2/4/2017

הרצאה #3

בשיעור שעבר למדנו מושגים סמנטיים בסיסיים:

- מה ערך נוסחה φ בסביבה ρ. סימון: $[\![\varphi]\!]_\rho$

1) נוסחה ספיקה בסביבת ρ
2) נוסחה ספיקה
3) נוסחה טאוטולוגיה
4) נוסחה סתירה
5) נוסחאות שקולות
6) קבוצת נוסחאות ספיקה
7) נביעה סמנטית: נוסחה φ נובעת סמנטית מקבוצת נוסחאות Γ אם כל סביבה שמספקת Γ גם מספקת φ.

סימון: $\Gamma \models \varphi$. מקרה פרטי: $\emptyset \models \varphi$ אם"ם φ טאוטולוגיה.

אלגוריתמים:

Evaluation Problem:

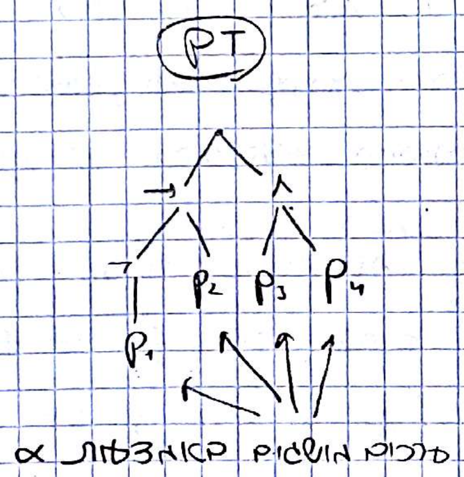
קלט: נוסחה φ וערכי אמת לכל משתנים שמופיעים ב-φ.

$\alpha : Var_\varphi \longrightarrow \{T,F\}$ (לכל משתנה ב-φ ערך T או F)

פלט: ערך של φ בכל סביבה של המשתנים ב-φ נותנת אותו ערכים כמו α

משפט:

יש אלגוריתם (ליניארי) לבעיית Evaluation.



אלגוריתם לחישוב ספיקות

נעבור על ההצבות (הסופיות) השונות של α ונריץ את האלגוריתם שתואר לעיל. סה״כ זמן ריצה לאלגוריתם דטרמיניסטי: $O(n\cdot 2^n)$

אם ניתן לנחש את הנוסחה המספקת - אלגוריתם לא דטרמיניסטי - זמן הריצה הוא $O(n)$.

משפט:

יש אלגוריתם שבודק האם φ נובעת מקבוצה (סופית) Γ.

דוגמה:

$\{\varphi_1, \varphi_2, \varphi_3\} \models \varphi$ אמ״מ $(\varphi_1 \wedge \varphi_2 \wedge \varphi_3) \to \varphi$ טאוטולוגיה.

מטרות להמשך:

1) תחשיב הוכחות עבור לוגיקת פסוקים.

2) האם יש לנו "מספיק" קשרים לוגיים?

נזכר:

סמנטיקה של נוסחה φ: לכל נוסחה נתאים פונקציה מהצבות ל-$\{T,F\}$.

האם לכל פונקציה f מהצבות ל-$\{T,F\}$ יש נוסחה φ ש-f "מגדירה" ($f(g) = [\![\varphi]\!]_g$) לכל הצבה g.

דוגמה:

- $f(g) = T$ לכל g. ניתנת לביטוי על ידי כל טאוטולוגיה $(p \vee \neg p)$.
- $f(g) = T$ אמ״מ $g(p_i) = \begin{cases} T & \text{אם i זוגי} \\ F & \text{אם i אי-זוגי} \end{cases}$

φ נוסחה. לכן יש מספר סופי של משתנים שמופיעים ב-φ (Var_φ הנ״ל סופית) $[\![\varphi]\!]_{g_1} = [\![\varphi]\!]_{g_2}$ עבור כל g_1, g_2 שמתלכדים על Var_φ. ל-f אין תכונה כזאת.

הגדרה:

קבוצת משתנים Δ נקראת תומכה של f: הצבות $\to \{T,F\}$ אם עבור כל הצבות g_1 ו-g_2 שמתלכדים על Δ $f(g_1) = f(g_2)$

הגדרה:

ל-f יש תומכה סופית אם יש Δ סופית שהיא תומכה של f.

משפט:

לכל פונקציה שמוגדרת על ידי נוסחה יש תמיכה סופית.

שאלה:

האם יש מספיק קשרים כדי לבטא פונקציות עם תמיכה סופית?

או:

האם לכל f עם תמיכה סופית קיים φ כך שלכל ρ:

$$f(\rho) = [\![\varphi]\!]_\rho$$

משפט 1:

לכל פונקציה f עם תמיכה סופית יש נוסחה φ כך ש- $f = [\![\varphi]\!]$

הגדרה:

קבוצת הקשרים Σ נקראת שלמה פונקציונלית אם כל פונקציה עם תמיכה סופית ניתן לבטא על ידי נוסחה שמכילה רק הקשרים ב- Σ

משפט 2:

$\{\neg, \vee, \wedge\}$ שלמה פונקציונלית.

