שאלה 3. בהינתן גרף לא מכוון וממושקל $G=(V,E)$ עם פונקצית משקל $w: E \to \mathbb{R}_+$ ותת־קבוצה של קודקודיו $M \subseteq V$, נאמר כי תת־גרף T של G מקשר את הקבוצה M אם T הוא גרף קשיר שמכיל את כל קודקודי M. נגדיר את בעיית ההכרעה הבאה:

$$\text{ConnectGraph} = \left\{ ((G,w),M,k) \;\middle|\; \begin{array}{c}\text{קיים תת־גרף } T \text{ של } G \text{ עם משקל לכל היותר } k \\ \text{שמקשר את } M.\end{array} \right\}$$

תחת ההנחה כי $P \neq NP$, האם הבעיה הינה NP־שלמה? הוכחנה את תשובתן.

טענה: הבעיה היא NP שלמה.

הוכחה:

נראה אוראקל פולינומי V_S לבעיה שמקבלת כקלט את הגרף G, המשקלים w, קבוצה M, k ולדות T - תת גרף של G.

$V_S(((G,w),M,k),T)$:

① נבדוק את תקינות הקלט: T אכן תת גרף של G, ושהוא גם קשיר וחסר מעגלים. אם לא - נחזיר 0.

② נבדוק כי כל קודקוד M מופיע ב- V_T ומחובר ב- T. אם לא, נחזיר 0. (ניתן לעשות פעולות ע"י הרצת BFS/DFS)

③ נבדוק כי סכום משקלי כל הצלעות ב- E_T הוא לכל היותר k. אם לא, נחזיר 0.

עלות שלב ①: $O(V_T+E_T)$ ← הוא גרף חסר מעגלים.
עלות שלב ②: מריצים BFS ובודקים שיש מסלול בין כל פעם קודקודים מ- M: $O(V_T+E_T)$
עלות שלב ③: $O(E_T)$

כל הבדיקות נעשות בזמן פולינומי ⇐ האוראקל פולינומי.

נראה SENPH ע"י רדוקציה מ- VC. בהינתן (G,k) ל- VC נבנה את גרף G':

① נוסף קודקודים שמייצגים את הקשתות: לכל קשת e יש קודקוד v_e, $V' = V \cup \{v_{\{u,v\}} \mid \{u,v\} \in E\} \cup \{s\}$
ונוסיף קודקוד נוסף - s.

② נוסף קשתות מקודקוד לקודקוד שמייצגים קשתות אליה הוא שייך. $E' = \{\{u, v_{\{u,v\}}\} \mid \{u,v\} \in E\} \cup \{\{s,u\} \mid u \in V\}$.
וגם נחבר בין s לשאר הקודקודים בגרף.

③ נגדיר את פונקציות המשקלים באופן הבא-

$$w(e) = \begin{cases} 1 & \{u, v_{\{u,v\}}\} \in E' \\ \frac{1}{k+1} & \{s,u\} \in E' \end{cases}$$

④ $M = \{v_{\{u,v\}} \mid \{u,v\} \in E\}$

⑤ $k' = \frac{k}{k+1} + |E|$

⑥ לבסוף נחזיר: $((G' = (V',E'), w), M, k')$

הרפוקציה פשוטה: עוברים על כל הקשתות וינתקים להן קודקודים, מתבדים אותן ע"י קודקודים שאותם הן משתיכות (מעבר על M) ומתבדים אות S לכל הקודקודים. סה"כ פשוט באורך הקלט.

<u>פונקציה לדוגמה:</u>

$k' = \frac{2}{3} + 4$

$k = 2$

<u>הוכחת נכונות הרפוקציה:</u> $(G,k) \in VC \iff f(G) \in CG$.

