חישוביות ומבוא לסיבוכיות

arch7486730@gmail.com -דורון מור abhauc97@gmail.com -שני שוב nir16832@gmail.com -ניר סון

מנהלות

שעות קבלה יפורסמו במודל.

ציון הקורס ייבנה מ 85% ציון מבחן ו- 15% ציון מטלות (מגן). יש לעבור את הבחינה בשביל

לשקלל את המטלות. יהיו 2-3 מטלות במהלך הקורס.

(הסילבוס במודל הוא עבור סמסטר רגיל. פרט לשמות הסגל וסדר הנושאים, הכל זהה).

יהיו לנו שני חלקים עיקריים לקורס:

1. <u>חישוביות:</u> בעיות שניתן לפתור על ידי מחשב.

2. <u>סיבוכיות:</u> נחלק את עולם הבעיות שלנו לכמה מחלקות לפי סיבוכיות זמן הריצה

שלהן. (אפשר לקרוא לחלק הזה "יעילות")

מודל חישובי

- מודל חישובי הוא מכונה תאורטית עם רכיבים מסוימים. למשל: גודל זיכרון, א"ב, סרט קלט.
 - כשנדבר על מודלים חישוביים נדבר על אלגוריתם כללי לפתרון הבעיה.
 - באוטומטים ראיתם מודלים חישוביים כמו אס"ד, ואוטומט מחסנית.
 - המודל החישובי העיקרי שלנו בקורס יהיה מכונת טיורינג- עליו נרחיב בהמשך.

פסוקים

- בשקפים הבאים יהיו כמה דוגמות לגבי "פסוק".
 - לא מדובר בפסוקים מהחומש או מהתנ"ך.
- פסוק שנעסוק בו הינו פונקציה בוליאנית בצורת CNF (המוכרת ממערכות oernic POS). לדוגמה:

$$(x_1 \lor \overline{x_2} \lor x_4) \land (x_2 \lor \overline{x_3} \lor x_4)$$

• "השמה מספקת" שנפגוש בשקפים הבאים – הצבת ערכי True, False למשתנים כך שהפסוק מקבל ערך True.

בעיה

אפשר להסתכל על שני סוגים של בעיות- בעיית קיימות ובעיית חיפוש. בקיימות אנחנו רק רוצים לדעת אם יש פתרון, בחיפוש אנחנו רוצים לדעת- אם יש פתרון, מהו.

דוגמות:

- בהינתן גרף האם יש בו מסלול המילטוני? אם יש בו אז מהו
- בהינתן פסוק האם הוא ספיק? אם כן אז מהי ההשמה המספקת שלו?
 - ?בהינתן לוח סודוקו $n^2 imes n^2$, האם הוא פתיר מהו הפתרון

אנו נעסוק בעיקר בבעיות הקיימות. נפגוש בבעיות האלו בהמשך וכמובן נגדיר במדויק את כל המונחים.

פתירות של בעיה

- פתירות של בעיה היא ביחס למודל חישובי כלשהו.
- כשנאמר שבעיה כלשהי לא פתירה על ידי מודל חישובי כלשהו, הכוונה שלנו היא שאין
 פתרון כללי לכל הבעיה, אין הכוונה שאין אלגוריתם היודע לפתור מקרים פרטיים.

למשל, בהינתן פסוק כלשהו, נרצה לדעת אם הוא ספיק או לא. אנחנו לא מחפשים לדעת עבור פסוק ספציפי אם יש פתרון, אלא אלגוריתם שבהינתן כל פסוק שהוא יקבל, ידע לענות אם קיימת השמה מספקת.

פתירות של בעיה

- . גם בעיות פתירות ניתן לסווג לבעיות 'קלות' ובעיות 'קשות'.
- י נסווג אותן לפי זמן הריצה המינימלי הנדרש כדי לפתור אותן, כאשר זמן ריצה הוא פונקציה של אורך הקלט. למשל עבור פסוק, זמן הריצה יחושב עבור n משתניו.
- . נאמר שבעיות 'קלות' הן בעיות שיש אלגוריתם שיודע לפתור את הבעיה בזמן ריצה פולינומי.
 - נאמר שבעיות 'קשות' אם כל אלגוריתם צריך זמן ריצה לפחות אקספוננציאלי בגודל הקלט.
 - כדי להראות שבעיה היא קלה- מספיק להראות קיימות של אלגוריתם בעל זמן ריצה פולינומי (ולהוכיח את זמן הריצה)
 - כדי להראות שבעיה היא קשה יש להוכיח שלא קיים אלגוריתם פולינומי שיפתור אותה.