ברור ש- משפט 2 $\Longleftarrow$ משפט 1.

הוכחת משפט 2:

לכל פונקציה עם תמיכה סופית Δ "נרשום" טבלה:

ערך של f	משתנים ב- Δ
T	T T ... T
	T F ... T

אם $\Delta = \{p_1, p_2\}$

f עבור ההשמה הנתונה	p_2	p_1
f(עבור השמה)	T	T
$\vdots$	F	T
	T	F
	F	F

למה:

לכל טבלה "T" יש נוסחה שמגדירה אותה פונקציה כמו "T".

לכל סדרת ערכים סופית $\beta_1,\dots,\beta_n$ $\beta_i \in \{T,F\}$ יש נוסחה φ עם משתנים $p_1,\dots,p_n$ כך ש- $[\![\varphi]\!]_f = T$ אמ"מ $\forall i.\ f(p_i)=\beta_i$

דוגמה:

$$TFFT \leftrightarrow p_1 \wedge \neg p_2 \wedge \neg p_3 \wedge \neg p_4$$

לכל שורה שנותנת אמת בטבלת אמת נבנה נוסחה φ_i כמו (ואז נעשה דיסיונקציה על כל ה- φ_i הנ"ל.

בעצם הוכחנו משפט יותר חזק ממשפט 2. הוכחנו שלכל f עם תמונה סופית יש נוסחה מהצורה $\vee\wedge$(אטומים או שלילה שלהם).

לצורה זו קוראים Disjunctive Normal Form

מסקנה:

כל נוסחה שקולה לנוסחה ב- DNF.

הגדרה:

1) אטום - משתנה או שלילתו
2) דיסיונקציה של אטומים (ברור)
3) קוניונקציה של אטומים (ברור).

נוסחה ב- Disjunctive Normal Form אם היא דיסיונקציה של קוניונקציות של אטומים.

נוסחה ב- Conjunctive Normal Form (CNF) אם היא קוניונקציה של דיסיונקציות של .

משפט:

כל נוסחה שקולה לנוסחה ב- DNF (הוכחנו עכשיו)

משפט:

כל נוסחה שקולה לנוסחה ב- CNF

נקח φ , $\neg\varphi$ שקולה ל- DNF (מעל $\neg$) $\wedge\vee$ ולכן φ שקולה

ל- (מעל $\neg$) $\wedge\vee$ CNF $\longrightarrow$ (מעל $\neg$) $\vee\wedge\neg$

<u>משפט:</u>

יש אלגוריתם שלכל נוסחה בונה DNF שקולה.

האם $\{\neg,\wedge\}$ שלמה פונקציונלית? כן!

כי $p_1 \vee p_2$ שקול ל- $\neg(\neg p_1 \wedge \neg p_2)$

- כדי להוכיח ש- Γ אינה שלמה פונקציונלית צריך להביא דוגמא לפונקציה עם תמונה סופית שלא ניתן להביע באמצעות נוסחה.

<u>דוגמה:</u>

$\{\vee,\wedge\}$ אינה שלמה פונקציונלית. (לא ניתן להביע את $\neg p_1$ באמצעות קוניונקציה ודיסיונקציה.

- גם $\{\neg,\vee\}$ שלמה פונקציונלית. וגם $\{\neg,\rightarrow\}$ שלמה פונקציונלית.

<u>הערה:</u>

ההנחה חשובה שהנחנו - "יש רק שני ערכי אמת" - True, False.

לפיה קוראים לוגיקה קלאסית.

דוגמאות למקומות שבהם יש יותר מ-2 ערכי אמת: אינטליגנציה מלאכותית, שפות תכנות.

תורת ההוכחות:

מושגים בסיסיים

הגדרה:

מערכת הוכחה פורמלית מורכבת מ:

1) אלפבית
2) נוסחאות - חלק מהמחרוזות קרויים נוסחאות
3) אקסיומות - חלק מהנוסחאות נקראות אקסיומות
4) כללי היסק - כל כלל היסק הוא יחס על נוסחאות. כללים בינריים תלת מקומיים.

$$R\frac{a}{b} \qquad R(a,b) \qquad R\frac{a_1,a_2}{b} \qquad R(a_1,a_2,b)$$

הגדרה:

הוכחה של נוסחה A מקבוצת נוסחאות Γ במערכת הוכחה S היא:

סדרת נוסחאות $A_1,A_2,\dots,A_n$ כך ש:

1) $A_n \equiv A$
2) לכל i אחד המקרים מתקיים:
   א) A_i אקסיומה (של S)
   ב) A_i בקבוצה Γ
   ג) יש כלל היסק תלת מקומי $j,k<i$ כך ש:
   $$R\frac{A_j,A_k}{A_i}$$

סימון: $\Gamma \vdash_S A$: יש הוכחה של A מ-Γ ב-S.

$\vdash_S$ יחס יכיחות של S

הגדרה:

A משפט (של S) אם A ניתנת להוכחה מקבוצה ריקה.