$\Leftarrow$ נניח $(G,k) \in VC$. אזי קיימת קבוצה של k קודקודים שאותה ניתן לכסות את כל קשתות המשולש. נסתכל על הקודקודים האלו במשולש G הנוצר ע"י $f(G)$. מכיוון שהם מכסים את כל הקשתות, אזי קיימת קשת בין כל קודקוד בקבוצה הזו לכל קודקוד שמייצג קשת $e \in V$ (כי זה כיסוי).

מכיוון שישנם $|E|$ קודקודים שמייצגים את הקשתות, ניתן לחבר אותם לקבוצת הקודקודים בכיסוי ע"י $|E|$ קשתות שאורכן 1 (לפי הפונקציה)

כל קודקוד בכיסוי מחובר ל- S עם קשת באורך $\frac{1}{k+1}$ (יש k קב' כאלו) ולכן קודקודי - M מחוברים ל-S באמצעים דרך קבוצת קודקודי הכיסוי, וסכום הקשתות באמצעים: $|E| + \frac{k}{k+1}$

<u>טענה</u>: אוסף הקודקודים והקשתות שבחרנו, נסמנם ב- T, הוא תת"ג של G' עם משקל k לכל היותר שמקשר את M.

- T מכיל רק את קודקודי G', והראנו שסכום הקשתות באוסף הזה הוא $|E| + \frac{k}{k+1} = k'$.
- מקשר את M: מכיל את כל קודקודי M ומשמר קשיר כי קיימת קשת N-S לכל קודקוד בכיסוי, וקיימת קשת מכל קודקוד $v_{\text{נמצא}}$ לקודקוד אחד מהכיסוי (אם לא, זו סתירה לכך שהקבוצה היא VC).

הראנו שקיים T כמו שביקשו ולכן $f(G) \in CG$

$\Rightarrow$ $f(G) \in CG$. יש $|E|$ קודקודים בקבוצה M שצריך לקשר. אין בינהם קשתות, לכן עלינו לקשר אותם צריך להשתמש ב- $|E|$ קשתות לפחות שמחוברות ל- M, באורך 1.

אם נשתמש ביותר מקשת אחת לכל קודקוד- נקבל סכום משקלים גדול יותר מ- $|E|+1$ שגדול מ- $|E| + \frac{k}{k+1}$ המסתיר ל-k'. (שהשתמשתי ב- $f(G)$). לכן נחבר את כל קודקודי M בקשת אחת בדיוק במשקל 1.

יתר על שהשלמת קשיר, לכן נצטרך להוסיף קשתות עד מנת להפוך אותו לקשיר. את כל הקודקודים שחברנו אליהם את קודקודי M נקשר ל-S. המשקל הכולל של הקשתות מהקבוצה הזו לבין S הוא $\frac{k}{k+1}$ לפי הפונקציה G',

לכן סה"כ שמשקל כל קשת $\frac{1}{k+1}$, יש בדיוק k קודקודים המחוברים ל-S.

לכן קיבלנו k קודקודים שמכסים את כל הקשתות המשולש, הם מהווים VC, כי באופן אוטומטי ניתן לכסות את כל הקודקודים שמתאימים לקשתות שנמצאות ב- G - כנדרש. קיבלנו $(G,k) \in VC$

▨

שאלה 4. בהינתן קבוצה של מחרוזות $S \subseteq \{0,1\}^*$ ומחרוזת $x \in \{0,1\}^*$, נגדיר

$$\mathrm{d}(x,S) = \min_{y \in S}\{\mathrm{d}_{\mathrm{Ham}}(x,y)\}$$

כאשר $\mathrm{d}_{\mathrm{Ham}}$ הוא מרחק ההמינג בין x ו־y.
הוכיחו, הפריכו או הראו שקילות לשאלה פתוחה עבור כל אחת מהטענות הבאות:

א. לכל בעיית הכרעה S מתקיים:

$$S \in \mathrm{NPC} \Leftrightarrow \{x \mid \mathrm{d}(x,S) \le 1\} \in \mathrm{NPC}$$

ב. קיימת בעיה $S \in \mathrm{NPC}$ כך שגם הבעיה

$$S' = \{x \in \{0,1\}^* \mid \mathrm{d}(x,S) \le 99\}$$

היא NP־שלמה.

