מודלים חישוביים ־ הרצאה 7

שרון מלטר, אתגר 17

30 באפריל 2024

1 תזכורת

כמה הגדרות מהרצאות קודמות:

$$ACCEPT = \Big\{ < M, w > \Big\}$$

כאשר w היא מילה ו־ M (מכונת טיורינג) מקבלת אותה.

$$HALT = \Big\{ < M, w > \Big\}$$

כאשר w היא מילה ו־ M עוצרת אותה.

$$NOT-EMPTY = \Big\{ < M >: L(M) \neq \emptyset \Big\}$$

בהרצאה הקודמת דיברנו על כך שנרצה לדעת האם שפות אלה כריעות.

ראינו ש־ $ACCEPT$, $HALT$ ו־ $NOT-EMPTY$ ניתנות לקבלה.

2 הקשר בין כריעות של $HALT$ לכריעות של $ACCEPT$

טענה: אם $HALT$ כריעה אז $ACCEPT$ כריעה.
או, בניסוח אחר, אם $ACCEPT$ לא כריעה אז $HALT$ לא כריעה.
נוכיח טענה זו, עוד לפני שאנו יודעים אם $HALT$ או $ACCEPT$ כריעות.

2.1 הוכחה

נניח ש־ $HALT$ כריעה כך שיש מ"ט M_{HALT} שמכריעה את $HALT$ נבנה מ"ט M_{ACCEPT} שמכריעה את $ACCEPT$:

M_{ACCEPT}: בהינתן קלט x, נפרש אותו כ־ $x =< M, w >$ (נצטרך לבדוק האם M מקבלת את w, כמו כן אסור להיכנס ללולאה אינסופית)
נריץ את $< M, w >$ על M_{HALT}. אם הוא לא מתקבל, אז M נכנסת ללולאה אינסופית עבור w כך שהיא לא מקבלת מילה זו ולכן $< M, w > \notin ACCEPT$.
אחרת, נריץ את w על M. אם המילה מתקבלת, אזי נקבל את $< M, w >$ ל־ $ACCEPT$ ואחרת הקלט יידחה (במילים אחרות, נחזיר מה שהמ"ט M מחזירה)

כמובן שנצטרך להוכיח ש־ M_{ACCEPT} מכריעה את $ACCEPT$.
כלומר, להוכיח שאם $ACCEPT \ni < M, w >$ אז M_{ACCEPT} מקבלת את $< M, w >$ ואחרת M_{ACCEPT} דוחה אותה.

<u>הוכחה 1:</u>
אם $< M, w > \in ACCEPT$ אז M מקבלת את w ולכן עוצרת עליה ולכן $< M, w > \in HALT$ כלומר M_{HALT}

עוצרת ומקבלת את $<M,w>$.
אזי נריץ את w על M ומאחר ש־ $<M,w>\in ACCEPT$, המילה w מתקבלת ב־ M, כך שבסופו של דבר נקבל ש־ $<M,w>\in M_{ACCEPT}$ כנדרש.

<u>הוכחה 2:</u>
אם $<M,w>\notin ACCEPT$ אזי M נכנסת ללולאה אינסופית עבור w או דוחה אותה, ובשני המקרים גם M_{ACCEPT} תדחה את $<M,w>$, כנדרש.

3 רדוקציות

ההוכחה שראינו משתמשת בכלי הכי חשוב במדעי המחשב, רדוקציה.
נניח שרוצים לממש פונקציה שמכפילה שני מספרים.
- סטודנט א: "אני אממש פונקציה שמכפילה שני מספרים."
- סטודנט ב': "אני אקח את הפונקציה שמממשת חיבור ואשתמש בה כדי לממש כפל" (כלומר, הוא מבצע רדוקציה מבעיית הכפל לבעיית החיבור)

- סטודנט א': התמהמה
- סטודנט ב': הוא הבין שהוא לא חייב לחכות שסטודנט א' יסיים. במקום זאת, הוא יכתוב תכנית שבה יש קריאות ל־ ADD (לא אכפת לנו איך היא ממומשת, אך זה אומר שגם לא נוכל להריץ אותה)

בסופו של דבר, סטודנט א' פרש מהקורס. אך האם יש ערך לתכנית שסטודנט ב' כתב?
אי אפשר להריץ אותה, אך ניתן להוכיח את נכונותה. סטודנט ב' המיר את הבעיה מלהוכיח נכונות של תכנית לכפל ללהוכיח נכונות של כפל כאשר אנו יודעים שקיימת תכנית לחיבור.
באופן דומה, מקודם הוכחנו שאם $HALT$ כריעה אז $ACCEPT$ כריעה.

