NP-completeness

תרגיל 1

הוכיחו שבעיית החיפוש של $3COL$ (כלומר, להחליט אם גרף הוא 3-צביע ואם כן לצבוע אותו), ניתנת לרדוקציה לבעיית ההכרעה. כלומר, בהינתן אלגוריתם פולינומי לבעיית ההכרעה **האם** גרף כלשהו הוא 3-צביע, נתאר אלגוריתם פולינומי למציאת צביעה כזו.

1. ניקח את האלגוריתם A שיודע לומר בזמן פולינומי האם גרף הוא 3-צביע. נניח ש-A רץ בזמן $O\big(f(n)\big)$.
2. נוסיף 3 קודקודים לגרף: $R,\ B,\ G$. 3 תתי-הקבוצות בגודל 2 הן: $C \coloneqq \big\{C_1 \coloneqq \{R,B\},\ C_2 \coloneqq \{B,G\},\ C_3 \coloneqq \{G,R\}\big\}$.
3. לכל C_i, נגדיר c_i את הצבע של הקודקוד שלא מופיע בו: $c_1 \coloneqq G, c_2 \coloneqq R, c_3 \coloneqq B$.
4. לכל $v \in V(G)$: זמן $O(n)$
   a. נגדיר קבוצה $B \coloneqq \emptyset$.
   b. לכל $C_i \in C$:
      i. נחבר את v לקודקודים של C_i ויהי G' הגרף המתקבל.
      ii. אם $A(G') = 1$, נגדיר $B \coloneqq B \cup \{c_i\}$. זמן $O\big(f(n)\big)$
      (כי זה אומר שיש צביעה כאשר v מחובר לשני הצבעים האחרים, כלומר יש צביעה כאשר v צבוע ב-c_i).
   c. נצבע את v באחד הצבעים שיש ב-B.

סה"כ זמן ריצה $O\big(n \cdot f(n)\big)$. אם f פולינומית, האלגוריתם פולינומי.

תרגיל 2

$$\text{3-CNF-SAT} \leq_p \text{NAE-4-CNF-SAT} \leq_p \text{NAE-3-CNF-SAT}$$

סעיף א: $\text{3-CNF-SAT} \leq_p \text{NAE-4-CNF-SAT}$

$$f\left(\underbrace{\left(\underbrace{(\ell_{1,1} \vee \ell_{1,2} \vee \ell_{1,3})}_{\varphi_1} \wedge \underbrace{(\ell_{2,1} \vee \ell_{2,2} \vee \ell_{2,3})}_{\varphi_2} \wedge \ldots \wedge \underbrace{(\ell_{m,1} \vee \ell_{m,2} \vee \ell_{m,3})}_{\varphi_m}\right)}_{\varphi}\right)$$
$$\coloneqq \underbrace{\left(\underbrace{(\ell_{1,1} \vee \ell_{1,2} \vee \ell_{1,3} \vee F)}_{\varphi_1'} \wedge \underbrace{(\ell_{2,1} \vee \ell_{2,2} \vee \ell_{2,3} \vee F)}_{\varphi_2'} \wedge \ldots \wedge \underbrace{(\ell_{m,1} \vee \ell_{m,2} \vee \ell_{m,3} \vee F)}_{\varphi_m'}\right)}_{\varphi'}$$

בגדול, פשוט נוסיף ליטרל שמקבל F לכל פסוקית.

אם φ ספיקה, זה אומר שיש השמה כך שבכל פסוקית יש T אחד לפחות. אז אותה השמה תספק גם את φ', ובגלל שהוספנו F, זו השמה NAE.

אם φ לא ספיקה, זה אומר שבכל השמה, יש פסוקית שמקבלת כולה F. אז גם בכל השמה שניתן ל-φ', תהיה פסוקית שהיא כולה F.