ייצוג בעיה על ידי שפה

מכונות טיורינג יעבדו על גרפים, פסוקים, פולינומים ועוד, כאשר המכונה תקבל כקלט קידוד של האובייקט עליו היא עובדת.

X>-אובייקט יסומן לרוב ב-X כאשר הקידוד שלו יסומן כ

כשנרצה לעסוק בבעיה כלשהי, לדוגמה בעיית קשירות של גרף, המכונה תקבל קידודי גרפים שונים והיא תצטרך לפעול עליהם.

לדוגמה, מכונת טיורינג שתבדוק אם גרף G כלשהו קשיר, תקבל כקלט את קידוד < G >.

מודל החישוב – מכונת טיורינג

למה שנדבר בכלל על מכונה שטיורינג המציא בשנות ה-40?

- כי נוכיח בהמשך שהיא שקולה למחשב. כלומר, כל מה שניתן לבצע ביעילות במ"ט, נוכל לבצע ביעילות גם במחשב.
 - . כי יהיה יותר נח לדבר עליה מאשר על מחשב
- כי האלגוריתמים שנדבר עליהם כלליים, ולא רוצים להוריד אותם לרמת "שפת תכנות" כזו או אחרת.
- יש המודל יחסית פשוט (בטח בהשוואה למחשב), ויהיה קל להוכיח עליו טענות.
- כי יש למ"ט זיכרון אינסופי, שזה כבר נשמע טוב ביחס לתוכנות מחשב גדולות
 - כי המרצים רוצים לאמלל לנו את החיים ולא מוכנים שנתכנת.

הקדמה למכונת טיורינג

- M מכונת טיורינג תסומן M
- בעלת סרט חד צדדי אינסופי. •
- . המקודדת על הסרט $x\in\Sigma^*$ המקודדת על הסרט $x\in\Sigma^*$
- ראש קורא כותב, מצביע על תא בסרט, קורא את התו שנמצא בו וכותב עליו במידת הצורך. לא הולך יותר שמאלה מהתא הכי שמאלי.
 - קבוצת **מצבי בקרה** (אי אפשר להיפטר מהם).

רכיבי מכונת טיורינג

- :כאשר $M=(Q,q_0,\!F,\!\Gamma,\!\Sigma,\!ar{b},\!\delta)$ כאשר $M=(Q,q_0,\!F,\!\Gamma,\!\Sigma,\!ar{b},\!\delta)$
 - היא קבוצת מצבים סופית. Q
 - . הינו המצב ההתחלתי q_0
 - הינה קבוצת המצבים הסופיים. $F \subseteq Q$
 - $(\Sigma = \{0,1\}$ הינה א"ב הקלט. (בדר"כ בקורס $\Sigma \subseteq \Gamma$
 - $(\Gamma = \{0,1,\overline{b}\}$ הינה א"ב עבודה. (בדר"כ בקורס Γ •
 - $(ar{b}
 otin \Sigma$ נקרא "בלנק", סימון של תא ריק. (לפי הגדרה, סימון של $ar{b}$ •
- δ : $(Q \setminus F) \times \Gamma \to Q \times \Gamma \times \{R,L,S\}$ היא פונקציית המעברים. δ •

פונקציית המעברים

תכונות מכונת טיורינג

- בהגיעה למצב סופי היא עוצרת, היא עשויה גם לא להגיע לכזה לעולם, היא עשויה גם לא להגיע לכזה לעולם, היא עשויה גם לא להגיע לכזה לעולם, היא עשויה גם לא להגיע לכזה לעולם...
- . והיא כל התווים על הסרט שמשמאל לראש $y \in \Gamma^*$ פלט המכונה הוא מילה $y \in \Gamma^*$
 - אם M לא עצרה על x, אזי הפלט שלה לא מוגדר. זה מאפשר חישוב פונקציות "לא מלאות".
 - ישנן מ"ט המחשבות פונקציות וישנן המזהות שפות.
 כשאנחנו במכונה המחשבת פונקציה- נתמקד בפלט המכונה.
 כשאנחנו במכונה המזהה שפה- נתמקד במצב בו סיימנו (מקבל או דוחה).
 - $f_M(x)$ בתור M בתור •