(א) **הפרכה:**

רסיון: Σ^* אינה שייכת ל- NPC כי אם הייתה $S \in NPC$ אום קיימת רדוקציה מקבלת קמ"ס ל- S.
יש שפה מלאה ולכן גם ניכל לנתם קלטים שאינם בשפה לקלטים שאינם ב-Σ^* לכן הרדוקציה
גם קיימת. נבחר בבעיה שידוע שהיא ב- NPC, למשל 3-SAT ונעזר במודל שלה בפתרון.

נתבונן בשפה: $S = \{0x \mid x \in \Sigma^*\} \cup \{1x \mid x \in 3\text{-SAT}\}$ כאשר $\Sigma = \{0,1\}^*$

טענה: $S \in NP$.

נראה מודל שיקבל כקלט מילה w ויכריע אם שייכת ל- S ואם לא.

$V_S(w)$:

① אם המילה מתחילה ב- 0, נחזיר 1. ← כל המילים שמתחילות ב- 0 שייכות ל- S.
② אם המילה מתחילה ב- 1, $w = 1x$, נפעיל את המודל של 3-SAT על x ונחזיר את תשובתו.

המודל פועל כיון שלפי ① הוא בדיקה ב- (1)O והמודל של 3-SAT פועל כי $3\text{-SAT} \in NP$.

נראה רדוקציה מ- 3-SAT ל- S שתקיים: $x \in 3\text{-SAT} \Leftrightarrow f(x) \in S$:

רדוקציה: בהינתן קלט x לרדוקציה, נחזיר $f(x) = 1x$. (מכיר שהרדוקציה פולינומית)

נכונות הרדוקציה:

$x \in 3\text{-SAT}$ אזי הפלט הוא $1x$ ולפי הגדרת השפה $1x \in S$.
$x \notin 3\text{-SAT}$ אזי הפלט הוא $1x$, גם אנו על הדרישה: $\{1x \mid x \in 3\text{-SAT}\}$ כי x אינו ב- 3-SAT, ושם מכוון שגם
מתחיל ב- 0 אז $\{0x \mid x \in \Sigma^*\} \not\ni 1x$ ולכן $f(x) \notin S$.

$x \notin 3\text{-SAT} \Rightarrow f(x) \notin S$. ולכן: $f(x) \in S \Rightarrow x \in 3\text{-SAT}$

טענה: $\{x \mid d(x,S)\le 1\} = \{0,1\}^*$

נוכיח הכלה דו־כיוונית:

$\{x \mid d(x,S)\le 1\} \subseteq \{0,1\}^*$ כי כל שפה מוכלת בשפת כל המילים הבינאריות.

$\{x \mid d(x,S)\le 1\} \supseteq \{0,1\}^*$ כי לפי הגדרת השפה - S:

1) מילה $x\in\{0,1\}^*$ שמתחילה ב-0 שייכת ל-S ולכן $d(x,S)=0\le 1 \Rightarrow x\in\{x \mid d(x,S)\le 1\}$
2) מילה $x\in\{0,1\}^*$ שמתחילה ב-1 ושייכת ל-SAT שייכת ל-S לפי הגדרת S ולכן כנ"ל $x\in\{x \mid d(x,S)\le 1\}$.
3) מילה $x\in\{0,1\}^*$ שמתחילה ב-1 ואינו שייכת ל-SAT רחוקה רק בביט הראשון (0) ממילה ב-S כי לכל $w\in\{0,1\}^*$: מתקיים ש:
$w\in S$ ו $w'=0\circ w$, עבור: $x=1\circ w$ ו $\delta(x,S)=\delta(x,w')=1$ ובפרט $x\in\{x \mid d(x,S)\le 1\}$

אופיוז כי $\{0,1\}^*$ אינה בעיה NPC כי הוינו בקורס מוצגים חישובים שאינו קיימת רדוקציה מ-$\emptyset$ ל-Σ^*.