סעיף ב: $\text{NAE-4-CNF-SAT} \leq_p \text{NAE-3-CNF-SAT}$

$$f\left(\underbrace{\left(\underbrace{(\ell_{1,1} \vee \ell_{1,2} \vee \ell_{1,3} \vee \ell_{1,4})}_{\varphi_1} \wedge \underbrace{(\ell_{2,1} \vee \ell_{2,2} \vee \ell_{2,3} \vee \ell_{2,4})}_{\varphi_2} \wedge \ldots \wedge \underbrace{(\ell_{m,1} \vee \ell_{m,2} \vee \ell_{m,3} \vee \ell_{m,4})}_{\varphi_m}\right)}_{\varphi}\right) \coloneqq$$

נפצל כל פסוקית לשתי פסוקיות:

$$(\ell_{i,1} \vee \ell_{i,2} \vee \ell_{i,3} \vee \ell_{i,4}) \coloneqq \underbrace{(\ell_{i,1} \vee \ell_{i,2} \vee w_i)}_{\varphi_{i,1}'} \wedge \underbrace{(\ell_{i,3} \vee \ell_{i,4} \vee \overline{w}_i)}_{\varphi_{i,2}'}$$

אם φ ספיקה NAE, זה אומר שיש השמה כך שבכל פסוקית יש לפחות T אחד ו-F אחד. ניקח את ההשמה הזו ל-φ'.

אם תחת ההשמה, $\ell_{i,1} = \ell_{i,2}$, נוכל להגדיר $w_i \coloneqq \overline{\ell}_{i,1}$.

אם $\ell_{i,1} = T$, אז $w_i = F$ והחלק הראשון מסופק NAE. באופן דומה אם $\ell_{i,1} = F$.

ובגלל ש $\ell_{i,1} = \ell_{i,2}$, אז $\ell_{i,3}, \ell_{i,4}$ חייבים להיות אחד T ואחד F (כי φ המקורית ספיקה NAE). אז גם החלק השני מסופק.

אחרת, $\ell_{i,1} \neq \ell_{i,2}$ אז החלק הראשון מסופק NAE. ונוכל להגדיר $w_i \coloneqq \bar{\ell}_{i,3}$. ואז באופן דומה למצב הראשון, נקבל השמה מספקת NAE.

אם φ' ספיקה NAE, זה אומר שיש השמה כך שבכל חלק $(1,2)$ של כל פסוקית יש לפחות T אחד ו-F אחד.

נניח שבאחד החלקים, ה-F הוא w והשניים האחרים הם T. אזי בחלק השני, ה-w הוא T אז אחד האחרים הוא F. סה"כ בין 4 המקוריים יש T ו-F.

אם באחד החלקים, ה-T הוא w והשניים האחרים הם F, אזי בחלק השני ה-w הוא F אז אחד מהאחרים הוא T.

אחרת, בשני החלקים, השניים המקוריים הם אחד T ואחד F.

בכל מצב יש לנו במקוריים לפחות אחד T ואחד F, אז ההשמה הזו מספקת את φ.

תרגיל 3

צ"ל:

$$L \coloneqq \{(G,k)\colon\ k \in \mathbb{N}\ \ \wedge\ \ (\alpha(G) \geq k\ \ \vee\ \ \omega(G) \geq k)\} \in NPC$$

כלומר, בדיקה האם בגרף יש קבוצה בת"ל בגודל k **ו/או** קליקה בגודל k.

ראשית, נוכיח שהיא NP ע"י אלגוריתם וידוא: בהינתן קבוצת קודקודים, נבדוק אם הקבוצה בגודל k ויש 0 או $\binom{k}{2}$ צלעות.

נוכיח שהיא NPH ע"י רדוקציה משפה NPH אחרת. נוכיח $IS \leq_p L$.

בהינתן גרף על n קודקודים ומספר k, נגדיר:

$$f\big((G,k)\big) \coloneqq (G', k+n)$$

ונגדיר את G' להיות G בתוספת n קודקודים מבודדים.

נניח שיש ב-G קבוצה בת"ל בגודל k. אזי, הוספת n קודקודים מבודדים נותנת לנו קבוצה בת"ל בגודל $k+n$ ב-G'.

