מודלים חישוביים - הרצאה 1

שרון מלטר, אתגר 17

21 באפריל 2024

1 הרצאה 1 - $5.3.24$

1.1 הקדמה

מודלים חישוביים הוא קורס המתייחס למחשבים כמדע, לא רק כנושא פרקטי.
כמו כן, זהו קורס מתמטי. כלומר נצפה לשאלה, תשובה והוכחה. נצפה לכתיבה פורמלית וברורה.
אנו נשאל את עצמנו בעיות ספציפיות. בעיות ספציפיות הן - נתון קלט X ונרצה לקבל פלט F(X). נשאל את עצמנו כדי מחשבים יכולים לתת לכך תשובה. לדוגמה:
פונקציית הכפל, שמקבלת שני מספרים ופולטת את מכפלתם.
הפונקציה הזאת היא פונקציה שבה מרחב הקלט הוא שני מספרים ומרחב הפלט הוא מספר אחד. נרצה לשמור את שניהם בעזרת מחרוזות. איך נעשה זאת?

1.2 הגדרות

א"ב סופי היא קבוצה Σ שאיבריה נקראים תווים, שהינה סופית ולא ריקה.
למשל קבוצה של האותיות האנגליות או הספרות מ-0 עד 9.

מילה/מחרוזת היא סדרה סופית של תווים.

שרשור של מילים הוא הוספת מילה לסוף של מילה אחרת, ויצירת מילה חדשה מצירוף זה. הוא מסומן $w_1 \bigcirc w_2$.

המילה הריקה, ϵ, היא מילה עם אפס תווים.

האורך של מילה w מתוך קבוצת מילים מסומן ב- $|w|$. זהו מספר התווים שלה.

קבוצת כל המילים של א"ב מסוים מסומנת ב- $\Sigma*$.

שפה L היא קבוצה של מילים.

שרשור של השפה L_1 עם L_2 שמסומן $L_1 \bigcirc L_2$, הוא השפה;

$$L_1 \bigcirc L_2 = \left\{w_1 \bigcirc w_2 | w_1 \in L_1, w_2 \in L_2\right\}$$

1.3 מבנה הקורס

בקורס דוגמאות לבעיה שמחשבים שיכולים לפתור עם מחרוזות: בדיקה של האם טקסט מהווה קובץ שניתן לקימפול בשפה C.
בדיקה של האם קוד מכניס ללולאה אינסופית. קל להבין למה נרצה לדעת איך לפתור בעיה כזאת.
אך מחשבים לא יכולים לפתור בעיה זאת, גם לא לאחר שיפור הטכנולוגיה. נוכיח זאת בהמשך הקורס. באופן כללי נלמד אילו בעיות מחשבים יכולים לפתור ואילו לא.

נעבור להגדרת לסוג ראשון ונפוץ של בעיות;
בעיות שבהן הפלט הוא כן או לא, נקראות **בעיות הכרעה**. כל בעיה כזו מגדירה שפה L ולהיפך. איך?
בהינתן מילה $w \in \Sigma*$, יש לקבוע האם $L \in L$. השיוך הזה קובע את ההכרעה עבור המקרה.

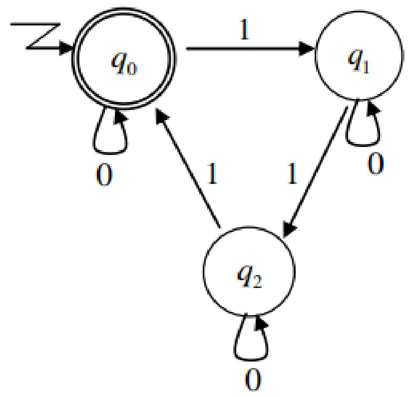
אבל אילו בעיות מחשבים לא יכולים לפתור?
קודם כל, נצטרך להגדיר מהו מחשב. רק כך נוכל להתייחס לשאלה באופן מתמטי. שליש מהקורס נקדיש להגדרה של מחשב.
לאחר מכן נוכל לבנות מודל מתמטי של בעיה שמחשב מסוגל לפתור. תחום זה נקרא חשיבות וקביעות ואי קביעות.
לאחר מכן, נשאל שאלה עדינה יותר־ מה מחשבים יכולים לפתור ביעילות? (בין היתר שאלת ה־P ו־ NP) זהו החלק האחרון של הקורס.

