

סיכומים לבוחן בסיבוכיות

פרופ' עודד רגב, 08/05/09 (סמסטר ב')

חישוביות :

משימה חישובית :

חישוב פונקציה $f: \{0,1\}^* \rightarrow \{0,1\}^*$, לרוב פונקציות בוליאניות (טווח $\{0,1\}$). בצורה שקולה נגדיר שפה: $L_f = \{x \in \{0,1\}^* \mid f(x) = 1\}$. ידוע גם בשם בעיות החלטה/הכרעה. מודל חישובי: אלגוריתמים בשפת תכנות כלשהי / מכונת טיורינג, אין מגבלת זיכרון.

מכונת החישוב האוניברסלית :

כל תוכנית בשפת תכנות כלשהי ניתן לייצג ע"י מחרוזת של $\{0,1\}$. תהי α תוכנית, נסמן ב- M_α את האלגי המייצג תוכנית זו.

משפט (טיורינג) : קיים אלגי U שבהינתן $x, \alpha \in \{0,1\}^*$ - כלומר U מסמלץ את M_α על הקלט x . אם $M_\alpha(x)$ נתקע, גם U תתקע. רעיון ההוכחה: U עובר על התוכנית α ומסמלץ כל שורה בה. טיורינג הראה שניתן להריץ תוכנית על מחשב.

משפט טיורינג (לקיום פוני לא חשיבה) :

קיימת פוני $UC: \{0,1\}^* \rightarrow \{0,1\}^*$ שלא ניתנת לחישוב ע"י אף אלגוריתם (פוני חשיבה): פוני f שקיים עבורה אלגי M כך שלכל קלט $x: M(x)$ עוצר ומחזיר את $f(x)$.

הוכחה :

דרך א': חישובי עוצמות – גודל קבוצת הפונקציות היא א לעומת גודל קבוצת התוכניות שהיא \aleph_0 .

דרך ב': שיטת הלכסון: נציב בטבלה את כל האלגי $M_0, M_1, M_{00}, M_{01}, \dots$ אל מול כל הקלטים $0, 1, 00, 01, \dots$ ונגדיר את UC באופן הבא:

$UC(\alpha) = \begin{cases} 0, & M_\alpha(\alpha) = 1 \\ 1, & o/w \end{cases}$ - כלומר מחזיר תוצאה הפוכה לאלכסון, או תוצאה כלשהי (0 או 1) אם התוצאה על האלכסון מתבדרת. לפי בניה

זו, אף אלגי לא יחשב נכון את UC לכל קלט. מניחים בשלילה שקיים קלט β עבורו M_β מחשב את UC , ומגיעים לסתירה מבניית UC על הקלט β .

משפט : HALT אינה ניתנת לחישוב.

$HALT = \{ \langle \alpha, x \rangle \mid M_\alpha \text{ stops on } x \}$. נניח בשלילה שקיים M_{HALT} , ונראה כיצד ניתן לחשב את UC : בהינתן קלט α, M_{UC} מריץ את $M_{HALT}(\alpha, \alpha)$. אם התוצאה לא עוצרת, נעצור ונוציא 1. אם התוצאה עוצרת, נחשבה ונחזיר את ההיפך.

פרק ראשון: סיבוכיות זמן ריצה :

נסתכל לרוב על מחלקות של שפות, כלומר של פונקציות בוליאניות.

הגדרה :

עבור פוני $T: \mathbb{N} \rightarrow \mathbb{N}$ נגדיר $DTIME(T(n))$ בתור אוסף השפות שניתן לפתור אותן בעזרת אלגוריתם שרץ בזמן $c \cdot T(n)$ עבור קבוע c כלשהו.

המחלקה P :

- $P = \cup_{c \geq 1} DTIME(n^c)$: הגדרה זו תקפה לכל מודל חישובי, כגון שפת $C, JAVA, TM$ וכו'.
- BPP : מחלקת אלגוריתמים הרצים בזמן פולי ומשתמשים באקראיות (שאלה פתוחה: $P = BPP$).
- מחלקת BQP (שימוש בפיסיקה קוונטית).

המחלקה NP :

מחלקת השפות שניתן לוודא שייכות אליהן בזמן פולינומיאלי. כלומר, שפה $L \subseteq \{0,1\}^*$ היא ב- NP אם קיים פולינום $p: \mathbb{N} \rightarrow \mathbb{N}$ ואלגוריתם M הרץ בזמן פולי כך שלכל קלט $x \in \{0,1\}^*$: $M(x, w) = 1 \Leftrightarrow \exists w \in \{0,1\}^{p(|x|)}$. כלומר, האלגי בהינתן הקלט ועד באורך פולי לאורך הקלט יחזיר t (1) אמ"מ x בשפה.