דוגמה:

1) אלפבית $\{0,1\}$
2) נוסחאות - כל המחרוזות
3) אקסיומה $\{1\}$
4) כללי היסק $R\frac{a,b}{ab}$, $R\frac{a}{10a}$

האם 11 משפט? כן: דוגמה לסדרה שמוכיחה זאת:

$1, 11$ או $1, 1, 11$

אקסיומות   נובע מכלל היסק R_1

האם 0011 ניתנת להוכחה מהקבוצה $\{0, 00\}$? כן:

$00, 1, 001, 0011$

$00 \in \Gamma$ 1 אקסיומה 001 לפי כלל 1 מ-00 ו-1 0011 לפי כלל 1 מ-001 ו-1

<u>משפט:</u> (תכונות של יחס יכיחות)

א) <u>מונוטוניות:</u>

אם $\Gamma \vdash_S A$ ו- $\Gamma \subseteq \Delta$ אזי $\Delta \vdash_S A$

<u>הוכחת מונוטוניות:</u>

אם $A_1,\dots,A_n$ הוכחה של A מ-Γ אזי $A_1,\dots,A_n$ הוכחה של A מ-Δ.

ב) <u>טרנזיטיביות</u>

אם $\Gamma \vdash_S B$ ו- $\Gamma \cup \{B\} \vdash_S A$ אזי $\Gamma \vdash_S A$.

<u>הוכחה:</u>

אם $A_1,\dots,A_n$ הוכחה של B מ-Γ ו- $A'_1,\dots,A'_m$ הוכחה של A מ- $\Gamma \cup \{B\}$ אזי $A_1,\dots,A_n,A'_1,\dots,A'_m$ הוכחה של A מ-Γ

ג) <u>טרנזיטיביות כללית:</u>

אם $\Gamma \vdash_S B$ עבור כל $B \in \Delta$ ו- $\Gamma \cup \Delta \vdash_S A$ אזי $\Gamma \vdash_S A$

(ההוכחה דומה להוכחת הטרנזיטיביות).

3) <u>קומפקטיות:</u>

אם $\Gamma \vdash_S A$ אזי קיימת תת קבוצה סופית $\Delta \subseteq \Gamma$ כך ש- $\Delta \vdash_S A$

<u>הוכחה:</u>

אם $A_1,\dots,A_n$ הוכחה של A מ-Γ אזי בסדרה מופיעים מספר סופי של נוסחאות מ-Γ ונסמן נוסחאות אלו ב-Δ ונקבל $\Delta \vdash_S A$

תחשיב הילברט לתורת הפסוקים

HPC: Hilbert Propositional Calculus

1) אלפא בית: משתנים $p_1, \ldots, p_n, \ldots$, הקשרים $\rightarrow, \neg$, סימני $($, $)$.

2) נוסחאות: נוסחאות של תורת הפסוקים עם הקשרים $\rightarrow, \neg$.

3) אקסיומות (בהמשך)

4) כללי היסק (בהמשך)

משפט: (השלמות)

$\Gamma \vdash_{HPC} A$ אמ"ם $\Gamma \models A$

יתרונות ב-HPC - תחשיב "הסן" והוכחה קצרה של משפט השלמות
חסרונות - קשה למצוא הוכחות ב-HPC .

אקסיומות של HPC:

$$Ax1 \quad (A \rightarrow (B \rightarrow A))$$

$$Ax2 \quad ((A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)))$$

$$Ax3 \quad ((\neg B \rightarrow \neg A) \rightarrow ((\neg B \rightarrow A) \rightarrow B))$$

כלל היסק: MP :

$$\frac{A, \ A \rightarrow B}{B}$$

משפט: (נאותות - soundness)

אם $\Gamma \vdash_{HPC} A$ אזי $\Gamma \models A$

הוכחה: (באינדוקציה על אורך הוכחה ב-HPC).

בסיס: הוכחות באורך 1 . אם A הוכחה מ-Γ באורך 1 אזי
א) A אקסיומה
או ב) $A \in \Gamma$

קל לראות: $Ax1$, $Ax2$, $Ax3$ טאוטולוגיות. ולכן אם אנו במקרה
א) סיימנו. במקרה ב) - כל סביבה שמספקת כל נוסחה ב-Γ בהכרח
מספקת גם את A (כי $A \in \Gamma$)

מעבר: $n \to n+1$

נניח $A_1,...,A_{n+1}$ הוכחה מ-Γ. אזי יש כמה מקרים:

1) A_{n+1} אקסיומה

2) A_{n+1} ב-Γ

3) A_{n+1} מתקבלת לפי MP מנוסחאות A_i, A_j שקדמו לה.

טענה:

ל-A_i ול-A_j יש הוכחה באורך קטן או שווה ל-n לכן: $\Gamma \models A_i, \Gamma \models A_j$

במקרה כזה $A_i \equiv (A_j \to A_{n+1})$. ניקח סביבה ρ שמספקת את Γ.

לפי הנחת האינדוקציה ρ מספקת את A_i ו- A_j לכן ρ חייבת לספק גם את A_{n+1}.

הערה:

האקסיומות חייבות להיות טאוטולוגיות בשביל שמשפט השלמות יתקיים, $\phi \vdash_S A$