נניח שאין ב-G קבוצה בת"ל בגודל k. אזי, ב-G' לא תהיה קבוצה בת"ל בגודל $k+n$. וגם לא תהיה קליקה בגודל $k+n$ כי הוספנו n קודקודים מבודדים.

תרגיל 4

צ"ל:

$$L \coloneqq \{\varphi\colon \varphi\ \ is\ a\ CNF\ formula\ with \geq 2\ satisfying\ assignments\} \in NPC$$

שפת כל הנוסחאות CNF שיש להן לפחות 2 השמות מספקות.

נוכיח שהיא NP ע"י אלגוריתם וידוא: בהינתן 2 השמות, נבדוק אם הן שונות ומספקות.

נוכיח שהיא NPH ע"י רדוקציה משפה NPH אחרת: נוכיח $\text{CNF-SAT} \leq_p L$

בהינתן נוסחת CNF, נגדיר משתנה חדש x:

$$f(\varphi) \coloneqq \varphi \wedge (x \vee \bar{x})$$

אם φ ספיקה, אז גם החלק שהוא φ ב-$f(\varphi)$ יהיה ספיק עם אותה השמה. ונוסיף השמה ל-x: $x = T$ או $x = F$, בשני המקרים $f(\varphi)$ ספיקה וזה שתי השמות.

אם φ לא ספיקה, אז גם $f(\varphi)$ לא תהיה ספיקה (ובפרט אין לה 2 השמות מספקות).

תרגיל 5

צ"ל:

$$L \coloneqq \left\{G\colon \omega(G) \geq \frac{v(G)}{2}\right\} \in NPC$$

NP-completeness

שפת כל הגרפים שיש להם קליקה על לפחות חצי מהקודקודים.

נוכיח שהיא NP ע"י אלגוריתם וידוא: בהינתן קבוצת קודקודים, נבדוק אם היא קליקה בגודל המתאים.

נוכיח שהיא NPH ע"י רדוקציה משפה NPH אחרת: נוכיח $\text{CLIQUE} \leq_p L$

בהינתן (G,k), נגדיר:

אם $k = \frac{v(G)}{2}$, אז $f\big((G,k)\big) \coloneqq G$.

אם $k > \frac{v(G)}{2}$:

יהי G' הגרף המתקבל ע"י הוספת t קודקודים מבודדים ל-G.

אנחנו רוצים שאם ב-G הייתה קליקה בגודל k, אז ב-G' יש קליקה בגודל $\frac{v(G')}{2}$. כלומר נדרוש:

$$\frac{v(G')}{2} = \frac{v(G)+t}{2} = k \Longrightarrow v(G) + t = 2k \Longrightarrow t = 2k - v(G)$$

שזה חיובי, כי $k > v(G)/2 \Longrightarrow 2k > v(G)$.

ואם ב-G לא הייתה קליקה בגודל k, אז הוספת קודקודים מבודדים לא תשנה את זה ב-G'.

אם $k < v(G)/2$:

יהי G' הגרף המתקבל ע"י הוספת t קודקודים ל-G, שכל אחד מהם מחובר לכל השאר ולכל הקודקודים ב-G.

אנחנו רוצים שאם ב-G הייתה קליקה בגודל k, אז ב-G' יש קליקה בגודל $\frac{v(G')}{2}$.

בגלל שהוספנו t קודקודים שכל אחד מחובר לכל השאר ולכל הקודקודים ב-G, אז גודל הקליקה ב-G' יהיה $k + t$.

כלומר נדרוש:

$$\frac{v(G')}{2} = \frac{v(G)+t}{2} = k + 2 \Longrightarrow v(G) + t = 2k + 2t \Longrightarrow v(G) - 2k = t$$

שזה חיובי, כי $k < v(G)/2 \Longrightarrow 2k < v(G)$.

ואם ב-G לא הייתה קליקה בגודל k, אז הוספת K_t לא תייצר K_{k+t} ב-G'. (כי אחרת, הורדת ה-t קודקודים תשאיר K_k ב-G).