המבנה הכללי של רדוקציות הינו;
"בהינתן מימוש ל־ A אני מממשת את B"
או
"אם D לא ניתן למימוש אז A לא ניתן למימוש"
עצה: כאשר עושים רדוקציות, נרצה להאמין בכל ליבנו שסטודנט א' יצליח.

3.1 דוגמה

נוכיח כעת שאם $ACCEPT$ כריעה, אז $HALT$ כריעה.
כמובן שנעשה זאת בעזרת הנחה ש־ $ACCEPT$ כריעה, כך שהמ"ט M_{ACCEPT} מכריעה אותה והוכחת נכונות תכנית שמכריעה את $HALT$, שמסומנת M_{HALT} ומשתמשת ב־ M_{ACCEPT}

כמובן שכל קלט x יתפרש כ־ $x=<M,w>$.
תחילה נריץ את הקלט על M_{ACCEPT}. אם הוא התקבל, אז נקבל אותו גם ב־ M_{HALT}.
אחרת, ניקח את M ונחליף בין $qaccept$ ל־ $qreject$ (כזכור, מ"ט סגורה תחת השלמה). נריץ את $<M,w>$ שוב ב־ M_{ACCEPT}. אם המילה מתקבלת, אז נקבל אותה ב־ M_{HALT} ואחרת נדחה אותה.
כמובן שמוכיחים דוגמה זו באמצעות הפרדה למקרי הקלט (מדובר בהוכחה קלה ♡)

4 $ACCEPT$ לא כריעה - הוכחה

נשים לב לשתי הטענות הבאות;

<u>טענה 1:</u> עבור השפה D שבה כל המילים $<M>$ ו־ M היא מ"ט שמקבלת את $<M>$. השפה $\overline{D}$ לא ניתנת לקבלה.

<u>טענה 2:</u> אם $ACCEPT$ כריעה אז D כריעה.

ביחד, שתי הטענות $1,2$ מוכיחות את המשפט כי אילו $ACCCEPT$ כריעה אז מ־ (2) D כריעה ולכן $\overline{D}$ כריעה (סגירות תחת משלים) אבל $\overline{D}$ לא ניתנת לקבלה ולכן גם לא כריעה, כך שקיבלנו סתירה.

4.1 הלכסון של קנטור

בשביל הוכחת טענה 1, נפתח טכניקת הוכחה (הוכחה ע"י לכסון של קנטור)
תחילה ניזכר בטכניקת הלכסון בדרך שבה הופיעה לראשונה בתורת הקבוצות;

<u>משפט:</u> אין פונקציה על $f : N \to P(N)$
($P(N)$ היא כמובן קבוצת כל תתי הקבוצות של N)

טכניקת ההוכחה: בשלילה, נניח שיש פונקציה F כזו שהיא על. נחשוב על F כעל מערך דו־מימדי אינסופי (של v, x)
במקום ה־ i, j נשאל האם $j \in f(i)$?
אם כן, אז נשמור במקום זה v ואחרת x.
מה מייצגת השורה ה־ i במערך? ־ היא מייצגת את הקבוצה $S = f(i)$. צריכים להראות שיש קבוצה $S^* \subseteq N$ כך שאין $i \in N$ כך ש־ $f(i) = S^*$. כלומר, צריכים להוכיח שקיימת תת־קבוצה של N שאינה מופיעה במערך כשורה.

הרעיון הטכני של קנטור הולך כך;
נסתכל באלכסון ונחשוב עליו כשורה. נהפוך בשורה זו כל v ל־ x ולהיפך. נגלה ש־ "ההיפך מהאלכסון אינו מופיע כשורה במערך" מכיוון שלכל שורה במערך (למשל השורה ה־ i) ההיפך מהאלכסון והשורה לא מסכימים על האיבר ה־ i.
ולכן הקבוצה S^* שמיוצגת ע"י ההיפך מהאלכסון לא מופיעה בשורה, ולא קיים i כך ש־ $S^* = f(i)$. קיבלנו סתירה לכך ש־ F על.