 $x1 \in \{0,1\}^*$:השפה

 $M=(Q,q_0,F,\Gamma,\Sigma,\overline{b},\delta)$:פתרון

Q/F	\Diamond	1	5
90			
91			

 $x1 \in \{0,1\}^*$:השפה

 $M=(Q,q_0,F,\Gamma,\Sigma,\overline{b},\delta)$:פתרון

Q/F		1	5
90	(q.,0,R)		
91	(90,0, R)		

1

 $x1 \in \{0,1\}^*$:השפה

 $M=(Q,q_0,F,\Gamma,\Sigma,\overline{b},\delta)$:פתרון

Q/F r		1	5
90	(q.,0,R)	(91, 1, 1)	
91	(90,0, R)	(91,1,R)	

 $x1 \in \{0,1\}^*$:השפה

 $M=(Q,q_0,F,\Gamma,\Sigma,\overline{b},\delta)$:פתרון

Q/F		1	5
90	(q.,0,R)	(91,1,12)	(grej, O,R)
91	(90,0, R)	(91,1,R)	(gace, 1, R)

$$f(x) = 0 \cdot x$$

$$M = (Q = \{q_0, q_1, q_{end}\}, q_0, F = \{q_{end}\}, \Gamma = \{0, 1, \overline{b}\}, \Sigma = \{0, 1\}, \overline{b}, \delta)$$

Q / F	\Diamond	1	5
90			
91			

$$f(x) = 0 \cdot x$$

$$M = (Q = \{q_0, q_1, q_{end}\}, q_0, F = \{q_{end}\}, \Gamma = \{0, 1, \overline{b}\}, \Sigma = \{0, 1\}, \overline{b}, \delta)$$

Q \ F		1	5
90	(q., O, R)		
91	(q0,0,1)		

$$f(x) = 0 \cdot x$$

$$M = (Q = \{q_0, q_1, q_{end}\}, q_0, F = \{q_{end}\}, \Gamma = \{0, 1, \overline{b}\}, \Sigma = \{0, 1\}, \overline{b}, \delta)$$

Q/F		1	5
20	(q., O, R)	(91,0,R)	
91	(90,01B)	$(q_1, 1, R)$	

$$f(x) = 0 \cdot x$$

$$M = (Q = \{q_0, q_1, q_{end}\}, q_0, F = \{q_{end}\}, \Gamma = \{0, 1, \overline{b}\}, \Sigma = \{0, 1\}, \overline{b}, \delta)$$

Q\F	Υ_		1	5
90		(q., O, P)	(91,0,R)	(gend, O, R)
91		(90,01B)	(q1,1,R)	(gend, 1, 12)

הפסקה

קונפיגורציה היא מעיין תמונת מצב במהלך ריצת המכונה- לפני או אחרי השלמה של פעולת חישוב ב- δ .

כאשר: c=(lpha,q,i) קונפיגורציה היא שלשה

- (עד הבלנק הראשון שהחל ממנו הכל בלנקים, לא כולל) תוכן הסרט. $\alpha \in \Gamma^*$
 - . המצב הנוכחי $q \in Q$
 - מיקום הראש הקורא כותב. $i \in \mathbb{N}$ •

ניתן לתאר ריצת מכונת טיורינג ע"י סדרת קונפיגורציות.

(דומה ברעיון למה שפגשנו באוטומטים כ "תיאור רגעי" של א"מ)

ההגדרה של "תוכן הסרט" קצת מורכבת. בקונפיגורציה הראשונה מדובר על הקלט, אבל עם התקדמות המכונה יתכן ויהיה כתוב שם תוכן שונה לחלוטין.

נסמן T מספר הצעדים ש M ביצעה עד כה על הקלט x. אזי, התא הימני $\max\{t,|x|\}$ יכיל את $t \leq T$ ביותר בו ביקרנו בסרט, t, מקיים $t \leq T$. נקבע ש t יכיל את התאים הראשונים של הסרט.

