מודלים חישוביים ־ הרצאה 11

שרון מלטר, אתגר 17

28 במאי 2024

1 תזכורת

בשיעור שעבר הוכחנו את משפט קוק לוין וראינו שתי רדוקציות חדשות.

2 $K-COLOR$

נתון לנו גרף G שניתן לצביעה תקינה ב־ k, צבעים.
צביעה היא פונקציה שנותנת לכל קודקוד צבע ואם כל צומת הוא לא שכן של צומת מאותו הצבע, אז היא תקינה. כלומר־ $C : V \to 1, ..., k$. ו־ C צביעה תקינה אם לכל קשת (u, v) מתקיים $C(u) \neq C(v)$

למה הבעיה חשובה?
נניח שיש לנו קורסים, שמסומנים בצמתים, כך שאם סטודנט כלשהו לוקח שני קורסים באותו הסמסטר, יש ביניהם קשת. נרצה לבדוק האם ניתן להשתמש ב־ k תאריכים שונים למבחן הסופי של כל קורס, כך שאין סטודנט שיש לו שני מבחנים באותו יום. בעיה זו שקולה ל־ $K - COLOR$.

בעיה זו שייכת ל־ NP, מכיוון שניתן לבדוק נכונות פיתרון (פונקציית צביעה) בזמן פולינומי.

קיים אלגוריתם פתרון ל־ $2 - COLOR$, למשל, בעזרת BFS שבו צובעים את שכני כל צומת בצבע אחר ממנו.
אם לא ניתן לעשות זאת, מפסיקים ועונים שפתרון בלתי אפשרי עם שני צבעים בלבד.
אך לא ניתן לפעול באותה השיטה עם $3 - COLOR$, מכיוון שניתכן שנתחרט בזמן הריצה על צביעה קודמת ונרצה לשנות אותה. ב־ $2 - COLOR$ אין כלל אלמנט של בחירה־ לכל שכן של צומת עם צבע יש רק אפשרות אחת לצביעה שלו.
בהמשך נראה מהו הדמיון או השני בין "האם קיים פתרון" למציאת פתרון.

נשתמש ברדוקציה באמצעות גדג'ט, שזוהי צורת מחשבה.
נסתכל בגרף שנכנה אותו $Gadget$, שבו משולש ולכל צומת במשולש מחוברת בקשת שרשרת צמתים. בכל שרשרת שני צמתים. כל צומת בקצה שרשרת נכנה קודקוד קצה והקודקוד שבינו לקודקוד המשולש יכונה קודקוד ביניים.
נתעניין בצביעות של $Gadget$ ב־3 צבעים, שנכנה אותם $\{T, F, A\}$. נכנה צביעה C לגרף $Gadget$ רלוונטית קודקודי קצה צבועים ב־ $\{T, F\}$ וקודקודי הביניים צבועים ב־ $\{F, A\}$. ־ למה? רונן לא מספר עדיין :(

טענה: אין צביעה תקינה ורלוונטית של $Gadget$ שבה שלושת קודקודי הקצה ב־ F
הגרף סופי, לכן קל להוכיח זאת.

טענה 2: בהינתן צביעה רק של קודקודי הקצה ב־ $\{F, T\}$, כך שלפחות אחד מהם צבוע ב־ T, ניתן להשלים את הצביעה לצביעה תקינה ורלוונטית.
שוב, עדיין מדובר על מספר מצבים סופי־ קל להוכיח.
למה זה מעניין אותנו? ־ מכיוון שאז מי שיימצא צביעה חלקית כזו, יידע שהוא יוכל להסתדר.

נבנה רדוקציה $R(\Phi)_{3-CNF} =< G >_{3-COLOR}$,
כך שנוכיח בעזרת $3 - SAT$ ש־ $3 - COLOR$ באותה מחלקה.