דוגמאות לבעיות :

- **קבוצה ב"ת (IS) – בעיה ב-NPC**: בהינתן גרף לא מכוון G ומספר טבעי k , האם יש ב- G קבוצה ב"ת בגודל לפחות k (קבוצת קודקודים ללא קשתות). העד יכול להיות רשימה של k קודקודים. האלגי המוודא M יעבור על העד ויבדוק את תקינותו.
- **HamPath – בעיה ב-NPC**: בהינתן גרף לא מכוון G , האם קיים בו מסלול המילטוני – מסלול המבקר בכל קודקוד בדיוק פעם אחת.
- **HamCycle – בעיה ב-NPC**: כני"ל רק בודק קיום מעגל המילטוני.
- **MaxIS – בעיה ב- Σ_2^P** : בהינתן גרף G ומספר k , האם גודל הקבוצה הבלתי תלויה המקסימלית היא בגודל k .
- **Linear Programming – בעיה ב-P**: בהינתן אוסף אי-שוויונים, האם יש להם פתרון מעל הממשיים.
- **Integer Programming – בעיה ב-NPC**: כמו קודם, רק מעל השלמים.

- **Graph Isomorphism – בעיה ב-NP**: לא הצליחו להראות שבעיה זו ב-NP או ב-P. בהינתן שני גרפים H, G , האם הם איזומורפיים, כלומר האם הם אותו גרף תחת שינוי שמות הקודקודים. העד יהיה פרמוטציה של שמות הקודקודים, והמוודא יבדוק את תקינות הפרמוטציה ונכונותה. אם בעיה זו ב-NP, אז $NP = coNP$.
- **Compositness – בעיה ב-P**: בהינתן מספר N האם הוא פריק, כלומר לא ראשוני. גודל הקלט הוא $\log N$, וביחס לגודל זה מוודאים יעילות. ב-NP בגלל שעד יכול להיות k מחלק כלשהו, שגודלו הוא $\log N$, והמוודא בודק שהוא מחלק. ב-P בגלל:
- **Primality**: בהינתן מספר N , האם הוא ראשוני. ב- $coNP$, כי ניתן לתת מחלק k . עם הזמן גילו אלגי ב- BPP ולבסוף אלגי דטרמיניסטי ב- P .
- **Factoring – בעיה ב-NP וב-coNP**: בהינתן מספרים N, k , האם ל- N יש מחלק ראשוני בתחום $\{k, k + 1, \dots, N - 1\}$. ב- NP : ניתן לתת כעד מחלק ראשוני בתחום, ולבדוק בזמן פולי שהוא בתחום, מחלק וראשוני. ב- $coNP$: ניתן לקבל רשימת מספרים a_1, \dots, a_j ולוודא שמכפלתם היא N , שכל אחד מהם ראשוני ושכולם קטנים מ- k .

$$\text{טענה: } P \subseteq NP \subseteq EXP = \bigcup_{c \geq 1} DTIME(2^{n^c})$$

הוכחה:

- $P \subseteq NP$: בונים מוודא שמתעלם מהעד – המוודא יהיה האלגי המקורי שפותר בזמן פולי.
- $NP \subseteq EXP$: תהי $L \in NP$ וכל המשתמע מכך. נבנה אלגי M' שמפעיל את האלגי המוודא M על כל $2^{p(|x|)}$ העדים האפשריים. אם לפחות אחת מהריצות קיבלה, נקבל. אחרת נדחה.

הגדרה חלופית ל-NP:

- ההגדרה החלופית משתמשת באי-דטרי. נגיד ששפה $L \subseteq \{0,1\}^*$ שייכת ל- $NTIME(T(n))$ אם קיים $c > 0$ וקיים אלגי לא דטרי M כך שלכל x : קיימת בחירה אי דטרמיניסטית שגורמת ל- M לקבל $x \in L \Leftrightarrow M$ עוצר אחרי $c \cdot T(n)$ צעדים עבור כל בחירה אי דטרי.
- משפט:** $NP = \bigcup_{c \geq 1} NTIME(n^c)$
- הוכחה:** עבור $L \in NTIME(n^c)$, נבנה אלגי מוודא: מריץ את האלגי האי דטרי המקורי, אך במקום פיצולים אי דטרי, מתפצל לפי העד הניתן לו (אלגי זה דטרי). עבור $L \in NP$, נבנה אלגי לא דטרי: מריץ את האלגי המוודא תוך כדי שבונה עד באופן לא דטרמיניסטי באורך $p(|x|)$.

תרגול:

סגירות לפעולות:

$$L^* = \{y \mid \exists k \in \mathbb{N}. y = y_1 \dots y_k, \forall i \in \{1, \dots, k\}. y_i \in L\}$$

תרגיל: האם NP סגורה ל- $*$?

פתרון: כן. עבור $L \in NP$, נגדיר ל- x קלט ל- L^* עד באופן הבא: $0 < i_1 < i_2 < \dots < i_k = n$ חלוקה ל- x ו- w_1, \dots, w_k עדים לכל אחד ממחרוזות בחלוקה של x . האלגי המוודא ישתמש במוודא של L לבדוק שכל קטע בחלוקה הוא מחרוזת ב- L . העד באורך $O(n \cdot p(n))$ (אורך עד ב- L) וזמן הריצה גם כן. נכונות ברורה.

תרגיל: האם P סגורה ל- $*$?

פתרון: כן. עבור מילה $x = x_1 x_2 \dots x_n$ נבנה גרף בו הצמתים $0, 1, 2, \dots, n$ ולכל קטע בחלוקה מאינדקס i ל- j נעביר קשת מכוונת (i, j) . נבדוק אם בגרף יש מסלול מכוון מ- 0 ל- n . זמן ריצה $O(n^2 \cdot p(n))$ - הרצת האלגי המכריע את L על כל הקטעים האפשריים, בדיקת מסלול מכוון ע"י BFS . נכונות ברורה.