כאשר x היא המילה אותה קיבלנו כקלט,

 $(x, q_0, 1)$ קונפיגורציה התחלתית: •

כאשר u הוא תוכן הסרט כעת ו- i הוא מיקום הראש כעת.

- (u, q_{accept}, i) קונפיגורציה מקבלת: •
- (u, q_{reject}, i) : קונפיגורציה דוחה •
- $q \in F$ כאשר (u, q, i) כאשר •

(לפעמים נקרא לזה קונפיגורציה סופית)

צעד חישוב

יבוצע כך: c=(lpha,q,i) יבוצע כך:

אם α_i (עברנו מצב); p יוחלף בq אזי: q יוחלף ב $\delta(q,\alpha_i)=(p,b,d)$ אם d יוחלף לפי d.

שימו לב כי אם d=L אזי מעדכנים את המיקום לפי (מאd=L שימו לב כי אם נופלים מצד שמאל של הסרט).

ניתן לתאר ריצת מכונת טיורינג ע"י סדרת קונפיגורציות.

 c_0, c_1, \dots על קלט x הינה סדרת קונפיגורציות M המקיימת:

- קונפיגורציה התחלתית c_0 -
 - $\forall i > 0: c_{i-1} \vdash_M c_i$
- אם קיימת קונפיגורציה סופית c=(lpha,q,i) אז היא האחרונה בסדרה, והפלט אם קיימת קונפיגורציה סופית $\alpha[1 \dots i-1]$ של m על m מוגדר להיות m
 - אם הסדרה לא מכילה קונפיגורציה סופית, אזי הסדרה היא אינסופית, $f_M(x) = \perp$ על M על x לא מוגדר. במקרה זה נסמן כי הפלט M

Q/F	γ_	0	1	5
90		(q., O, R)	(q1,0,R)	(gend, O, R)
91		(90,01K)	(q1,1,R)	(gend, 1, R)

דוגמת הרצה + קונפיגורציות

1001 = x כאשר

, $f(x) = 0 \cdot x$ נניח שאנחנו במכונה המחשבת את הפונקציה

$$C_{0} = (1001, 90, 1)$$

Q/F r	\Diamond	1	5
90	(9., 0, R)	(q1,0,R)	(gend, O, R)
91	(90,01 K)	(q1,1,R)	(qend, 1, 12)

דוגמת הרצה + קונפיגורציות

, $f(x) = 0 \cdot x$ נניח שאנחנו במכונה המחשבת את הפונקציה

1001 = x כאשר

$$C_{0} = (1001, q_{0}, 1)$$

$$C_{1} = (1001, q_{0}, 1)$$

$$C_{2} = (0101, q_{0}, 2)$$

$$C_{3} = (0101, q_{0}, 4)$$

$$C_{4} = (0100, q_{1}, 5)$$

$$C_{5} = (01001, q_{0nd}, 6)$$

$$0100155$$

$$C_{5} = (01001, q_{0nd}, 6)$$

הוכחת נכונות הבנייה

?כיצד נוכיח שהמכונה שבנינו עובדת

ההוכחה הפורמלית מתייחסת לקלט x באורך n. הטענה החזקה שנוכיח היא שהחישוב של x הוא רצף קונפיגורציות מהצורה הבאה:

$$c_0,c_1,\dots,c_{n+1}$$
 , $c_0=(q_0,x,1)$ כאשר $c_0:c_i=(q_{x_i},0x_i\dots x_{i-1}x_{i+1}\dots x_n,i+1)$, $c_0:c_i=(q_{x_i},0x_i\dots x_{i-1}x_{i+1}\dots x_n,i+1)$, $c_0:c_{n+1}=(q_{end},0x,n+2)$ ולבסוף $c_0:c_{n+1}=(q_{end},0x,n+2)$

ההוכחה לא קשה, אך לא נעשה זאת. בד"כ אפילו לא ננסח את הטענה הזו.