בניית R: בהינתן נוסחה Φ נסמן ב־ n את מספר המשתנים וב־ m את מספר הפסוקיות. ראינו ש־ $|\Phi|$ פולינומי ב־ m.
נבנה את הגרף בשלבים: נתחיל מרכיב המשולש, שבו הקודקודים מכונים a, f, t. לאחר מכן לכל משתנה x_i נוסיף

קשת בין צומת המייצג אותו לצומת המייצג את שלילתו, ונחבר את שני הצמתים לצומת A ברכיב המשולש.
לבסוף, לכל פסוקית $l_1 \vee l_2 \vee l_3$ כאשר l_1, l_2, l_3 ליטרלים נשים לב שקודקודים מייצגים l_1, l_2, l_3 כבר נמצאים ברכיב ההשמה. לכן לכל פסוקית כזו אנחנו ניצור עותק של $Gadget$ שמשתמש באותם צמתים כקודקודי קצה.
בסך הכל מדובר בבניית מספר קבוע של רכיבים לכל משתנה ופסוקית, לכן R פולינומי.

כיוון ראשון של השוויון: נניח ש־ Φ ספיקה, כלומר ישנה השמה α שמספקת אותה α (מספקת כל אחת מפסוקיות Φ)
נגדיר צביעה של G עם 3 צבעים;
נצבע את רכיב המשולש כך־ $C(t) = T, C(a) = A, C(f) = F$. כמו כן לכל הליטרלים נבחר $C(l) = \alpha(l)$ ונבחר גם $C(x_i) = \alpha(x_i), C(\hat{x_i}) = \hat{\alpha}(x_i)$. לכל משולש שהוסף עבור פסוקית, נצבע את קודקודי הביניים שלו ב־ T או F (לא מאוד משנה לנו. גם ברור שניתן להתאים לשכנים) לפי הטענה, קיימת השלמת צביעה תקינה ורלוונטית.
ניתן לראות שלכל השכנים בגרף לא יתקיים שאחד בצבע של השני (!). נעבור על הרכיבים ונראה זאת־

- כמובן שההשמה של x_i שונה מההשמה $\hat{x_i}$
- קודקודי רכיב המשולש צבועים ב־3 צבעים שונים.
- צלעות מקודקודים והשמה ל־ a תקינות, מכיוון שכל קודקודי רכיב ההשמה צבועים ב־ T/F ולא ב־ A (הצבע של a).
- צלעות בין קודקודי הביניים של $Gadget$ ל־ t תקינות, מכיוון שהצביעה של כל עותק של $Gadget$ היא רלוונטית.
- צלעות בתוך $Gadget$ תקינות מכיוון שהצביעה של כל עותק תקינה.

בסך הכל צביעה זו תקינה ורלוונטית.

כיוון שני: נניח שקיימת צביעה תקינה ל־ G ונוכיח ש־ Φ ספיקה.
כיוון ש־ C תקינה, את קודקודי רכיב המשולש צובעים בשלושה צבעים שונים. בה"כ ניתן להניח ש־ $C(t) = T, C(f) = F, C(a) = A$ (ניתן לשנות את שמות הצבעים בהתאם, אין השפעה בכך על תקינות הצביעה) כל קודקוד ביניים ב־ $Gadget$ צבועים ב־ $\{A, F\}$ מכיוון שהם מחוברים ל־ t.
נגדיר השמה α למשתני Φ :

$$\alpha(x_i) = C(x_i) \in \{T, F\}$$

נשים לב ש־ $\alpha(\hat{x_i}) = \hat{\alpha}(x_i)$ מכיוון שהם שכנים. כמו כן לכל ליטרל l מתקיים $\alpha(l) = C(\alpha)$.

ידוע לנו ש־ C צביעה תקינה.
טענה: לכל פונקציה על $Gadget$, הצביעה היא תקינה ורלוונטית.

הוכחה:
ברור שהצביעה תקינה. נוכיח שהיא רלוונטית.
קודקודי קצה צבועים T/F וקודקודי קצה ב־ A/F כנדרש.

מכאן נובע שלכל פונקציה על $Gadget$, לפחות אחד מהקודקודים החיצוניים צבוע ב־ T. במילים אחרות: לכל פסוקית קיים ליטרל ש־ α מספקת אותו, מכיוון ש־ $\alpha(l) = C(l)$.
כלומר, קיבלנו שההשמה α מספקת את כל הפסוקיות־ כך ש־ α מספקת את Φ והיא ספיקה.