אינטואיציה: הבדלה בין שאלות שמחשב יכול לפתור לשאלות שלא.

קלט: גרף G
פלט: האם יש מסלול אוילריאני (מסלול בו עוברים בכל קשת פעם אחת בלבד)
בעיה זאת ניתן לפתור בלי לעבור על כל מסלול. ניתן פשוט לבדוק האם הדרגה של כל צומת היא זוגית. לכן זוהי בעיה ששייכת למחלקה P

לעומת זאת, נסתכל על הבעיה הבאה:
קלט: גרף G
פלט: האם קיים מסלול המילטוני (מסלול שבו עוברים בכל צומת פעם אחת)
יש סיבות טובות לחשוב שאין פתרון יעיל לבעיה. לכן, זוהי בעיה שחושבים שהיא שייכת למחלקה NP.
אחת השאלות הגדולות היא האם $P = NP$, כלומר האם בכלל קיימות בעיות קשות.
נעבור למחשבים הראשונים שנראה בקורס.

אוטומט סופי דטרמיניסטי - אס"ד
אוטומט סופי דטרמיניסטי מורכב ממצבים, אחד המצבים ייקרא התחלתי ומסומן בזיגזג עם חץ. חלק מהמצבים ייקראו מקבלים, יש לפחות מצב אחד כזה. מכל מצב יוצאים חצים, חץ לכל מילה מעל הא"ב. חלקם יכולים להצביע בחזרה לאותו מצב.
האס"ד הינו מחשב. הוא מגדיר שפה (שכפי שצוין היא בעיית הכרעה) של כל המילים שמגיעות למצב המקבל.
דוגמה:



קל לראות שאס"ד זה מקבל את קבוצת המילים שמספר האחדות שלהן מתחלק ב־3. ניתן להוכיח זאת פורמלית באינדוקציה.
טענת האינדוקציה: כאשר יש i אחדות במילה, היא תגיע למצב q_i. זוהי טענה חזקה יותר מהטענה שרצינו להוכיח, אך מצבים אלה נפוצים. הוכחה זו קלה.

אילו שפות נוכל להגדיר עם אס"ד?
תחילה נגדיר אס"ד באופן מתמטי ולא ציורי. אס"ד הוא החמישייה $M = (Q, \Sigma, \delta, q_0, F)$.
שאלו קבוצת המצבים (קבוצה סופית, כמובן), א"ב סופי, מצב התחלתי $q_0 \in Q$, $F \subseteq Q$, ו־ $\delta : Q \times \Sigma \to Q$ פונקציית המעבר.
לכל מילה W שמעבירים אותה לאס"ד M יש מסלול חישוב, שזוהי סדרה סופית של מצבים אשר מוגדרת כך;

$$r_0 = q_0, \quad r_{i+1} = \delta(r_i, a_{i+1})$$

כמו כן נסמן $S_M(W) = r_n$, כך שזהו האיבר האחרון במסלול החישוב ונסמן קבוצת המילים שמתקבלות באס"ד.