4.2 הוכחת טענה 1

תזכורת: ישנה קונבציה האומרת שכל מחרוזת $x \in \{0,1\}^*$ היא קידוד של מ"ט $<M>$ כמובן שכל x כזה הוא קידוד של מספר (בא"ב בינארי) כלומר;
מספר טבעי $\Leftrightarrow$ קידוד בינארי $\Leftrightarrow$ מ"ט M

כלומר, קיבלנו מספור של כל המ"ט כך שכל המ"ט מופיעות בו (אולי חלקן מופיעות בו יותר מפעם אחת וזה בסדר)
אנחנו רוצים להוכיח ש־ $\overline{D}$ לא ניתנת לקבלה. האם קל לעשות זאת?
ראינו כעת שמספר המ"ט הוא בן מניה מכיוון שהתאמנו לכל מ"ט מספר טבעי.
כמה מילים יש מעל הא"ב $\{0,1\}$? ־ מספר בן מניה.
כמה שפות יש מעל הא"ב $\{0,1\}$? ־ כל שפה היא קבוצה $L \subseteq \{0,1\}^*$ אז במילים אחרות הן איברים $L \in P(\{0,1\}^*)$
העוצמה של $\{0,1\}^*$ היא בת מניה $\aleph_0$ העוצמה של $P(\aleph_0)$ היא רצף.
־ יש $\aleph_0$ מכונות טיורינג וכל אחת מקבלת שפה אחת. עם זאת, יש רצף של שפות (יותר מ־ $\aleph_0$)
כך שאכן מצאנו שישנה שפה שאינה ניתנת לקבלה.

נרצה טיעון יותר עדין שיוכיח ש־ $\overline{D}$ איננה ניתנת לקבלה. ניעזר בלכסון;
נסתכל על המערך הדו־מימדי הבא: במקום ה־ i, j נשים v/x כתלות בהאם M_i מקבלת את המחרוזת j. לכן, כל שורה במערך היא שפה.
כמו מקודם, השפה שמיוצגת על ידי ההיפך מהאלכסון לא יכולה להופיע במערך כשורה, כלומר, היא לא מתקבלת ע"י מ"ט.
נשים לב ש־ $\overline{D}$ היא שפת המילים $<M>$ כך ש־ M מ"ט ו־ M לא מקבלת את $<M>$. כלומר, זוהי השפה שמייצגת את ההיפך של האלכסון (כל איברי האלכסון מייצגים האם קידוד המ"ט מתקבלים על ידי אותה המ"ט)
זוהי הוכחת טענה 1.

כעת שהוכחנו ש־ $D, \overline{D}$ לא כריעות (ולא מתקבלות) כדי להוכיח ששפה אחרת, למשל $ACCEPT$ לא כריעה, מספיק לעשות רדוקציה, כלומר להוכיח שאם $ACCEPT$ כריעה אז D כריעה.

4.3 הוכחת טענה 2

אם $ACCEPT$ כריעה אז D כריעה. נצטרך להניח שיש מ"ט M_{ACCEPT} שמכריעה את $ACCEPT$ ולהשתמש בה כדי לבנות מ"ט M_D שמכריעה את D.

M_D: בהינתן קלט x נחשוב עליו כקידוד של מ"ט $x = <M>$. נצטרך לענות האם M מקבלת את $<M>$.
יש לנו מ"ט M_{ACCEPT} האם M מקבלת את w, לכן יש רק להריץ בה את הקלט $<M,<M>>$.

<u>הוכחת נכונות:</u> מכיוון ש־
$<M> \in D \Leftrightarrow$ M מקבלת את $<M> \Leftrightarrow <M,<M>> \in ACCEPT$
וכיוון ש־ M_{ACCEPT} מכונה מכריעה, אז M_D שבסה"כ קוראת לה, עוצרת על כל קלט.

סיימנו את שתי ההוכחות ♡
כעת אנו יודעים ש־ $ACCEPT$ איננה כריעה.

תזכורת ־ שאלות שהיו לנו וכעת יש לנו תשובות אליהן

- בתחילת הקורס, שאלנו מהו הוא בעצם מחשב, התשובה לכך הייתה מ"ט.
- שאלנו אילו שפות הן כריעות, וכעת אנו יודעים ששפה היא כריעה אם ניתן לבנות מ"ט שמכריעה אותה וכדי להראות שהיא לא כריעה מספיק להראות שאילו הייתה כריעה קיימת שפה לא־כריעה ידועה שהייתה כריעה.
- גילינו מדוע תכנית מחשב לעולם לא תוכל לדעת האם היא תיכנס ללולאה אינסופית. לכן אנו גם יודעים מדוע היה לנו הרבה יותר קל אילו $HALT$ הייתה כריעה.