תרגיל 6

בעיית *subset-sum* מוגדרת:

$$SUSU \coloneqq \{(C,T)\colon\ C \subseteq \mathbb{N}, T \in \mathbb{N}, \exists S \subseteq C\ s.t. \Sigma_{s\in S} s = T\}$$

נתון לנו ש $SUSU \in NPC$ ע"י רדוקציה $\text{3-CNF-SAT} \leq_p SUSU$. ההוכחה כאן, בעמוד 1118 (טענה 34.15). והיא מגעילה. אל תנסו להבין אפילו.

בעיית $PARTITION$ מוגדרת:

$$PARTITION \coloneqq \left\{C\colon C \subseteq \mathbb{N}, \exists S \subseteq C\ s.t.\ \Sigma_{t\in S} t = \Sigma_{t\in C\setminus S} t\right\}$$

נוכיח שהיא NPC.

נוכיח שהיא NP ע"י אלגוריתם וידוא: בהינתן קבוצה S, נבדוק האם הסכום שלה הוא חצי סכום הקבוצה C.

נוכיח שהיא NPH ע"י רדוקציה $SUSU \leq_p PARTITION$:

ננתח את הבעיות: יהי (C,T) קלט לבעיית $SUSU$. באופן כללי, נגדיר $\Sigma_C \coloneqq \sum_{c\in C} c$.

אם $T = \Sigma_C/2$, סיימנו.

אם $T < \Sigma_C/2$ או $T > \Sigma_C/2$, אנחנו רוצים בעצם לשאול האם אפשר לחלק את C לשתי קבוצות: אחת בגודל T והשנייה בגודל $\Sigma_C - T$.

הבעיה היא ש-*partition* יודעת רק לחלק קבוצה לשני חלקים שווים. נניח ששמנו בקבוצה אחת T. בצד השני נשאר $\Sigma_C - T$.

אם $T < \Sigma_C/2$, זה אומר שנשאר בצד השני יותר מחצי הסכום. אז נרצה לאזן את זה עם משהו שנוסיף לצד של T. נוסיף משהו בגודל t:

$$T + t = \Sigma_C - T \Longrightarrow t = \Sigma_C - 2T$$

אם $T > \Sigma_C/2$, זה אומר שבצד השני נשאר פחות מחצי מהסכום. נרצה להוסיף t לצד הזה:

$$T = \Sigma_C - T + t \Longrightarrow t = 2T - \Sigma_C$$

אז בהינתן בעיית $SUSU(C,T)$, תלוי ביחס בין T ל-$\Sigma_C/2$, נייצר איבר t ואז נפתור את $PARTITION(C \cup \{t\})$.

לפי תהליך הבנייה, אם $(C,T) \in SUSU$ אז $(C \cup \{t\}) \in PARTITION$.

בכיוון השני, נניח ש $(C \cup \{t\}) \in PARTITION$. כלומר קיימת חלוקה $C = S_1 \uplus S_2$ כך ש $\Sigma_{S_1} = \Sigma_{S_2}$.

אנחנו צריכים להוכיח ש $(C,T) \in SUSU$.

אם $t = 0$, אז $T = \Sigma_C/2$ והחלוקה היא פתרון גם ל-*SUSU*.

אם $t = \Sigma_C - 2T$, נניח בה"כ ש- $t \in S_1$. אזי נגדיר $S \coloneqq S_1 \setminus \{t\}$ ונקבל:

$$\Sigma_{C \cup t} = 2\Sigma_{S_1} = 2(\Sigma_S + t) = 2(\Sigma_S + \Sigma_C - 2T) = 2\Sigma_S + 2\Sigma_C - 4T$$

וניזכר ש:

$$\Sigma_{C \cup t} = \Sigma_C + t = \Sigma_C + \Sigma_C - 2T = 2\Sigma_C - 2T$$

אז:

$$2\Sigma_C - 2T = 2\Sigma_S + 2\Sigma_C - 4T \Longrightarrow 2T = 2\Sigma_S \Longrightarrow T = \Sigma_S$$

כלומר S היא תת קבוצה של C בסכום T, כנדרש.

