית קארפ ותתעלם מy.
(זאת אומרת תפעיל את h על x)

<u>הוכחת נכונות:</u>

נוכיח את התנאים עבור רדוקציית קארפ החלשה, נוכיח 2 את הכיוונים –

<u>כיוון ראשון $x\in S'\rightarrow f\left(x,y\right)\in S$ -</u>

נתון כי $x\in S'$ ולכן הפונקציה f תפעילה את h עם x וy כלשהו לא משנה מה, כעת ידוע לנו כי קיימת רדוקציית קארפ מS' ל S ולכן ידוע כי $x\in S'\rightarrow h\left(x\right)\in S$ וזה בעצם אם נתעלם מy בדיוק כמו שרצינו להראות $x\in S'\rightarrow f\left(x,y\right)\in S$.

<u>כיוון שני $x\in\notin S'\rightarrow f\left(x,y\right)\notin S$ -</u>

נתון כי $x\notin S'$ ולכן הפונקציה f תפעילה את h עם x וy כלשהו לא משנה מה, כעת ידוע לנו כי קיימת רדוקציית קארפ מS' ל S ולכן ידוע כי $x\notin S'\rightarrow h\left(x\right)\notin S$ וזה בעצם אם נתעלם מy בדיוק כמו שרצינו להראות $x\in\notin S'\rightarrow f\left(x,y\right)\notin S$.

בהכרח הרדוקציה הינה בזמן פולינומי כי רק משתמשת ברדוקציה אחרת שבהכרח גם היא בזמן פולינומי.

4)ב)

שקילות לבעיה פתוחה,

נוכיח כי הוכחה בסעיף זה שקולה להוכחה כי $NP = CONP$

נוכיח את 2 הכיוונים –

<u>כיוון ראשון, נניח כי $NP = CONP$ ונוכיח את סעיף זה –</u>

יהיה בעיה $S \in NPC$ אנו יודעים כי קיימת רדוקציית קארפ בכל בעיה בNPC אליה.
בנוסף אנו יודעים על פי סעיף א כי אם קיימת רדוקציית קארפ מ S' ל S אזי קיימת גם רדוקציית קארפ חלשה מתאימה.

בנוסף, אנו יודעים כי $S \in NPC$ ולכן $S \in NP$ ובנוסף להנחה הראשונה שהנחנו אנו יודעים כי $S \in CONP$ ולכן נשים לב כי $S \in NP \cap CONP$.

ולכן הוכחנו כי קיימת $S \in NP \cap CONP$ כך שלכל $S' \in NP$ קיימת רדוקציית קארפ חלשה מתאימה.

<u>כיוון שני הוכחת סעיף זה גוררת כי $NP = CONP$ -</u>

נניח כי $S \in NP \cap CONP$ כך שלכל $S' \in NP$ קיימת רדוקציית קארפ חלשה מ S' ל S
ונרצה להראות כי $\overline{S'} \in NP$ שכמובן זה גורר כי $NP = CONP$.

יהי $S' \in NP$ כלשהו, לכן על פי ההנחה קיימת רדוקציית קארפ חלשה מS' לS.
מכיוון ש $S' \in NP$ זאת אומרת שקיים מוודא V כך ש:

$$\forall x \in S' \quad \exists y \quad |y| \le p(|x|) \text{ ו } \forall x \notin S' \quad \forall y \quad V(x,y) = 0$$

כעת נשים לב כי
$$S \in NP \cap CONP \to S \in NP \wedge S \in CONP$$
$$\to \overline{S} \in NP \wedge \overline{S} \in CONP \to \overline{S} \in NP \cap CONP$$

זאת אומרת כי קיימים מוודאים גם לS וגם ל $\overline{S}$.

<u>כעת נגדיר את המוודא עבור $\overline{S'}$:</u>

המוודא יקבל x וגם זוג של y ו 'y.