?הפסקה

שקילות מודלים

לכל מודל A של מכונת חישוב, נגדיר:

A קבוצת כל הפונקציות הניתנות לחישוב ע"י מכונה כלשהי מהמודל F_A

 $A_{A}=F_{B}$ אז: בהינתן שני מודלים שונים A_{A} נאמר שהם שקולים אם"ם

מסקנה: כדי להוכיח ששני מודלים שקולים, צריך להוכיח ש<u>הקבוצות</u> של הפונקציות המתאימות לשני המודלים שוות.

(ע"י הכלה דו כיוונית)

.TM אינו שקול לPDA, ולא ל $DFA \equiv NFA \equiv \epsilon - NFA$, אינו שקול ל הוכחה (לחלק השני): תהי

 $Primality = \{p \in \{0,1\}^* | p \text{ is binary representation of a prime number}\}$ מ"ט מכריע את השפה (לבדוק חלוקה עד השורש) אבל השפה אינה ח"ה.

שקילות מודלים – מכונות שקולות

 $x \in \Sigma^*$ יקראו שקולות אם לכל קלט M_1, M_2 הגדרה: שתי מכונות טיורינג המכונות זהה.

- $M_1(x)$ אם $M_1(x)$ מוגדר, אז גם $M_2(x)$ מוגדר, ושווה ל $M_1(x)$
 - . אם $M_2(x)$ לא מוגדר, אז גם $M_1(x)$ לא מוגדר $M_1(x)$

$$f_{M_1}(x) = f_{M_2}(x)$$
 כלומר,

י דוגמה: מ"ט זריזה, שבה מותר גם לזוז שני צעדים לכל כיוון ולא רק אחד. (רעיון ϵ ההוכחה: כיוון אחד בדיחה, בכיוון השני נוסיף מצבי q_R ו- q_L שבהם במסע מבצעים את התזוזה הנוספת).

תזת צ'רץ'-טיורינג

<u>התזה</u>: כל מודל כללי וסביר שקול למכונת טיורינג

- כללי = הכוונה למודל חזק לפחות כמו מכונת טיורינג.
 - סביר = הכוונה למודל שלא מכיל רכיבים אינסופיים.

<u>שאלה</u>: אבל למכונת טיורינג יש רכיב אינסופי – הסרט הוא אינסופי.

<u>אבחנה</u>: המשמעות מבחינתנו של הסרט האינסופי, היא רק שבמהלך הריצה של מכונת טיורינג לא יקרה מצב שחסר מקום אחסון. בפועל כל כמות של תווים שנוכל לכתוב על גבי הסרט היא תמיד <u>סופית</u>.

כלומר, אם נתייחס לאורך המילה כקבוע תמיד נשתמש באורך סרט סופי אבל לא חסום.

שינויים אפשריים

- מספר **קבוע** של סרטים אינסופיים. •
- הסרט יכול להיות אינסופי לשני הכיוונים.
- שינויים קלים בקבוצת הצעדים האפשריים. (כך שניתן לבצע את הצעדים המקוריים, ע"י שילוב כלשהו של הצעדים החדשים).
 - הוספת מספר **קבוע** של ראשים קוראים כותבים.
 - באופן כללי- שינויים שלא כוללים רכיב אינסופי.

מכונה מרובת סרטים

הגדרנו מודל יחיד של מכונת טיורינג. מודל נוסף הוא מכונה בעלת k סרטים $(k \geq 1)$.

- לכל סרט יש ראש קורא-כותב משלו •
- בתחילת הריצה הקלט רשום בסרט מספר 1, ושאר הסרטים ריקים (בלנק בכל הריבועים)
 - $\delta: Q' \times \Gamma^k \to Q \times \Gamma^k \times \{L,R,S\}^k \bullet$
- הפלט מוגדר להיות תוכן הסרט הראשון בזמן העצירה.

בתרגול יוכח שמודל בעל שני סרטים שקול למודל הרגיל שהגדרנו.

מודל אינסופי

מכונת טיורינג עם קבוצת מצבים אינסופית:

נגדיר מודל M^{*} הזהה למכונת טיורינג הרגילה, רק שקבוצת המצבים יכולה להיות <u>אינסופית</u>.

<u>טענה</u>: המודל <u>איננו שקול </u>למכונת טיורינג.

<u>הסבר</u>: כל פונקציה הינה בעצם רשימה אינסופית של מחרוזות. אזי, בהינתן פונקציה כלשהי, ניתן לשמור את כל המחרוזות המתאימות באינסוף המצבים הנתונים לנו.