3 קיים פתרון VS מציאת פתרון

בחיים האמיתיים (למי שיש) פחות מעניינות אותנו גירסאות ההכרעה של שאלה (האם קיים פתרון...) אלא גירסת החיפוש, כלומר גירסא שדורשת פתרון לבעיה.
עד כה, התעניינו רק בבעיות הכרעה (שפות). בכל פעם שתלמיד שאל על משהו שאיננו שפה, רונן טען שזה לא משנה. כעת נראה שאכן אין הבדל גדול מדי.

נניח ש־ $P = NP$, כלומר ישנה מ"ט פולינומית שפותרת (בגירסת ההכרעה) את $3-SAT$. האם יש מ"ט פולינומית שפותרת את גירסת החיפוש?

משפט: אם $P=NP$, לכל בעיה ב־ NP קיימת מ"ט שפותרת את גירסת החיפוש שלה.

נוכיח את נכונות המשפט עבור $3-SAT$. האם זה מסייע להוכחת המשפט שמעלינו? ־ סוג של. נראה בהמשך.

נניח ש־ $P=NP$, כך שישנה מ"ט פולינומית D שפותרת את גירסת ההכרעה של $3-SAT$. נוכיח שקיימת מ"ט פולינומית S שפותרת את גירסת החיפוש.
בניית S: קלט נוסחה Φ על n משתנים ב־ $3-CNF$. נריץ $D(P)$, אם התשובה היא "לא", אז אין פתרון וסיימנו. אחרת, נגדיר נוסחאות חדשות Φ_0, Φ_1 כאשר Φ_b מתקבלת ע"י הצבת $x_n=b$ ב־ Φ. l_1, l_2 הן נוסחאות $3-CNF$ מאורך שאינו עולה על אורך Φ והן על $n-1$ משתנים.
בהכרח לפחות אחת מ־ Φ_0, Φ_1 ספיקה. נריץ את $D(\Phi_0), D(\Phi_1)$. לפחות על אחת מהן, בה"כ Φ_0, D יענה 1.
נשים לב שאלגוריתם זה אכן פולינומי, מכיוון שאנו לא בודקים כל אפשרות, אלא רק ממשיכים בכל פעם עם האפשרות שעובדת עד כה.

האם המשפט נכון?
כן. באותה גישה ניתן לבנות מ"ט שפותר כל גירסת חיפוש.

4 נושא אחרון ־ מבוא למורכבות חישובית

מבוא לסיבוכיות:
$$P=\cup_{c=1}^{\infty} DTime \in (n^c)$$
היא שפה המוכלת ב־
$$NP=\cup_{c=1}^{\infty} NTime \in (n^c)$$
וזוהי שפה המוכלת ב־
$$EXP=\cup_{c=1}^{\infty} DTime \in (2^{n^c})$$

4.1 שאלות

האם $P \neq NP$?
לא ידוע, אבל חושבים שכן.

האם $NP \neq EXP$?
גם לא ידוע וחושבים שכן.

האם $P \neq EXP$?
כן. צריכים רק להציג בעיה שיש לה רק פתרון אקספוננציאלי.

מסקנה: או $P \neq NP$ או $NP \neq EXP$.
רוצים כלי כדי להראות ששפה L היא לא ב־ P.

משפט ההיררכיה לזמן: ישנה שפה L (מקרה פרטי) כך ש־ $L \in DTime(n^c)$, $L \notin DTime(n^c)$.
נוכיח את המשפט, אך כפי שהוא מנוסח במסקנה מהשאלות.

איך נוכיח? ־
נבנה מ"ט N, כך ש־ $L=L(N)$.
בהינתן קלט, נחשוב עליו כקידוד של מ"ט $<M>$. נסמן $n=|<M>|$.
נמסלץ את הרצת M על $<M>$ למשך n^2 צעדים.

- M עצרה וענתה "כן", ענה "לא".
- M עצרה וענתה "לא", ענה "כן".
- M לא עצרה לאחר n^3 צעדים. נענה משהו, בה"כ "כן".

כלומר, המכונה עונה את ההיפך ממה שהיא תענה על עצמה.
כמובן ש־ N עצרה בזמן $O(n^3)$

צ.ל ש־ $L \notin DTime(n^2)$
תהי M מ"ט שרצה בזמן n^2, נראה ש־ $L \neq L(M)$. על איזה קלט L ו־ $L(M)$ לא מסכימות ־ על $< M >$:)
(לפי האלגוריתם של N)