לכן הראינו שקיימת $S\in NPC$ כך ש: $S\notin NPC$ $\{x \mid d(x,S)\le 1\}$ ופי **הפרכה**.

ב) הוכחה: באופן דומה, מכיוון ש- $VC\in NPC$ נוכל להגדיר בהתאמה את השפה הבאה-

$$S=\{\underbrace{1111\ldots1}_{100\text{ פעמים}}\circ x \mid x\in VC\}$$

נבנה מוודא $V_S(w)$ שמקבל כקלט מילה:

1. נבדוק שהמילה מתחילה ב-100 אותיות אחרות מעיר - 0.
2. עבור המילה x שמקיימת: $w=\underbrace{1111\ldots1}_{100\text{ פעמים}}\circ x$ נריץ את המוודא של VC עליה ונחזיר את תשובתו.

נוכיח כי $S\in NPC$ ע"י רדוקציה מ- VC ל- S: $x\in VC \Leftrightarrow f(x)\in S$

רדוקציה: נקבל כקלט x, ונחזיר $\underbrace{1111\ldots1}_{100\text{ פעמים}}\circ x$. (ברור שהרדוקציה פולינומית)

נכונות הרדוקציה:

אם $x\in VC$ אזי $\underbrace{1111\ldots1}_{100\text{ פעמים}}\circ x\in S$ לפי הגדרה.

אם $x\notin VC$ אזי $\underbrace{1111\ldots1}_{100\text{ פעמים}}\circ x\notin S$ לפי הגדרה.

כעת, הבעיה S': $S'=\{x\in\{0,1\}^* \mid d(x,S)\le 99\}$ נותר להראות ש- $S'\in NPC$.

נבנה מוודא: $V_{S'}(w,I)$: כאשר I הם האינדקסים בהם נשנה את w.

1. נבדוק ש- $|I|\le 99$, אם לא נחזיר 0.
2. נשנה את w במקומות שצוינו ב- I (נחליף את הביטים) ונפעיל על המילה שהתקבלה את המוודא של - S.
3. נחזיר את תשובתו של V_S על המילה החדשה.

כעת נראה רדוקציה מהבעיה S לבעיה 'S:

$$f(x) = \begin{cases} x \circ 1^{100} = x & x \circ 1 \circ 0^{99} \\ \text{else} & x \circ 0^{100} \end{cases}$$

למשל: $1^{100} = \underbrace{1111\ldots1}_{\text{100 פעמים}}$

(מהיר שהרדוקציה פולינומית)

הוכחת נכונות הרדוקציה:

$x \in S \iff f(x) \in S'$.

$\Leftarrow$ $x \in S$ אז היו מתקבלים $x \| 1^{100}$ כך ש- $x' \in VC$. הרדוקציה שולחת את x למילה: $f(x) = 0^{99} \circ 1 \circ x'$
ההפרש בין x לבין $f(x)$ הם ה- 99 ביטים הראשונים ולכן $H_d(f(x), S) = 99$. לכן $f(x) \in S$.

$\Rightarrow$ $x \notin S$
אם המילה x לא מתחילה ב- 100 אחדות אז הפלט הוא $x \| 0^{100}$. לכן ה- 100 ביטים הראשונים שונים מכל מילה ב-S ולכן $f(x) \notin S$. כי $H_d(S, x \| 0^{100}) \geq 1$.

אם המילה x מתחילה ב- 100 אחדות אבל משורשרת עם $x' \notin VC$. ולכן $0^{99} 1 x'$ נבדל ב- 99 ביטים בדיוק רק אם $1^{100} \circ x'$ היו מילה ששייכת לשפה. אבל ידוע ש- $x' \notin VC$ לכן $1^{100} \circ x' \notin VC$ וסה"כ נקבל $f(x) \notin S'$.

וסה"כ: הוכחנו את נכונות הרדוקציה. ▨