תרגיל: האם $coNP$ סגורה ל- $*$?

פתרון: בהינתן קלט x באורך n יש להוכיח כי ב- G_x אין מסלול מכוון מ- 0 ל- n . העד: אוסף זוגות הצמתים שאין ביניהם קשת ועדות לכך שאין ביניהם קשת ($\bar{L} \in NP$) ולכן קיימים עדים כאלה. נקח את הגרף השלם ונסיר ממנו את אותן קשתות, ונבדוק שאכן אין עליו מסלול מכוון מ- 0 ל- n .

רדוקציות ושלמות ב-NP:

רדוקציית Karp:

פולי משפה A לשפה B היא פולי f חשיבה בזמן פולי (בגודל הקלט) כך שלכל $x: x \in A \Leftrightarrow f(x) \in B$. נסמן $A \leq_p B$.

$$\bullet A \leq_p B \text{ וגם } B \leq_p C \text{ אז } A \leq_p C$$

$$\bullet \text{ אם } A \leq_p B \text{ או } B \in P \text{ או } B \in NP \text{ אז } A \in P \text{ או } A \in NP \text{ בהתאם.}$$

NP-hard: A תהיה NP -קשה אם לכל $L \in NP$: $L \leq_p A$.

NP-Complete: A תהיה NP אם היא NP -קשה וגם $A \in NP$.

משפט: $TMSAT \in NPC$

קיים $u \in \{0,1\}^n$ כך שהאלגוריתם M_α מוציא 1 על הקלט $\langle x, u \rangle$ תוך זמן t $TMSAT = \{ \langle \alpha, x, 1^x, 1^t \rangle \mid t \text{ תוך זמן } t \}$. הסיבה שמשתמשים בייצוג אונארי הוא כדי שהאלג' ירוץ בזמן פולי ל- n ולא $\log n$.

הוכחה בקיצור: $TMSAT \in NP$: בונים מוודא המקבל u כעד ומסמלץ את M_α על $\langle x, u \rangle$ למשך t צעדים. גודל הקלט זמן הריצה פולי $(n + t \geq)$. $TMSAT \in NP - hard$: תהי $L \in NP$ עם אלג' מוודא M_α הרץ בזמן $p(|x|)$ עם עד בגודל $q(|x|)$. $L \leq_p TMSAT$: הרדוקציה תתרגם קלט x ל- L : $\langle \alpha, x, 1^{q(|x|)}, 1^{p(|x|)} \rangle$.

משפט Cook-Levin: $SAT \in NPC$

טענה: לכל פונק בוליאנית מעל l משתנים $f: \{0,1\}^l \rightarrow \{0,1\}$ יש נוסחת CNF שקולה בגודל $l \cdot 2^l \geq$.

הוכחה: $SAT \in NP$: ברור. $\forall L \in NP. L \leq_p SAT$: תהא M מ"ט לא דטר' המחשבת את L ורצה בזמן $p(|x|)$, עם שתי פוני מעברים δ_0, δ_1 . נתרגם קלט x ל- L לנוסחה φ_x כך ש- $x \in L \Leftrightarrow \varphi_x \in SAT$. לכל קלט x נבנה נוסחה המתארת טבלה בגודל $p(|x|) \times q(|x|)$ המתארת את ריצת המכונה M על x – כל שורה בטבלה היא שלב. לייצוג כל תא נדרש למקום קבוע: $\log |\Sigma| + \log |Q| + 1$. φ_x תורכב מתנאים המוודאים שכל השורות מורכבות באופן תקין (השורה הראשונה עם q_0 מעל התא הראשון, השורה האחרונה מייצגת מצב קבלה, מעברי השורות – מצבים – נכונים ע"פ δ_0 או δ_1). סה"כ יתקבל מסי פולי של תנאים מעל מסי קבוע של משתנים – סה"כ נוסחת φ_x בגודל פולי והרדוקציה פולי. יש להוכיח אמ"מ.

טענה: $IS \in NPC$

הוכחה: $IS \in NP$: ברור. $IS \leq_p E3SAT$ $\exists E3SAT = \text{exactly 3 literals in each clause}$ $NP - hard$: לכל φ עם m הסגרים ניצור גרף עם m משולשים שקודקודי כל משולש הם הליטרלים בהסגר. בנוסף כל ליטרל יחובר לשלילתו. אם הנוסחה ספיקה אז יש בגרף קבוצה ב"ת בגודל m – לוקחים את אחד המשתנים המספקים בכל הסגר. אם יש קבוצה ב"ת בגודל m , חייב להיות בה קודקוד אחד בכל שלישייה ולכן ישנה השמה מספקת ע"י סיפוק הליטרלים כפי שמופיעים בקבוצה הב"ת.