ייבצע את $f(x,y)$ וישמור את תוצאתו (p), אם התוצאה היא $\perp$ אזי המוודא יחזיר 0, אחרת המוודא יחזיר את $V_{\overline{S}}(p, y')$

הוכחת נכונות:

כיוון ראשון $x \in \overline{S'} \rightarrow V_{\overline{S'}}\left(x,\left(y, y'\right)\right)=1$ –

$$x \in \overline{S'} \rightarrow \exists y \quad f\left(x, y\right) \notin S \rightarrow f\left(x, y\right) \notin \overline{S} \rightarrow f\left(x, y\right) \neq \perp \rightarrow$$
$$\exists y' \quad V_{\overline{S}}\left(f\left(x, y\right), y'\right)=1 \rightarrow V_{\overline{S'}}\left(x,\left(y, y'\right)\right)=1$$

כיוון שני $x \notin \overline{S'} \rightarrow V_{\overline{S'}}\left(x,\left(y, y'\right)\right)=0$ -

$$x \notin \overline{S'} \rightarrow \forall y \quad f\left(x, y\right) \neq \perp \rightarrow V_{\overline{S}}\left(p, y'\right)=0 \rightarrow V_{\overline{S'}}\left(x,\left(y, y'\right)\right)=0$$

בנוסף המוודא פועל בזמן פולינומי כי הוא משתמש ברדוקציה ומוודא שגם הם בזמן פולינומי.

4)ג)

הוכחה,

נגדיר את S להיות $S \subseteq \sum^*$ (אך לא שווה, וגם לא שפה ריקה). כעת נניח כי $S \in P$ זאת אומרת שקיים אלגוריתם פולינומי שמכריע את S.

ראשית נבחר את מילים x,y כך ש $x \in S, y \notin S$.

בנוסף נשים לב כי אם $S' \in NP \cap CONP$ אזי קיים מוודא $V_{S'}$

וכך גם אם $\overline{S'} \in NP \cap CONP$ אזי קיים מוודא $V_{\overline{S'}}$

<u>כעת נגדיר את רדוקציית קארפ החלשה כך –</u>

נקבל x,y הרדוקציה תריץ את המוודא $V_{S'}$ על x ו y ואם הוא יחזיר 1 אזי הרדוקציה תחזיר את p

אם היא מחזירה 0, אזי נריץ את המוודא $V_{\overline{S'}}$ על x וy ואם הוא יחזיר 1 אזי הרדוקציה תחזיר את q.

אחרת, הרדוקציה תחזיר $\perp$.

*בהכרח זה יעבוד כי זאת רדוקציית קארפ חלשה וקיים y כלשהו שזה יעבוד עבורו.

הוכחת נכונות: נוכיח את 2 הכיוונים

<u>כיוון ראשון</u> $\underline{x \in S' \to f(x,\mathrm{y}) \in S}$ -

נניח כי $x \in S'$ ובנוסף אנו יודעים כי $S' \subseteq NP \cap CONP$ ולכן אנו יודעים כי

$$\exists y\ V_{S'}(x,\mathrm{y}) = 1 \to \exists y\ f(x,\mathrm{y}) = p \to f(x,\mathrm{y}) \in S$$

<u>כיוון שני</u> $\underline{x \notin S' \to f(x,\mathrm{y}) \notin S}$

נניח כי $x \notin S'$ ובנוסף אנו יודעים כי $\overline{S'} \subseteq NP \cap CONP$ ולכן אנו יודעים כי

$$x \in \overline{S'} \to \exists y\ V_{\overline{S'}}(x,\mathrm{y}) = 1 \to \exists y\ f(x,\mathrm{y}) = q \to f(x,\mathrm{y}) \notin S$$

בנוסף אנו יודעים כי לפי הגדרת המוודא כי $\exists y\ V_{S'}(x,\mathrm{y}) = 1$ ולכן קיים פולינום p (לא האיבר שהגדרנו קודם) כך שלכל $x \in \{0,1\}^*$ קיים $y \in \{0,1\}^*$ $|y| \le p(|x|)$ (חסום פולינומית ע"י x) כך ש $f(x,y) \neq \perp$. וזהו התנאי הראשון של רדוקציית קארפ חלשה.