ואם $t = 2T - \Sigma_C$, נניח בה"כ ש- $t \in S_1$. אזי נגדיר $S \coloneqq S_2$ ונקבל:

$$\Sigma_{C \cup t} = \Sigma_C + t = \Sigma_C + 2T - \Sigma_C = 2T$$

ויש חלוקה לשתי קבוצות שוות, כלומר:

$$\Sigma_{S_1} = \Sigma_{S_2} = T$$

כלומר S היא תת קבוצה של C בסכום T, כנדרש.

תרגיל 7

בעיית תרגיל הגב בשלמים – *KNAPSACK*:

נתונה רשימה של מוצרים $A \coloneqq [n]$, רשימת ערכים $V \coloneqq (v_1, v_2, \dots, v_n)$ ורשימת משקלים $W \coloneqq (w_1, w_2, \dots, w_n)$,

כך שלמוצר i יש משקל w_i וערך v_i.

בנוסף, נתונים הגבלת משקל $C \in \mathbb{N}$ ורווח $P \in \mathbb{N}$. צריך לקבוע האם קיימת $B \coloneqq \{i_1, i_2, \dots, i_k\} \subseteq A$ כך ש:

$$\sum_{j=1}^{k} w_{i_j} \le C, \qquad \sum_{j=1}^{k} v_{i_j} \ge P$$

צ"ל: $SUSU \le_p KNAPSACK$

בהינתן $C \subseteq \mathbb{N}, T \in \mathbb{N}$ כך ש- $|C| = n$, נגדיר:

$$W \coloneqq V \coloneqq C, \qquad A \coloneqq [n], \qquad C \coloneqq P \coloneqq T$$

נניח ש- $(C,T) \in SUSU$, כלומר קיימת $S \subseteq C$ כך ש- $\Sigma_S = T$. אזי ניקח את B להיות האיברים המתאימים ל-S מתוך W ו-V, ונקבל:

$$\sum_{j=1}^{k} w_{i_j} = T \le C, \qquad \sum_{j=1}^{k} v_{i_j} = T \ge P$$

כנדרש.

נניח ש- $(A,W,V,C,P)\in KNAPSACK$. כלומר קיימת $B\coloneqq\{i_1,i_2,\dots,i_k\}\subseteq A$ כך ש:

$$\sum_{j=1}^{k} w_{i_j}\le C=T,\qquad \sum_{j=1}^{k} v_{i_j}\ge P=T$$

כלומר:

$$\sum_{b\in B} b\le T,\sum_{b\in B} b\ge T\Rightarrow\sum_{b\in B} b=T$$

כנדרש.

תרגיל 8

בהינתן גרף מכוון $D\coloneqq(V,E)$, קבוצה $K\subseteq V$ תיקרא $kernel$ של D אם:

$$\forall u,v\in K\colon(u,v)\notin E(D)$$

$$\forall v\in V\setminus K\colon\ \exists u\in K\ \ s.t.(v,u)\in E(D)$$

לכל שני קודקודים ב-K אין צלע ביניהן. ולכל קודקוד u שלא ב-K, קיים קודקוד v ב-K כך שיש צלע מ-v ל-u.

כלומר K היא קבוצה בת"ל ש"שולטת" על הגרף.

צ"ל:

$$KERNEL\coloneqq\{D\colon D\ is\ a\ directed\ graph\ with\ a\ kernel\}\le_p \text{CNF-SAT}$$

בהינתן גרף מכוון, נצטרך לבנות בשבילו נוסחת CNF מתאימה.

לכל $v\in V$, נגדיר משתנה x_v. אנחנו רוצים בעצם (אינטואיטיבית, לא פורמלית) שאם $v\in K$ אז $x_v=T$. ונגדיר פסוקיות שיתפסו את ההגבלות.

