

לוגיקה למדעי המחשב - תרגול 3

שיעור שעבר דיברנו עם מערכת עם סמנטיקה, והשיעור נדבר עם אספקט אחר של מערכות. (בשיעור הבא נקשר ביניהם באמצעות משפט השלמות)

מערכת פורמלית (עבור שפה T) - מה יש לנו בה?
 - אקסיומות, קבוצה חלקית של פסוקים בשפה
 - כללי היסק, בדר"כ קבוצה סופית

נגדיר את מושג ההוכחה:

נגיד של- A יש הוכחה מ- T (תורה) אם ישנה סדרת הוכחה של A מ- T .
 סדרת הוכחה: סדרה סופית של פסוקים המסתיימת ב- A כך שכל אחד מהפסוקים בה הוא באחת מהצורות הבאות:

א. אקסיומה

ב. איבר של T

ג. מתקבל מקודמים ע"י כלל היסק

נגדיר עוד מושג - משפט:

A הוא משפט של המערכת אם הוא יכיח מהתורה הריקה. (זה כמעט כמו להגיד שהוא טאוטולוגיה, אך פה אין נו השמות ערכי אמת וכו', אז צריך הזהר בקישור, נעשה אותו יותר מאוחר)

עד כאן דיברנו באופן כללי מה זה מערכת פורמלית. יש אינסוף כאלה כמובן. אנחנו נעבוד בעיקר עם מערכת נוסח היברט (נקרא ה HPC), שהיא באה לדמות את הדברים שהם "נכונים" (באמת שיעור הבאה נראה שמה שיכיח במערכת הוא "נכון" ומה ש"נכון" הוא יכיח. לא כל מערכת חייבת להיות עם מערכת שקלולה סמנטית כמו שלזו יש. בכלל יש מערכת שאין להן סמנטיקה)

נזכר בהגדרה של מערכת נוסח הילברט:
 האקסיומות (לא כולן):

$$\begin{aligned} (I_1) \quad & A \rightarrow (B \rightarrow A) \\ (I_2) \quad & (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)) \\ (N_1) \quad & (A \rightarrow B) \rightarrow ((A \rightarrow \neg B) \rightarrow \neg A) \\ (N_2) \quad & \neg \neg A \rightarrow A \\ & \vdots \end{aligned}$$

(נזכר שבעצם יש לנו כאן אינסוף אקסיומות)

וכלל ההיסק היחיד שלנו:

$$MP: \frac{A \quad A \rightarrow B}{B}$$

עוד מערכת שהזכרנו, HPI, שהמערכת הפורמלית שלה היא בדיוק כמו HPC חוץ מהחלפת N2 באקסיומה:

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

HPI בעיקר לא מקבלת את חוק השלישי הנמנע, ואז הדבר הכי פשוט, הגדרת פונ' בצורה הבא:

$$F(x) = \begin{cases} 0 & x \neq 3 \\ 1 & x = 3 \end{cases}$$

לא קיים אצלם [הפכנו אותם לכת] (כי לאו דווקא x שווה 3 או לא שווה 3) המקבילה לזה שמסתירה נובע כ דבר ב- CPL, ב- HPC היא:

$$A, \neg A \vdash_{HPC} B$$

(ב- HPI אין את "התפוצצות" מהצורה הזו)

נוכיח זאת:

(קצת ארוך, אז עמוד הבא..)

- 1) $\neg A \rightarrow (\neg B \rightarrow \neg A)$ $[I_1]$
- 2) $\neg A$ $[הנחה]$
- 3) $\neg B \rightarrow \neg A$ $[1, 2, MP]$
- 4) $A \rightarrow (\neg B \rightarrow A)$ $[I_1]$
- 5) A $[הנחה]$
- 6) $\neg B \rightarrow A$ $[4, 5, MP]$
- 7) $(\neg B \rightarrow A) \rightarrow ((\neg B \rightarrow \neg A) \rightarrow \neg B)$ $[N_1]$
- 8) $(\neg B \rightarrow A) \rightarrow \neg B$ $[6, 7, MP]$
- 9) $\neg B$ $[8, 3, MP]$
- 10) $\neg B \rightarrow B$ $[N_2]$
- 11) B