ביצענו רדוקציה משאלות גדולות ומסובכות לשאלות שאנו יכולים להתמודדד איתן.
שימו לב שהצגנו את הרדוקציות לפני שידענו האם $ACCEPT$, $HALT$ כריעות. כביכול הדבר הטבעי הוא קודם להוכיח ש־ $ACCEPT$ לא כריעה ואז להציג את הרדוקציה. כאן הפכנו את הסדר כדי להראות שאפשר לעשות רדוקציות גם בלי לדעת האם השפות כרעיות או לא כריעות.
עם זאת, נרצה לפתח שיטה מסודרת יותר לשימוש ברדוקציות.

5 שיטה סיסטמתית לרדוקציות

<u>הגדרה:</u> עבור שתי שפות L_1, L_2 אומרים ש־ L_1 ניתנת לרדוקציית מיפוי ע"י L_2, ומסמנים זאת $L_1 \leqslant_m L_2$ אם קיימת מ"ט R (שמקבלת מחרוזת ומחזירה מחרוזת) כך שמתקיים:

1. לכל $x \in \Sigma^*$, R עוצרת על x.
2. לכל $x \in \Sigma^*$, $x \in L_1 \Leftrightarrow R(x) \in L_2$

מה שזה אומר, זה שקיימת פונקציה $R : \Sigma^* \to \Sigma^*$ שלכל קלט שהינו מילה מ־ L_1 הפלט שלה יהיה מילה מ־ L_2.
שימי ♡ ־ R לא חייבת להיות על או חח"ע.

5.1 אינטואיציה

נניח שאנו רוצים לבנות מ"ט שמכריעה את L_1. כלומר, אנו בתור קלט $x \in \Sigma^*$ ושואלים "האם $x \in L_1$?"
הרדוקציה R מאפשרת לנו לחשב $y = R(x)$ כך ש־ $x \in L_1 \Leftrightarrow R(x) \in L_2$. כלומר, אם למשל יש לנו מ"ט M_2 שמכריעה את L_2 אז נוכל לבנות מ"ט M_1 שמכריעה את L_1, ע"י $M_1(x) = M_2(R(x))$ על קלט x הרץ R כדי לקבל $R(x)$ ואז הרץ M_2 על $R(x)$ ועונה מה שהוא עונה.
ההגדרה מבטיחה לי ש־ M_1 מכריעה את L_1.
באופן כללי, רדוקציה היא דרך להעביר את השאלה מהאם $x \in L_1$ לשאלה האם $R(x) \in L_2$.

5.2 תכונות

משפט: אם $L_1 \leqslant_m L_2$ אז:

1. אם L_2 כריעה אז L_1 כריעה.
2. אם L_1 לא כריעה אז L_2 לא כריעה.

שימי לב שכמובן החלק השני הוא פשוט הקונטרפוזיטיב של הראשון.
הוכחה: (1) –
תהיה M_2 מ"ט שמכריעה את L_2 וידוע לי שיש מ"ט R כך שלכל $x \in \Sigma^*$:
R עוצרת על x ו־ $x \in L_1 \Leftrightarrow R(x) \in L_2$.
נבנה מ"ט M_1 ע"י $M_1(x) = M_2(R(x))$.
צ.ל ש־ M_1 מכריעה את L_1.

טענה: M_1 עוצרת על כל קלט.
טענה זו נכונה מכיוון ש־ R ו־ M_2 עוצרות על כל קלט.

זוהי כל ההוכחה שצריכים :)
כעת, כדי להוכיח שאיזושהי שפה L_2 לא כריעה, מספיק להוכיח ש־ $L_1 \leqslant_m L_2$ כך ש־ L_2 לא כריעה.

השערה: כל שפה שקשורה בבדיקה של חישוב של מ"ט היא לא כריעה.

ההשערה הזו לא יכולה להיות נכונה. למשל, שפת כל הקידודים $< M >$ של מ"ט M היא שפה כריעה. אבל אנחנו נראה שההשערה נכונה, אם כי בניסוח מעט שונה.

6 משפט $RICE$

"כל בעיה שקשורה בבדיקה של מ"ט אינה כריעה"

קונבנציה של רונן: כל מחרוזת מעל Σ^* היא קידוד של איזושהי מ"ט.
בחלק זה נתעניין בשפות מהצורה שבהן מילים שמיוצגות כ־ $< M >$.