

סיבוכיות

ארזים ©

1 במרץ 2016

1 ביורוקרטיה

מרצה: אמיר בנבנישתי שפילקה

מתרגלים: בן לי וולק דור מינצר

תרגילים: יש חובת הגשה. 15% ציון התרגילים לפי $n - 1$ התרגילים הטובים ביותר מתוך n . צריך לעבור את המבחן.

בוחן אמצע: לא חובה. בונס. כל מי שציונו גבוה מ-57 מקבל 4 נקודות נוספות לקורס. הבוחן ב-4.21.

2 הקדמה לקורס

2.1 מטרות הקורס

1. להבין את כמות המשאבים הנדרשות כדי לפתור בעיות חישוביות. (זמן חישוב, זיכרון, אקראיות).

2. להבין את הקשרים בין המשאבים השונים.

2.2 דוגמה לשאלות

1. כמה מהר ניתן לפתור מערכת משוואות לינארית ב- n משתנים? כמה זיכרון צריך?

2. מה יותר קשה? חיבור או כפל? כמעט אותו הדבר. ה

3. אם אקראיות באמת עוזרת?

4. האם יש אלגוריתם יעיל למצוא הוכחות לטענות מתמטיות נכונות?

5. איך בודקים באופן יעיל האם למישהו יש כח חישוב גדול משלנו?

6. מה הכח של מחשבים קוונטים? (אם וכאשר)

7. האם הטבע פותר שאלות קשות?

8. מה זה אומר "ללמוד"? "לדעת"? מהי "בטיחות"?

9. מה זה חישוב?

עבורינו, לשאלה האחרונה נתנו תשובה ב"מודלים חישוביים" - מכונות טיורינג. למה דווקא מכונות טיורינג?

• זה מודל פשוט.

• זה מודל פורמאלי.

• הוא מאפשר יותר בקלות לחקור שאלות סיבוכיות בלי להסתבך בפרטים.

בקורס נתעניין בשאלות אסימפטוטיות כאשר אורך הקלט הולך וגדל.

סימונים: בדרך כלל מחשוב על קלט $x \in \{0, 1\}^*$ ונסמן ב- $|x|$ את האורך של x . לעתים נדבר על קלטים ב- $2^{\{0,1\}^*}$. נסמן את המחרוזת הריקה ב- ε .

2.3 בעיות חישוב:

2.3.1 בעיית חיפוש

יהי $R \subseteq \{0, 1\}^* \times \{0, 1\}^*$ יחס. נסמן $R(x) = \{y \in \{0, 1\}^* \mid (x, y) \in R\}$. הפונקציה $f : \{0, 1\}^* \rightarrow \{0, 1\}^* \cup \{\perp\}$ פותרת את בעיית החיפוש עבור אם לכל $x \in \{0, 1\}^*$ מתקיים $f(x) \in R(x)$ אם $R(x) \neq \emptyset$ אזי $f(x) = \perp$.

דוגמה: $R = \{(\bar{A}, b), \bar{y} : A\bar{y} = \bar{b}\}$

2.3.2 בעיית הכרעה

יהי $S \subseteq \{0, 1\}^*$. בהינתן x רותים לדעת האם $x \in S$. הפונקציה $f : \{0, 1\}^* \rightarrow \{0, 1\}$ פותרת את בעיית ההכרעה עבור S אם מתקיים $x \in S \Leftrightarrow f(x) = 1$.

2.4 מודל החישוב: מכונת טיורינג

מכונת טיורינג עם סרט אחד היא שביעה $\langle Q, \Sigma, \Gamma, \delta, q_0, q_a, q_r \rangle$, כאשר:

1. Q קבוצת מצבים
2. Σ א"ב קלט (ללא $\perp$)
3. $\Sigma \subset \Gamma$ (מכיל $\perp$)
4. $\delta : Q \times \Gamma \rightarrow Q \times \Gamma \times \{\leftarrow, \rightarrow, -\}$
5. q_0 מצב התחלתי $q_0 \in Q$
6. $q_r \in Q$: מצב דוחה.
7. $q_a \in Q$: מצב מקבל.

מוסכמה: אם רוצים לחשב פונקציה, נאמר שמה שכתוב על הסרט מימין לראש בסוף החישוב זו תוצאת החישוב.

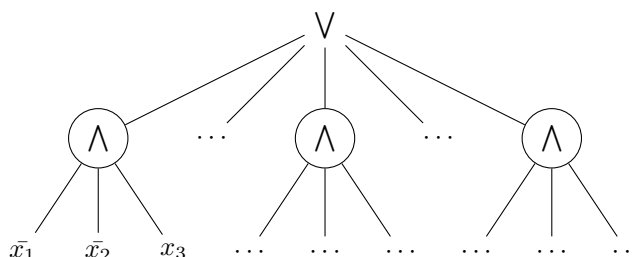
וריאנט: להוסיף סרט פלט *write-only*.