תכונות של הוכחות במערכת:

1. רפלקסיביות: $T \vdash_{HPC} A \quad sk \quad A \in T$ (סדרת הוכחה באורך 1: A)

2. מונוטוניות: $T_2 \vdash_{HPC} A \quad sk \quad T_1 \subseteq T_2 \rightarrow T_1 \vdash_{HPC} A$

(אותה סדרת הוכחה תעבוד גם ב- T_2)

3. טרמיטיביות: $T \vdash_{HPC} B$ אם $T \vdash_{HPC} A$ ו- $T \cup \{A\} \vdash_{HPC} B$ s/c

(למה זה נכון? נכתוב את ההוכחה עבור A בהתחלה ואז נוכל להשתמש בו)

[מה נובע משלושת התכונות עד כאן? שיחס היכיחות הזה הוא יחס נביעה!]

4 קומפקטיות:

$T' \vdash_{HPC} A$ - e כן $T' \subseteq T$ $\sim N''$ s/c $T \vdash_{HPC} A$

(את המשפט עבור CPL היה לא קל להוכיח [כל כך לא קל עד שעדיין לא הוכחנו אותו!], כאן המשפט הוא פשוט טריוויאלי - חישבו איך להוכיח אותו!)

טענה

נניח כי לכל $A \in T_1$ מתקיים $T_2 \vdash_{HPC} A$.

הוכח כי לכל B אם $T_1 \vdash_{HPC} B$ אז $T_2 \vdash_{HPC} B$.

הוכחה

יהי B פסוק כך שהוא: $T_1 \vdash_{HPC} B$.

לכן קיימת סדרה $B_1, \dots, B_n$ שהיא סדרת הוכחה של B.

נעבור על הסדרה הנ"ל אחד אחד לפי הסדר.

- אם B_i אקסיומה של HPC - נשאיר אותו.

- אם B_i שייך ל- T_1 אז $T_2 \vdash_{HPC} B_i$ ולכן נוכל להחליפו בסדרת ההוכחה שלו מ- T_1 ל- T_2 .

- אם B_i מתקבל ע"י MP נשאיר אותו.

משפט הדדוקציה

$$T, A \vdash_{HP\subseteq} B \iff T \vdash_{HP\subseteq} A \rightarrow B$$

(הוא יאפשר לנו להוכיח דברים כשיש לי יותר הנחות - ולכן יהיה יותר קל)

תרגיל
נוכיח כי:

$$A \rightarrow B \vdash_{HP\subseteq} \neg B \rightarrow \neg A$$

על פי משפט הדדוקציה מספיק להוכיח כי:

$$A \rightarrow B, \neg B \vdash_{HP\subseteq} \neg A$$

כעת, זה הרבה יותר פשוט, וההוכחה:

1) $\neg B \rightarrow (A \rightarrow \neg B)$	[I1]
2) $\neg B$	[הנחה]
3) $A \rightarrow \neg B$	[MP, 1, 2]
4) $A \rightarrow B$	[הנחה]
5) $(A \rightarrow B) \rightarrow ((A \rightarrow \neg B) \rightarrow \neg A)$	[N1]
6) $(A \rightarrow \neg B) \rightarrow \neg A$	[MP, 4, 5]
7) $\neg A$	[MP, 3, 6]

תרגיל

נגדיר מערכת חדשה HPC' על ידי כך שנחליף את N1 ו-N2 ב-N:

$$(N) \quad ({}^{\gamma}A \rightarrow {}^{\gamma}B) \rightarrow (({}^{\gamma}A \rightarrow B) \rightarrow A)$$

הוכח כי HPC שקולה ל-HPC'.
מה זה אומר להוכיח שקילות בין מערכות? מה שיכיח כאן יכיח גם שם והיפך.