טענות נוספות: $Clique, VC \in NPC$

תרגול:

רדוקציות Cook / Karp

תרגיל: להראות רדוקציית $Karp$: $HamPath \leq_p HamCycle$

פתרון: בהינתן G הרדוקציה תחזיר G' כך ש- $V(G') = V \cup \{u\}$ ו- $V(G) = V \cup \{u\}$ (מוסיפים קודקוד ומחברים אותו לכולם). נכונות: אם G - מסלול המילטוני $v_1 \rightarrow \dots \rightarrow v_n \rightarrow u$, ב- G' מעגל המילטוני $u \rightarrow v_1 \rightarrow \dots \rightarrow v_n \rightarrow u$. אם ב- G' מעגל המילטוני, מסירים את u ומקבלים מסלול המילטוני.

טענה: NP סגורה לרדוקציות $Karp$.

תרגיל: להראות רדוקציית $Cook$: $HamCycle \leq_{cook} HamPath$

פתרון: בהינתן G' קלט לבעיית מעגל המילטון, נבדוק האם $E' = \emptyset$. אם כן, נחזיר שאין מעגל המילטון. אם לא, נבחר קשת כלשהי (u, v) ונרץ את $HamPath(V \cup \{w, z\}, E \cup \{(z, v), (u, w)\})$. אם מחזיר כן, נחזיר כן – כי יחד עם הקשת (u, v) ניתן להשלים מעגל המילטון. אחרת, נסיר את הקשת הזו ונחזור לשלב ההתחלה.

טענה: NP סגורה לרדוקציית $Cook$ פולי אמ"מ $NP = coNP$.

הוכחה: אם NP סגורה לרדוקציית $Cook$ פולי, והרי לכל $L \in NP$ $\bar{L} \leq_{cook} L$ ע"י החזרת התשובה ההפוכה לתשובת האלג' המכריע את L , נקבל כי $\bar{L} \in NP$ ולכן $NP \subseteq coNP$ וגם $coNP \subseteq NP$ ולכן $NP = coNP$. אם $NP = coNP$, תהיה $L \in NP = coNP$ ו- $L' \leq_{cook} L$ נראה $L' \in NP$. יהי A אלג' המכריע את L' . בהינתן קלט x לשפה L' , יהי k מספר הקריאות של A לאלג' המכריע את L . העד שנצפה לו הוא התשובות $a_1, \dots, a_k \in \{0,1\}$ של האלג' המכריע את L , וכן עדים לנכונות תשובות L : w_1, \dots, w_k . כיוון ש- $L \in NP = coNP$, ניתן לוודא האם קלט שייך או לא שייך ל- L באמצעות עד. האלג' של L' יסמלץ את A ובכל קריאה לאלג' הפותר את L יודא בעזרת w_i אם a_i התשובה הנכונה. אם לאורך כל החישוב העדים ענו על הדרישה ו- A קיבל, אז נקבל. אחרת נדחה.

חיפוש לעומת החלטה:

משפט: אם $P = NP$ אז לכל $L \in NP$ יש אלגי פולימי שבהינתן $x \in L$ מוציא עבורו עד.

הוכחה על SAT: נסמן את האלגי הפולימי הפותר את SAT ב- A . בהינתן φ נבדוק האם ספיקה. אם לא – נעצור. אם כן, נקבע את x_1 ל- t ע"י הוספת (x_1) לנוסחה ונבדוק האם ספיקה. אם כן, נמשיך עם $x_1 = t$, אחרת נמשיך עם $x_1 = f$ (נוסיף את (\bar{x}_1) במקום (x_1)). לבסוף מתקבלת השמה מספקת. נדרשת הוכחת נכונות.

הוכחה כללית: תהא $L \in NP$ עם אלגי מוודא M . נתרגם את M למי"ט דטר' M' המחשבת את L . לפי $C-L$ בהינתן x ניתן לבנות φ_x כך ש- $x \in L \Leftrightarrow \varphi_x \in SAT$, ולפי הוכחת $C-L$, בהינתן השמה מספקת ל- φ_x ניתן בזמן פולימי לשחזר את הבחירות הלא דטר' ומהן לבנות את העד שגורם ל- M לקבל.

המחלקה coNP:

$coNP = \{L \mid \bar{L} \in NP\}$. הגדרה חלופית: קיים פולינום p ומי"ט פולימי M כך שלכל $x \in \{0,1\}^*$ $M(x, v) = 1 : \exists v \in \{0,1\}^{p(|x|)}$. או באופן שקול: $x \in L \Leftrightarrow \forall v \in \{0,1\}^{p(|x|)}. M(x, v) = 1$. NP ידועה גם כ- NP , ו- $coNP$ ידועה גם כ- $coNP$.

דוגמא: $CNF - EQUIV = \{ \langle \varphi, \psi \rangle \mid \forall x \in \{0,1\}^*. \varphi(x) = \psi(x) \}$.

טענה: $SAT \in coNPC$ (תחת רדוקצית Karp)

טענה: $CNF - EQUIV \in coNPC$

$CNF - EQUIV \leq_p SAT$: $\langle \varphi, (x) \wedge (\bar{x}) \rangle \rightarrow \varphi$ - הנוסחה השניה תמיד לא ספיקה. נכונות ברורה.

המחלקות EXP, NEXP:

$EXP = \bigcup_{c \geq 1} DTIME(2^{n^c})$, $NEXP = \bigcup_{c \geq 1} NTIME(2^{n^c})$ (ניתן להגדיר גם באמצעות עד).

ברור שמתקיים: $P \subseteq NP \subseteq EXP \subseteq NEXP$.