נאמר שמכונת טיורינג מקבלת קלט x אם עוצרת במצב q_a על x . דוחה אם עוצרת במצב q_r . $L(M) = \{x \mid M \text{ accepts } x\}$. מכונת טיורינג M מכריעה שפה A אם מקבלת כל $x \in A$ ודוחה כל $x \notin A$. ראינו שיש שפות שאי אפשר להכריע. (*HALT*) אפשר גם להסיק זאת משיקולי ספירה (מספר בן מניה של מכונות טיורינג ומספר לא בן מניה של שפות). מכונות טיורינג הן מודל חישוב יוניפורמי (*Uniform*). "אלגוריתם" שעובד לכל אורך קלט.

מודל לא יוניפורמי: תהי $A \subseteq \{0, 1\}^*$. נסמן A_n כל המחרוזות באורך בדייק n . נגדיר $f : \{0, 1\}^n \rightarrow \{0, 1\}$ על ידי $x \in A \iff f(x) = 1$ עבור בטבלה הבאה, דוגמה לחישוב של f_n

f	0	0	0	1	0	1	1	0
x_3	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1
x_1	0	0	0	0	1	1	1	1

טבלה 1: ערכי f_n

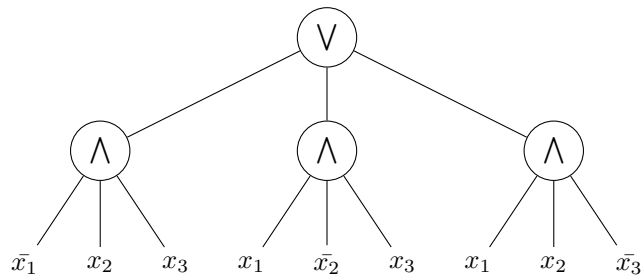


טבלה 2: חישוב f_n בצורת DNF

3 מעגלים בוליאניים

הגדרה 3.1) מעגל בולאני הוא גרף מכוון חסר מעגלים (DAG או גמ"ל) כל שער במעגל הוא:

1. אם דרגת כניסה $= 0$ השער הוא שער קלט, ומסומן על ידי אחד המשתנים.
2. אחרת, שער לוגי (AND, OR, NOT). דרגת כניסה של שער NOT היא 1 ושל $AND \setminus OR$ היא 2.
3. שער עם דרגת יציאה 0 נקרא שער פלט.

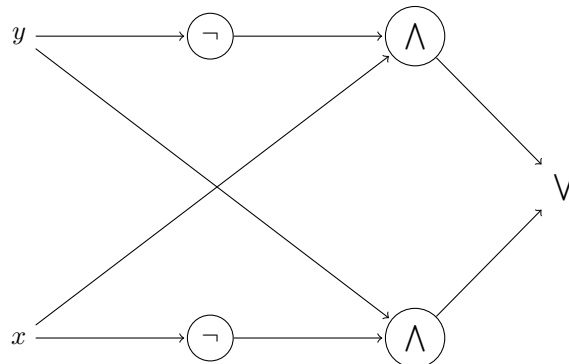


איור 1: דוגמה למעגל בולאני

3.1 חישוב

באופן טבעי, בהנתן קלט, a שער המסומן ב- x_i מחשב את a_i . כל שער לוגי מחשב את תוצאת הפעולה הלוגית על בניו. כמה סימונים:

- $fan - in$ דרגת כניסה.
- $fan - out$ דרגת יציאה.
- גודל מעגל = מספר שערים + מספר קשתות.
- עומק - אורכו של המסלול הארוך ביותר בגרף. (תמיד יוצא מקלט ומסתיים בפלט). אינטואיטיבית: הגודל מתאר את זמן החישוב. העומק את זמן החישוב המקסימלי.



איור 2: דוגמה למעגל, $x \oplus y$

הגדרה 3.2 נוסחה בולאנית היא מעגל בולאני שדרגת היציאה קטנה או שווה ל-1 בעל שער. (גרף החישוב הוא עץ).

נאמר כי משפחת מעגלים C_n , המעגל C_n על n משתנים, מכריעה שפה A מוכלת ב- $\{0,1\}^n$ אם לכל n המעגל C_n מחשב את A_n . זאת אומרת, עבור $x \in \{0,1\}^*$, מתקיים ש $x \in A_n \Leftrightarrow C_n(x) = 1$.

עובדה: לכל שפה יש משפחת מעגלים המחשבים אותה.

ראינו: לכל $f: \{0,1\}^n \rightarrow \{0,1\}$ יש מעגל בגודל $\mathcal{O}(n \cdot 2^n)$ המחשב אותה.

משפט 3.3 רוב הפונקציות הבולאניות על n משתנים, צריכות מעגל באורך $\Omega\left(\frac{2^n}{n}\right)$.

הוכחה: נספור את מספר המעגלים בגודל S : מספר השערים קטן או שווה ל- S . יש S^3 אפשרויות להחליט מה השערים $(\neg, \vee, \wedge)$. (מראש נתון שיש n קלטים). כמו כן, לכל שער יש $\binom{S}{2} \geq \binom{S}{2}$ אפשרויות לבחור את ילדיה, סה"כ: $\binom{S}{2}^S \Leftarrow$ מספר המעגלים קטן מ $3^S \cdot S^{2S}$ ומספר הפונקציות על n קלטים היא $2^n \rightarrow |\{0,1\}^n|$. ■