על מנת להוכיח זאת, נראה ש:

$$\frac{}{HPC'} (N_2), \frac{}{HPC'} (N_1), \frac{}{HPC} (N)$$

הערה:

כשאנו מחליפים מערכת, לא מתחייב שהדברים שהתקיימו קודם יתקיימו גם עכשיו. לכן צריך לשים לב שב-HPC' מתקיים משפט הדדוקציה (כי היא הסתכמה רק על דברים שבכל מקרה קיימים ב-HPC' - ראו שיעור). כלומר צריך לשים לב ולא אוטומטית להניח שמשפט הדדוקציה מתקיים שם.

הערה 2:

נשים לב ש-

$$\frac{}{HPC/HPC'} A \rightarrow A$$

(כלומר בשתייהן זה קורה, לא ב-HPC מודולו HPC')

נתחיל עם להראות:

$$\frac{}{HPC'} {}^{\gamma}A \rightarrow A$$

זה הוא N2 ב-HPC, ואנו מראים שב-HPC' זה משפט.
על פי משפט הדדוקציה:

$${}^{\gamma}A \mid \frac{}{HPC'} A \Leftrightarrow \frac{}{HPC'} {}^{\gamma}A \rightarrow A$$

וכעת להוכחה:

1) $A \rightarrow (A \rightarrow A)$

2) A

3) $A \rightarrow A$

4) $(A \rightarrow (A \rightarrow A)) \rightarrow ((A \rightarrow A) \rightarrow A)$

5) $(A \rightarrow A) \rightarrow A$

6) $A \rightarrow A$

7) A

Σ_1

גורם

N

3, 4, 5, 6

[זר, נעשה 2, 5, 6]
[HPC]

(את שתי ההוכחות באחרות נשאיר כתרגיל)

טענה

אם $T \vdash_{HPC} A$ אז $T \{B_i\}_\rho \vdash_{HPC} A \{B_i\}_\rho$

הוכחה

לכן ישנה סדרת הוכחה ש-A מ-T: $A_1, \dots, A_n$

נוכיח כי $T \{B_i\}_\rho \vdash_{HPC} A \{B_i\}_\rho$ באינדוקציה על אורך ההוכחה. (בניגוד לאינדוקציה מבנית, במקרה זה לא נעשה משהו דומה, אלא הוכחה "כמו בתיכון")

בסיס:

נניח את הטענה עבור $n < k$ ונוכיח עבור n :

כי האקסיומה שלנו הן (הגיוניות, ניימן, זהויות, כהן)

$n=1$: אלא A-אקסיומה $A \{B_i\}_\rho \Leftarrow A \{B_i\}_\rho$ אקסיומה ולכן יכ'ח.

אלא $A \in T$ - $A \{B_i\}_\rho \Leftarrow A \{B_i\}_\rho \in T \{B_i\}_\rho$ ולכן יכ'ח.

מעבר:

- (1) אם A_n אקסיומה - כן קורא
 (2) אם $A_n \in T$ - כן קורא

(3) אם A_n מתקבל $A_j \rightarrow A_i$ ו- A_j אכן $A_k = A_j \rightarrow A_i$ עבור $j, k < n$

ע"פ MP A_k, A_j מתקבל אכן A_k גזירי/קונקלודי וכן

$$A_j \{B_p\} \rightarrow A_k \{B_p\} \text{ יכילול } \neg \{B_p\} T$$

כל הוכחה שלט מעטים:

$$\begin{array}{l} \text{סדר הוכחה } \neg \{B_p\} T \\ \left\{ \begin{array}{l} \vdots \\ A_j \{B_p\} \end{array} \right. \quad (*) \\ // \quad \left\{ \begin{array}{l} \vdots \\ (A_j \rightarrow A_n) \{B_p\} = A_j \{B_p\} \rightarrow A_n \{B_p\} \quad (***) \end{array} \right. \end{array}$$

$$MP \{ A_n \{B_p\} \} \text{ ו- } (***) \rightarrow (**)$$