משפט: אם $EXP \neq NEXP$ אז $P \neq NP$.

הוכחה: נניח $P = NP$. ברור כי $EXP \subseteq NEXP$, נראה $NEXP \subseteq EXP$. תהי $L \in NEXP$, נגדיר בשיטת ה-**Padding**:

$L_{pad} \in NP$. $L_{pad} = \{ \langle x, 1^{2^{|x|^c}} \rangle \mid x \in L \}$. בהינתן קלט נבדוק שהוא מהצורה הנדרשת, ואם כן נפעיל עליו את האלגי הלא-דטר' הרץ בזמן

$O(2^{|x|^c})$. זמן הריצה הוא פולימי בגודל הקלט ב- L_{pad} . אם כן, לפי הנחה, $L_{pad} \in P$, ומכאן קל לבנות אלגי אקספי דטר' המכריע את L .

המחלקות Σ_2^P, Π_2^P :

Σ_2^P : מחלקת השפות שיש עבורן מי"ט פולימי M ופולינום p כך שלכל $x \in \{0,1\}^*$ $M(x, u, v) = 1 : \exists u \in \{0,1\}^{p(|x|)}. \forall v \in \{0,1\}^{p(|x|)}$. או $x \in L \Leftrightarrow \exists u \in \{0,1\}^{p(|x|)}. \forall v \in \{0,1\}^{p(|x|)}. M(x, u, v) = 1$.

דוגמא: $MIN - DNF$ - בהינתן נוסחת DNF ומספר k , האם קיימת נוסחת DNF בגודל לכל היותר k כך ש- $\varphi = \psi$: $\exists \psi. \forall x. \varphi(x) = \psi(x)$. (בעיה Σ_2^P -שלמה).

Π_2^P : מוגדרת בצורה דומה עם החלפת ה- \forall עם ה- \exists . מתקיים: $L \in \Sigma_2^P \Leftrightarrow \bar{L} \in \Pi_2^P$.

דוגמא: $MAX - IS = \{ \langle G, k \rangle \mid G's \text{max. ind. set is exactly of size } k \}$. ניתן להביע את התנאי בשתי הצורות הני"ל, שייך ל- $\Sigma_2^P \cap \Pi_2^P$. הקרויה גם DP . בעיה זו היא DP -שלמה.

ניתן להמשיך ולהוסיף תנאי \forall, \exists ולהגדיר Σ_3^P, Π_3^P וכן הלאה, והיררכיה זו קרויה ההיררכיה הפולינומיאלית - PH .

משפט: $P = NP \Leftrightarrow \Sigma_2^P = P$

הוכחה: כיוון אחד ברור. אם נניח $P = NP$, ותהי $L \in \Sigma_2^P$, אז $L \in \Sigma_2^P$ או $L \in \Sigma_2^P$. נגדיר

$L' = \{ \langle x, u \rangle \mid u \in \{0,1\}^{p(|x|)}, \forall v \in \{0,1\}^{p(|x|)}. M(x, u, v) = 1 \}$. מהגדרה $L' \in coNP = P$, ונניח M' הוא האלגי המוודא של L' . מכאן:

$x \in L \Leftrightarrow \exists u \in \{0,1\}^{p(|x|)}. M'(x, u) = 1$. באופן דומה זו שפה ב- NP ולפי הנחה ב- P .

משפט היררכיית הזמן:

לכל פונקציות f, g כך ש- $g(n) = \omega(f(n) \cdot \log f(n))$ מתקיים: $DTIME(f(n)) \not\subseteq DTIME(g(n))$.

הוכחה: נגדיר בעיית החלטה: בהינתן אלגי α האם הפעלת U (המי"ט האוניברסלית) לסמלץ את M_α על α למשך $g(|\alpha|)$ צעדים עוצרת? מהגדרה, הבעיה ב- $DTIME(g(n))$, נראה שאינה ב- $DTIME(f(n))$. חסר.

תרגול:**3-צביעה:**

- בעיית הכרעה: בהינתן גרף G , האם ניתן לצבוע את צמתיו בשלושה צבעים $\{1,2,3\}$ כך שכל שני צמתים סמוכים צבועים שונה?
- בעיית חיפוש: בהינתן גרף G , מצא צביעה לקודקודיו בשלושה צבעים $\{1,2,3\}$ כך שכל שני צמתים סמוכים צבועים שונה.

תרגיל: למצוא רדוקצייה עצמית (Cook) מבעיית החיפוש לבעיית ההכרעה (כלומר: בהינתן אלג' מכריע ל-3-col, למצוא אלג' המוצא צביעה).
פתרון: בהינתן G תחילה נבדוק האם $G \in 3-col$, אם לא אז נדחה. אם כן, נוסיף לו שלושה צמתים חדשים $\{x, y, z\}$ שנחברם במשולש ונסמן גרף זה G' . לכל $v \in V$ נפעיל את אלג' ההכרעה על שלושה גרפים עם צמתי G' וקשתות G' , כאשר לראשון נוסיף הקשתות $\{v, x\}, \{v, y\}$, לשני $\{v, x\}, \{v, z\}$ ולשלישי $\{v, y\}, \{v, z\}$. מתוך הגרפים האלה נבחר גרף כלשהו G_i ($1 \leq i \leq 3$) שהוא 3-צביע ונסמנו G' . הצבע של הצומת v יהיה i כאשר G_i הוא הגרף שנבחר מהאיטרציה על v . נכוונת: G' 3-צביע ולכן ל- v צביעה בצבע מבין 1,2,3, ולכן הוספת 2 קשתות לצמתים מבין x, y, z שאינם צבועים בצבע זהה, תשאיר את הגרף 3-צביע לפי אותה צביעה.