1.4 אוטומט מכפלה

זהו אוטומט שמטרתו לקבל את המכפלה הקרטזית של שתי שפות, הוא מקבל מילים לפי איך שנבחר־ ניתן להגדיר שהוא יקבל מילה רק אם היא בשתי השפות, או בשפה כלשהי, או כן באחת ולא באחרת... נראה בקרוב כיצד.
הדרך הראשונה שקופצת לראש כאשר רוצים לבדוק האם מילה מתקבלת באחד משני אס"דים היא פשוט להעביר אותה דרך אחד ואז דרך השני. אך הזיכרון היחיד שיש לנו במכונת מצבים הוא המצב הנוכחי והתו הבא, אין איך לגשת לתווים פעם שנייה.
לכן הפתרון הוא להגדיר אוטומט שבו כל מצב הוא זוג סדור של מצבים־ המצב עבור צעד באס"ד והמצב עבור צעד באס"ד שני. נבנה אותו כך:
יהיו

$$M_1 = (Q_1, \Sigma_1, \delta_1, q_0^1, F_1), \quad M_2 = (Q_2, \Sigma_2, \delta_2, q_0^2, F_2)$$

שני אס"דים. אוטומט המכפלה שלהם יהיה;

$$M = (Q, \Sigma, \delta, q_0, F)$$

כאשר;

$$Q = Q_1 \times Q_2, \quad \Sigma = \Sigma_1 \cup \Sigma_2, \quad \delta((q,p),a) = (\delta(q,a), \delta(p,a))$$

ואת F בוחרים לפי מתי רוצים לקבל מילה. למשל;

$$F = F_1 \cap F_2, \quad F_1 \cup F_2, ...$$

1.5 משפטים והוכחות ־ סגירות פעולות על שפות

<u>משפט:</u>
אם ניתן לקבל שפה L באס"ד, אז ניתן גם לקבל את השפה המשלימה $\overline{L}$ באס"ד אחר.

<u>הוכחה:</u>
תהי L שפה <u>מתוארת</u> על ידי אס"ד. כלומר, קיים אס"ד $M = (Q, \Sigma, \delta, q_0, F)$ כך ש־ $L = L(M)$. צ"ל שיש אס"ד M' כך ש־ $L(M') = \overline{L(M)}$.
רעיון: הוכחה ע"י בנייה, נתאר איך בונים את M' בהינתן M. נחליף בין מצבים מקבלים, ללא מקבלים.
(הערת המרצה: זהו קורס מתמטי בו אין לחשוב שמשהו הוא נכון אלא אם הוא הוכח וגם ברור לקורא שהוא הוכח. יש לוודא שהכתיבה ברורה ופורמלית)
בנייה: נגדיר $M' = (Q', \Sigma, q_0', \delta', F')$

$$Q' = Q, q_0' = q_0, \delta' = \delta, F' = \{q \in Q : q \notin F\} = Q/F = \overline{F}$$

נוכיח ש־ $L(M) = L(M')$:

$$L(M') = \{w \in \Sigma^* : S_{M'}(w) \in F'\}$$

$$L(M') = \{w \in \Sigma^* : S_M(w) \in F'\}$$

$$L(M') = \{w \in \Sigma^* : S_M(w) \notin F\}$$

$$L(M') = \overline{L(M)}$$

משפט שני־
אם L_1, L_2 מתקבלות על ידי אס"ד אז $L_1 \cap L_2$ מתקבלת ע"י אס"ד.
<u>הוכחה:</u>
יהיו L_1, L_2 שפות שמתקבלות על ידי אס"ד. נסמן $L_1 = L(M_1), L_2 = L(M_2)$ עבור אס"דים:

$$M_1 = (Q_1, \Sigma, q_0^1, \delta_1, F_1), \quad M_2 = (Q_2, \Sigma, q_0^2, \delta_2, F_2)$$

צ"ל שיש אס"ד $M = (Q, \Sigma, \delta, q_0, F)$ כך ש־ $L(M) = L(M_1) \cap L(M_2)$.
איך נדע אם מילה שייכת לשני האס"דים?
האינטואיציה הראשונה אומרת להעביר את המילה דרך שני האס"דים. אך במכונות מצבים הזיכרון היחיד הוא המצב הנוכחי, ברגע שעוברים על תו הוא נשכח. אזי נעבור על שני האס"דים במקביל.
רעיון: (את הרעיון אנו כותבים בשביל האנשים שקוראים את ההוכחה)
נגדיר $Q = Q_1 \times Q_2 = \{(q_1, q_2) : q_1 \in Q_1, q_2 \in Q_2\}$. נשים לב שמכיוון ש־ Q_1, Q_2 סופיות, גם Q סופית. תוך כדי הריצה, ננסה לשמר את השמורה שהמצב אליו M מגיע הוא בדיוק זוג המצבים q_1, q_2 שאליהם הוא מגיע ב־ M_1, M_2 בקריאת אותה המילה. אם אשמור את השמורה, אז בסוף הריצה נחליט לקבל את המילה אס"ם $q_1 \in F_1, q_2 \in F_2$.
בניית M:

$$Q = Q_1 \times Q_2, \quad q_0 = (q_0^1, q_0^2), \quad F = \{(q_1, q_2) \in Q : q_1 \in F_1, q_2 \in F_1\}, \quad \delta((q_1, q_2), a) = (\delta_1(q_1, a), \delta_2(q_2, a))$$

טענה: $L(M) = L(M_2) \cap L(M_1)$
טענת עזר: לכל $w \in \Sigma^*$ מתקיים $S_M(w) = (S_{M_1}, S_{M_2})$
נוכיח את הטענה המרכזית בעזרת טענת העזר.

$$L(M) = \{w \in \Sigma^* : S_M(w) \in F\}$$

$$= \{w \in \Sigma^* : (S_{M_1}(w) \in F_1) \cap (S_{M_2}(w) \in F_2)\}$$

$$= L(M_1) \cap L(M_2)$$

כלומר, אם טענת העזר נכונה, הטענה המרכזית נכונה. נוכיח את טענת העזר באינדוקציה, על $|w|$.
<u>בסיס:</u> $|w| = 0$
אזי $w = \epsilon$ כך ש־ $S_M(w) = S_M(\epsilon) = q_0 = (q_0^1, q_0^2)$
<u>צעד:</u>
נניח שהטענה נכונה לכל $|w| \leqslant k$ עבור k טבעי ונוכיח שהיא נכונה עבור המספר הטבעי העוקב $k+1$.
תהי מילה w באורך $k+1$. נפרק אותה לשרשור $w = a \bigcirc u$ כך ש־ $a \in \Sigma, u \in \Sigma^*$. כמובן ש־ $|a| = n$ ולכן טענת האינדוקציה נכונה עבור מילה זו. מכאן נקבל ש־

$$S_M(w) = S_M(u \bigcirc a)$$

$$S_M(w) = \delta(S_M(u), a)$$

$$S_M(w) = \delta((S_{M_1}(u), S_{M_2}(u)), a)$$

$$S_M(w) = (\delta_1(S_{M_1}(u), a), \delta_2(S_{M_2}(u), a))$$

$$S_M(w) = (S_{M_1}(u \bigcirc a), S_{M_2}(u \bigcirc a))$$

$$S_M(w) = (S_{M_1}(w), S_{M_2}(w))$$

כנדרש.

(לא בכל ההרצאות נוכל להוכיח באותו פירוט של ההוכחה הבאה, אך כן נדרשים לכך בתרגילי הבית ובמבחן)

<u>משפט שלישי</u>

פעולת האיחוד סגורה תחת אס"ד. כלומר, אם שתי שפות ניתנות לתיאור על ידי אס"ד, גם האיחוד שלהן ניתן לקבלה ע"י אס"ד.

<u>הוכחה:</u>

לפי חוקי דה־מורגן, מתקיים $L_1 \cup L_2 = \overline{\overline{L_1} \cap \overline{L_2}}$ וגם $L_1/L_2 = L_1 \cap \overline{L_2}$, כך שמאחר שחיתוך והשלמה סגורים תחת אס"ד, גם איחוד סגור תחת אס"ד.

ישנה גם הוכחה אלטרנטיבית, שהינה זהה להוכחה לכך שפעולת החיתוך הסגורה, אך קבוצת המצבים המקבלים היא $F = F_1 \cup F_2$ ולא $F = F_1 \cap F_2$.