דוגמה למודל אינסופי

```
Q = \{q_{\varepsilon}, q_{0}, q_{1}, q_{00}, q_{01}, q_{10}, q_{11}, q_{000}, q_{001}, \ldots\}
```

כל מצב כזה "זוכר" את הפלט המתאים לו, כאשר נקרא את המילה נוכל לעבור בין המצבים לפי המילה שקראנו. ולבסוף, כאשר נגיע לרווח הראשון, נדע שסיימנו לקרוא את המילה ונחזיר את הפלט שהמצב שהגענו אליו זוכר. (נחזור לתחילת הסרט ונכתוב את הפלט המתאים)

• תרגיל: השלימו את הפרטים.

מכונת טיורינג זריזה

מכונה זו מוגדרת בדומה למכונת טיורינג רגילה, רק שאפשר לבצע בה גם שני צעדים ימינה ושני צעדים שמאלה.

> כלומר, פונקציית המעברים נראית כך: גער מים אינו אינו

$$\delta: (Q \setminus F) \times \Gamma \to Q \times \Gamma \times \{LL, L, S, R, RR\}$$

<u>טענה</u>: מודל מכונת טיורינג זריזה שקול למודל מכונת טיורינג רגילה (זו שהגדרנו).

<u>רעיון ההוכחה</u>: כפי שהסברנו, על מנת להוכיח שקילות מודלים, ניקח מכונה הפועלת במודל אחד ונראה מכונה שקולה לה במודל השני, ולהיפך.

כיוון ראשון:

תהי M מ"ט רגילה. נבנה מ"ט זריזה 'M שתחשב את אותה הפונקציה ש-M מחשבת.

נשים לב ש-M מתאימה למודל של מ"ט זריזה, פשוט לא משתמשת LL-ו RR ו-LL, על כן נוכל לבחור M'=M.

כיוון שני:

תהי M מ"ט זריזה, נבנה מ"ט 'M מהמודל הרגיל, שתחשב את אותה הפונקציה ש-M מחשבת.

$$M' = (Q', q_0', F', \Gamma', \Sigma', \overline{b}', \delta')$$

את רוב הרכיבים אין לנו צורך לשנות, לכן

$$q_0' \coloneqq q_0 \qquad F' \coloneqq F \qquad \Gamma' \coloneqq \Gamma \qquad \Sigma' \coloneqq \Sigma \qquad \overline{b}' \coloneqq \overline{b}$$

המשך 1 כיוון שני:

המוטיבציה שלנו היא 'לזכור' כשהמכונה M רוצה לזוז שני צעדים באותו כיוון, ותיישם זאת.

נגדיר אם כך:

$$Q' \coloneqq Q \cup Q_L \cup Q_R$$

$$Q_L \coloneqq \{q_{iL} \mid q_i \in Q\}$$

$$Q_R \coloneqq \{q_{iR} \mid q_i \in Q\}$$

עבור δ' בכל פעם ש- δ משתמשת ב- L, R, S עבור $\delta'(q,a)\coloneqq\delta(q,a)$

המשך 2 כיוון שני:

,LL או RR-כאשר δ משתמשת

$$\delta(q, a) = (q_i, b_i, LL) \Rightarrow \delta'(q_i, a) = (q_{iL}, b_i, L)$$

$$\delta(q, a) = (q_i, b_i, RR) \Rightarrow \delta'(q_i, a) = (q_{iR}, b_i, R)$$

וכך 'נזכור' הזזה נוספת שיש לנו להשלים.

:ההשלמה תעשה כך: לכל q_i ולכל a נבצע

$$\delta'(q_{iL}, a) = (q_i, a, L)$$

$$\delta'(q_{iR},a) = (q_i,a,R)$$

תרגיל לבית

תהי מ"ט בעלת כיווני הצעדים הבאים:

{S, Right, Reset}

.1 כאשר Reset הינו לחזור לתא

?האם מ"ט זו שקולה למכונה רגילה

הכוונה: כדי להפריך, מספיקה שפה אחת שניתן להכריע בעזרת אחת מהן ולא בעזרת השנייה. כדי להוכיח, יש להראות איך מבצעים Left במודל החדש.