תרגיל: אם קיימת שפה אונארית NP-שלמה אז $P = NP$.

הוכחה: תהא $L \in \{1\}^* NPC$, ולכן $L \leq_p SAT$. תהא f הרדוקצייה שלכל φ מחזירה $f(\varphi) = 1^i$ כאשר $i \leq p(n)$ כאשר p פולינום ו- n מספר משתני הנוסחה / אורך φ . נראה אלג' ל- SAT הרץ בזמן פולי' ומכך נסיק $P = NP$. נשתמש במערך A שכל ערכיו מאותחלים ל- $unknown$. נגדיר את $SAT(\varphi(x_1, \dots, x_n), A)$:

• אם $n = 0$ החזר את φ (או t).

• אם $A[|f(\varphi)|] \neq unknown$, החזר את $A[|f(\varphi)|]$.

• אם $SAT(\varphi(t, x_2, \dots, x_n), A)$ או $SAT(\varphi(f, x_2, \dots, x_n), A)$ נשים t ב- $A[|f(\varphi)|]$ ונחזיר t , אחרת נשים f ונחזיר f .

הרעיון: עבור קלט בגודל n יתכנו 2^n קלטים אפשריים, אך f ממפה אותם לקבוצה קטנה יחסית – בגודל $p(n)$ (כי לכל i היחיד באורך i הוא 1^i ואין עוד קלטים אחרים אפשריים באורך i). לכן שמירת הערכים ב- A תחסוך בדיקות בהמשך = תחסוך התפלצויות בעץ האלג' הנאיבי.
 נכוונת: נובעת מכך ש- $\varphi(x_1, \dots, x_n)$ ספיקה אמ"מ $\varphi(t/f, x_2, \dots, x_n)$ ספיקה. זמן ריצה: בכל שלב נבחר צומת שמתאים לקריאה רקורסיבית בעץ הרקורסיה (לא עלה) ונסיר אותו ואת המסלול המוביל אליו מהשורש: $O(n)$ צמתים. נעשה זאת עד שהעץ יתרוקן. כל קריאה רקורסיבית כזו הנמצאת בתחתית המסלול מתאימה לערך שונה מהמערך A , ולכן לכל היותר יוסרו $p(n)$ מסלולים. סה"כ: $O(n \cdot p(n))$. בכל קריאה כזו מפעילים את f ולכן סה"כ $O(p^2(n) \cdot n)$.

אורקלים ומגבלת הלכסון:

אורקל:

תהא $O \subseteq \{0,1\}^*$ שפה כלשהי. אלג' עם גישה לאורקל O הוא אלג' שיש לו פקודה המאפשרת לו לפתור את O בצעד אחד של קריאה לאורקל. אלג' זה יסומן M^O . בצורה דומה נגדיר אלג' לא דטר' עם גישה לאורקל ומכאן את המחלקות P^O, NP^O .

טענה: $\overline{SAT} \in P^{SAT}$. הוכחה: הפעלת האורקל על קלט φ והחזרת התשובה ההפוכה.

טענה: עבור $O \in P$ מתקיים $P^O = P$. הוכחה: $P^O \subseteq P$ - ברור. $P \subseteq P^O$ - ניתן לסמלץ את האורקל ע"י מכונה ב- P ולהישאר בזמן פולי'.

טענה: $NP^{EXPCOM} = P^{EXPCOM} = EXP$; $EXPCOM = \{ \langle \alpha, x, 1^n \rangle \mid M_\alpha(x) = 1, \text{ runs in } 2^n \text{ steps} \}$

הוכחה:

(1) $EXP \subseteq P^{EXPCOM}$: תהי $L \in EXP$ עם מכונה M_α הפותרת את L בזמן 2^{nc} עבור c כלשהו. נבנה אלג' המשתמש ב- $EXPCOM$ הרץ בזמן פולי'

באורך הקלט: על קלט x מחזיר את תשובת האורקל ל- $\langle \alpha, x, 1^{nc} \rangle$.

(2) $P^{EXPCOM} \subseteq NP^{EXPCOM}$: ברור.

(3) $NP^{EXPCOM} \subseteq EXP$: בזמן אקספ' ניתן לעבור על כל האפשרויות הלא-דטר' גם עם האורקל.

משפט Baker-Gill-Solovay: קיים אורקל A כך ש- $P^A \neq NP^A$

הוכחה: לכל שפה A נגדיר $U_A = \{1^n \mid \exists x \in A. |x| = n\}$. לכל A מתקיים $U_A \in NP^A$ כי העד יכול להגיד לנו איפה נמצא את המחרוזת $x \in A$.

נותר לבנות A כך ש- $U_A \in P^A$.