ההגבלות שלנו הן:

1. אם שני קודקודים ב-K, אז אין ביניהן צלע.
2. אם קודקוד לא ב-K, אז יש צלע מקודקוד כלשהו ב-K אליו.

הגבלה 1: לכל צלע $uv\in E$, נגדיר פסוקית. אנחנו רוצים שהפסוקית לא תסופק אמ"מ שניהם ב-K. כלומר אנחנו רוצים שרק אם שניהם T, הפסוקית מקבלת F, כלומר: $\overline{x_u\wedge x_v}$. אבל זה לא צורה של פסוקית CNF. נשתמש בחוקי דה-מורגן כדי לקבל:

$$\varphi_{uv}\colon=\overline{x_u\wedge x_v}=\bar{x}_u\vee\bar{x}_v$$

הגבלה 2: לכל $v\in V$ נגדיר פסוקית שתהיה T אם הקודקוד לא ב-K (כלומר הוא F) ויש צלע מקודקוד כלשהו ב-K אליו. אז הקודקוד עצמו נותן ליטרל חיובי – אם הקודקוד ב-K, הוא T ואז הפסוקית T (כי לא צריך שתהיה צלע). אם הקודקוד לא ב-K, הוא יהיה F, ואז צריך שתהיה צלע מקודקוד ב-K אליו. אז שאר הליטרלים בפסוקית יהיו כך שאם יש צלע מקודקוד ב-K ל-v, הליטרל יהיה T. ניקח את כל המשתנים שמייצגים קודקוד שיש צלע ממנו ל-v. מספיק שאחד מהם T (כלומר ב-K) והפסוקית תהיה מסופקת. כלומר נגדיר את החלק של השכנים:

$$\varphi_v\coloneqq\bigvee\nolimits_{u:uv\in E} x_u$$

והפסוקית כולה היא:

$$x_v\vee\varphi_v$$

בסה"כ, הביטוי שמייצג את הגרף:

$$f\big(D\coloneqq(V,E)\big)\coloneqq\bigwedge\nolimits_{v\in V}\varphi_v\wedge\bigwedge\nolimits_{uv\in E}\varphi_{uv}$$

תהליך הבנייה הוא $O(n^2)$ עבור הבנייה של הפסוקיות של הצלעות. ו-$O(n\cdot n^2)=O(n^3)$ עבור הבנייה של הפסוקיות של הקודקודים (לכל קודקוד נעבור על כל הצלעות). בסה"כ זמן $O(n^3)$, פולינומי.

נוכיח נכונות: נניח שהגרף הוא גרף מכוון עם $kernel$. נתאר השמה מספקת ל-$f(D)$:

לכל קודקוד ב-K נגדיר T. לכל קודקוד אחר נגדיר F.

כל הפסוקיות של הצלעות מסופקות כי לפי ההנחה, אין צלעות בתוך K אז אין פסוקית ששני הקודקודים T, אז אין פסוקית ששני הליטרלים ההפוכים הוא F, אז כל פסוקית כזו מסופקת.

כל הפסוקיות של הקודקודים מסופקות כי אם הקודקוד v ב-K אז הוא קיבל T, ואם הקודקוד לא ב-K אז הוא F אבל לפי ההנחה קיים קודקוד ב-K שיש ממנו צלע ל-v אז המשתנה של אותו קודקוד קיבל T.

כיוון שני: נניח שקיימת לנוסחה השמה מספקת. ניקח השמה כזו. בכל פסוקית של צלע יש T אחד לפחות, כלומר יש במשתנים שלה F אחד לפחות. ניקח את הקודקודים שקיבלו T ל-K. ובגלל שבכל צלע יש לפחות F אחד במשתנים, זה אומר שאין צלע ששני הקודקודים שלה ב-K.

וגם, כל הפסוקיות של הקודקודים מסופקות. אם המשתנה של הקודקוד מסופק, זה אומר שלקחנו אותו ל-K. אם הוא F, אז אחד המשתנים האחרים הוא T, כלומר יש צלע מקודקוד ב-K אל הקודקוד שלנו. כנדרש.

.