תרגיל:

טענה: $EXP^{EXP} \neq EXP$

הוכחה: נראה ש- $DTIME(2^{2^n}) \subseteq EXP^{EXP}$ ואז לפי משפט היררכית הזמן: $EXP \not\subseteq EXP^{EXP}$. תהא $L \in DTIME(2^{2^n})$ אז קיימת מ"מ M

הרצה בזמן $2^{2^n} \cdot c$ ומכריעה את L . נראה כי $L \in EXP^{EXPCOM} \subseteq EXP^{EXP}$: בהינתן קלט x ניצור את הקלט לאורקל $\langle M, x, 1^{2^n+c'} \rangle$ ונחזיר

את תשובת האורקל. נשים לב כי $\langle M, x, 1^{2^n+c'} \rangle \in EXPCOM \Leftrightarrow x \in L \forall x$. זמן הריצה של M חסום ע"י 2^{2^n} ולכן $EXP \not\subseteq EXP^{EXP}$

סיבוכיות מקום:

פרק שני : סיבוכיות מקום :

תהי $t: \mathbb{N} \rightarrow \mathbb{N}$ פונקציה סיבוכיות מקום (מונוטונית לא יורדת).

$SPACE(t(n))$: מחלקת השפות שניתנות להכרעה במקום $O(t(n))$ ע"י מ"ט דטרמיניסטית.

$NSPACE(t(n))$: מחלקת השפות שניתנות להכרעה במקום $O(t(n))$ ע"י מ"ט לא דטרמיניסטית.

המחלקות NL, L :

$L = SPACE(\log(n)), NL = NSPACE(\log(n))$. נגדיר מ"ט בעלת שלושה סרטים באופן הבא:

1. סרט קלט: קריאה בלבד.

2. סרט עבודה: קריאה וכתובה. גודל סרט זה קובע את סיבוכיות המקום.

3. סרט פלט: לכתובה בלבד.

קונפיגורציות:

מספר הקונפיגורציות עבור קלט בגודל N וסרט עבודה בגודל S : $|\Sigma|^N \times \begin{matrix} N \\ \text{מיקום הראש} \\ \text{בסרט הקלט} \end{matrix} \times \begin{matrix} |\Gamma|^S \\ \text{תוכן סרט העבודה} \end{matrix} \times \begin{matrix} S \\ \text{מיקום הראש} \\ \text{בסרט העבודה} \end{matrix} \times \begin{matrix} |Q| \\ \text{המכונה מצב} \end{matrix}$

דוגמאות לשפות ב- L : $a^n b^n, a^n b^n a^n, a^n b^{2n} a^n, \text{palindrome}, a^n b^{2n} a^{4n} b^{8n} \dots$

שאלה פתוחה: האם קיימת שפה ב- $NL \setminus L$; האם $NL \not\subseteq P$.

רדוקציה \log -space Karp:

$A \leq_L B$ אם קיימת פונ' $f: \Sigma^* \rightarrow \Sigma^*$ הרצה במקום לוגריתמי כך שלכל $w: w \in A \Leftrightarrow f(w) \in B$.

משפט:

המחלקות $EXP, PSPACE, NP, P, NL, L$ סגורות תחת רדוקציה מקום לוגריתמי.

רדוקציה לוגריתמית במקום מ- A אל B : מסמלצים ריצה של f (סרט ה- out לא חסום במקום, לכן ניתן לסמלץ צעד צעד, ולשמור על שימוש במקום לוגריתמי).

בעיית $CONN$:

בהינתן גרף G וקודקודים s, t , האם קיים מסלול מ- s ל- t . $CONN \in NL$.

להלן אלג' במקום לוגריתמי לא דטר': יהי $u = s$ קודקוד התחלתי נבצע $|V|$ איטרציות: בכל שלב u בוחר שכן כלשהו וממשיך אליו. אם $u = t$, נקבל, אחרת נמשיך. אם לא הגענו ל- t , נדחה. את u ואת i (מספר הצעדים שביצענו עד כה, עד שנגיע ל- $|V|$) מחזיקים ב- $\log |V|$ מקום.

$NL-TM$:

1. סרט קלט: קריאה בלבד.

2. סרט עבודה: קריאה וכתובה.

3. סרט עדות: לקריאה בלבד, רק משמאל לימין, ללא אפשרות לחזור אחורה.

$CONN \in NL - Complete$

בהינתן מכונה M וקלט x ניצור את t, s, G : נגדיר קונפיגורציה מקבלת: נמחק את סרט העבודה, ונגדיר קוני' זו כמקבלת. $G_{M,x}$ יהיה גרף הקונפיגורציות, שכל קודקוד בו יתאים לקונפיגורציה של M על הקלט x . מסי' הקוני' הוא פולי' באורך x . קשת (u, v) תהיה ב- G אם יש מעבר $u \rightarrow v$ לפי δ (פוני' מעברים לא דטר') ב- M , כלומר מעבר קונפיגורציות חוקי. s יהיה הקוני' ההתחלתי ו- t תהיה הקוני' היחידה (כפי שהוגדרה לעיל) המקבלת.

$G_{M,x}$ ניתן ליצירה במקום לוגריתמי: נחזיק את הגרף במטי' שכנויות התופסת מקום לינארי, אך נעבוד על קשת אחת בכל זמן נתון לפני הדפסתה לסרט הפלט – ולכן נזדקק לסרט עבודה לוגריתמי בלבד.

נותר להוכיח כי $\forall M, x: M \text{ accepts } x \Leftrightarrow \exists s \rightarrow t \text{ in } G_{M,x}$.

משפט Savitch:

$\forall S(n) \geq \log(n): NSPACE(S(n)) \subseteq SPACE(S^2(n))$: כל מכונה המשתמשת במקום $S(n)$ לא דטר', ניתן לסמלץ ע"י מכונה דטר' עם

$S^2(n)$ מקום. להלן אלג' דטר' ל- $CONN$ המשתמש ב- $\log^2(n)$ מקום:

נראה אלג' הבודק האם בגרף מכונן G קיים מסלול מ- u אל v באורך לכל היותר d , ואז נבדוק על $|V|$: אם $(u, v) \in E$, נקבל. אחרת, אם

$d = 1$, נדחה. אחרת, נבדוק האם לכל $w \in V$ מתקיים האלג' על $\left\lfloor \frac{d}{2} \right\rfloor$ ועל $u, w, \left\lfloor \frac{d}{2} \right\rfloor$. אם כן, נקבל. אחרת נדחה. עומק הרקורסיה באלג' הוא

$\log |V|$. בכל רמה של הרקורסיה צריך לשמור w – דורש מקום לוגריתמי בלבד. סה"כ: $\log^2 |V|$ מקום.

תרגול: **$2SAT \in coNL - Complete$** **$\overline{2SAT} \in NL$**

בהינתן $\varphi \in 2CNF$ בעלת n משתנים, נבנה גרף עם $2n$ משתנים (לכל משתנה ושלילתו). נייצג את האילוצים בגרף ע"י קשתות מתאימות באופן הבא: כדי שהסגר כלשהו יסופק צריך להתקיים שאם שלילת הראשון מקבל t , אז הליטרל השני צריך לקבל t . כמו כן אם שלילת הליטרל השני מקבלת t , הליטרל הראשון צריך לקבל t (כדי שיהיה לפחות ליטרל אחד מתוך ה-2 בהסגר שמקבל t). לכל הסגר $(x_1 \vee x_2)$ נסמן את t בגרף את הקשתות (\bar{x}_1, x_2) ו- (x_2, \bar{x}_1) .

טענה: ל- φ אין השמה מספקת \Leftrightarrow קיים משתנה x_i שיש מסלול ממנו ל- \bar{x}_i (ומסלול הפוך גם כן). אם הטענה נכונה, קל להראות ש- $\overline{2SAT} \in NL$: ננחש באופן אי דטר' את x_i , וננחש באופן לא דטר', כמו באלג' המכריע את $CONN$, מסלול מ- x_i אל \bar{x}_i ולהיפך. אלג' זה עובד עם מקום $\log(n)$ לא דטר'.

הוכחת הטענה:

אם קיים i כך שיש מסלול מ- x_i אל \bar{x}_i ולהיפך, אז לפי הגדרת הגרף כל צומת שניתן להגיע אליו מ- x_i , אם $x_i = t$ אז גם אותו צומת מקבל t . לפיכך נקבל כי גם $\bar{x}_i = t$, וכמו כן אם $\bar{x}_i = t$ אז $x_i = t$, וזו סתירה. לפיכך ל- φ אין השמה מספקת.

נניח כעת כי לכל i לא קיים מסלול מ- x_i אל \bar{x}_i . כאמור, אם $x_i = t$, כל x_j שיש מסלול מ- x_i אליו מקבל t . נראה שלא יתכן שנקבל סתירה. נניח כי במתן ערכי אמת ל- x_i, x_k , קיבלנו סתירה לערכו של x_j . מכאן שקיימים מסלולים מ- x_i ל- x_j ומ- x_k ל- \bar{x}_j . לפיכך, יש גם מסלול מ- x_j ל- \bar{x}_k , ולכן מסלול מ- x_i אל \bar{x}_k . לכן, כאשר קבענו את ערכו של x_i להיות t , קבענו בכך את ערכו של x_k להיות f , ומכאן שלא היתה סתירה בקביעת x_j .

 $CONN \leq_L \overline{2SAT}$

בהינתן G, s, t נגדיר את φ באופן הבא: $\varphi = (sVs) \wedge (\bar{t}\bar{V}\bar{t}) \wedge_{(u,v) \in E} (\bar{u}Vv)$. אם קיים מסלול בין s ל- t , אז כדי ש- φ תסופק, s חייב להיות t ו- t חייב להיות f וכל צומת שיש מסלול מ- s אליו חייב להיות t . לכן, לא יתכן שיש השמה מספקת ל- φ . אם אין ב- G מסלול מ- s ל- t , ניתן ערך t ל- s ולכל המשתנים שיש מסלול מ- s אליהם. נשים לב שאין קשת מצומת u שיש מסלול מ- s אליו לצומת v שאין מסלול מ- s אליו (אחרת היה מסלול $s \rightarrow u \rightarrow v$). לכן, כל ההסגרים מהצורה $(\bar{u}Vv)$, אם $\bar{u} = f$ או $u = t$, ומכיוון שיש מסלול מ- s אל v אז גם $v = t$. לכן כל ההסגרים יסתפקו. **הרדוקציה במקום לוגריתמי:**