לוגיקה למדעי המחשב - הרצאה 2

ביסוס השימוש בטבלאות האמת

בדוגמאות (בסוף ההרצאה הראשונה) השתמשנו בטבלאות שמאפשרות לנו לבדוק האם כל השמה שמספקת קבוצת פסוקים מספקת גם פסוק נוסף. נשאלת השאלה - האם אכן בדקנו את כל ההשמות האפשריות? כמובן שלא, שהרי השמה נותנת ערך אמת לכל אחד מהפסוקים האטומיים $p_1, p_2, \ldots$ (ולא רק לאלו שמופיעים בפסוקים הרלוונטיים), כלומר ישנן אינסוף ($2^{\aleph_0} = \aleph$) השמות אפשריות. נוכיח אם כן, טענה שמבססת את השימוש בטבלאות הנ"ל:

<u>טענה</u>: אם v, v' השמות כך ש- $v'(p) = v(p)$ לכל פסוק אטומי המופיע בנוסחא φ אז $v'(\varphi) = v(\varphi)$.

לשם הוכחת הטענה נצטרך קודם להגדיר בצורה פורמלית מה הכוונה במילה "מופיע" בטענה:

<u>הגדרה</u>: קבוצת הנוסחאות האטומיות בנוסחא φ (מסמנים $At(\varphi)$) מוגדרת ברקורסיה כנ"ל:

- $At(p) = \{p\}$ (p פסוק אטומי)
- $At(\neg\varphi) = At(\varphi)$
- $At(\varphi \diamond \psi) = At(\varphi) \cup At(\psi)$ כאשר $\diamond \in \{\wedge, \vee, \rightarrow\}$

נגדיר גם את קבוצת תת-הנוסחאות של φ ($Sf(\varphi)$) למרות שאין צורך בזה לשם הוכחת טענה זו:

- $Sf(p) = \{p\}$ (p פסוק אטומי)
- $Sf(\neg\varphi) = Sf(\varphi) \cup \{\neg\varphi\}$
- $Sf(\varphi \diamond \psi) = Sf(\varphi) \cup Sf(\psi) \cup \{\varphi \diamond \psi\}$ כאשר $\diamond \in \{\wedge, \vee, \rightarrow\}$

<u>הוכחה</u>: באינדוקציה על מבנה φ:

- בסיס האינדוקציה: אם $\varphi = p$ כאשר p פסוק אטומי אז $p \in At(\varphi)$ (למעשה $At(\varphi) = \{p\}$), לכן מהנתון על v, v': $v'(p) = v(p)$, כלומר $v'(\varphi) = v(\varphi)$ (שהרי $\varphi = p$).
- הנחת האינדוקציה: אם ψ פסוק קצר מ-φ ו-v, v' שתי השמות המקיימות $v'(p) = v(p)$ לכל $p \in At(\psi)$ אז $v'(\psi) = v(\psi)$.
- מעבר האינדוקציה:

1. $\varphi = \neg\psi$. נניח כי $v'(p) = v(p)$ לכל $p \in At(\varphi)$. אבל $At(\varphi) = At(\psi)$ ולכן מתקיים גם $v'(p) = v(p)$ לכל $p \in At(\psi)$. לכן, מהנחת האינדוקציה, $v'(\psi) = v(\psi)$. סה"כ:

$$v'(\varphi) = v'(\neg\psi) = \neg(v'(\psi)) = \neg(v(\psi)) = v(\neg\psi) = v(\varphi)$$

נפרט כל מעבר:

(א) $v'(\varphi) = v'(\neg\psi)$ פשוט מכיוון ש- $\varphi = \neg\psi$.
(ב) $v'(\neg\psi) = \neg(v'(\psi))$ לפי תכונות של השמה (להזכר מה המשמעות של $\neg$ בכל צד של השוויון).
(ג) $\neg(v'(\psi)) = \neg(v(\psi))$ שהרי, מהנחת האינדוקציה, כפי שהראנו, $v'(\psi) = v(\psi)$.
(ד) $\neg(v(\psi)) = v(\neg\psi)$ שוב לפי תכונות של השמה.
(ה) $v(\neg\psi) = v(\varphi)$ שוב מכיוון ש- $\varphi = \neg\psi$.

2. $\varphi = \psi_1 \diamond \psi_2$ כאשר $\diamond \in \{\wedge, \vee, \rightarrow\}$. נניח כי $v'(p) = v(p)$ לכל $p \in At(\varphi)$. מכיוון ש-$At(\psi_i) \subseteq At(\varphi)$, מתקיים גם $v'(p) = v(p)$ לכל $p \in At(\psi_i)$, ואז, לפי הנחת האינדוקציה, $v'(\psi_i) = v(\psi_i)$ ($i \in \{1, 2\}$). לכן:

$$v'(\varphi) = v'(\psi_1 \diamond \psi_2) = \diamond(v'(\psi_1), v'(\psi_2)) = \diamond(v(\psi_1), v(\psi_2)) = v(\psi_1 \diamond \psi_2) = v(\varphi)$$

שאלות עיקריות

1. נתונה תורה T. האם יש לה מודל (בניסוח טכני: האם T ספיקה), כלומר האם קיימת השמה v כך ש-$v \models T$?
2. נתונה תורה T ונוסחא φ. האם $T \vdash_{CPL} \varphi$?

כאשר התורה T סופית אז שאלות אלו הן <u>כריעות</u> כלומר יש לנו אלגוריתם שנותן להם תשובה (ובמקרה של תשובה חיובית אפילו נותן מודל של T). רדוקציות אפשריות של השאלה השניה:

- $T \vdash_{CPL} \varphi$ אמ"ם $T \cup \{\neg\varphi\}$ אינה ספיקה.
- לתורות סופיות - $\{\psi_1, \psi_2, \ldots, \psi_n\} \vdash_{CPL} \varphi$ אמ"ם הפסוק $(\psi_1 \wedge \psi_2 \wedge \ldots \wedge \psi_n) \rightarrow \varphi$ הינו טאוטולוגיה (כלומר כל השמה מספקת אותו).

תשובה לשאלות אלו נותן משפט הקומפקטיות.

משפט הקומפקטיות

1. T ספיקה אמ"ם כל קבוצה סופית חלקית שלה היא ספיקה.
2. $T \vdash_{CPL} \varphi$ אמ"ם יש $\Gamma \subseteq T$ סופית כך ש- $\Gamma \vdash_{CPL} \varphi$.

הבטחה: הוכחה תגיע בהמשך.

הגדרת יחס הנביעה בצורה סינקטית - HPC (מערכת נוסח הילברט לתחשיב הפסוקים)

קישור wikipedia: http://en.wikipedia.org/wiki/Proof_theory

אקסיומות

I1. $A \to (B \to C)$
I2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
N1. $(A \to B) \to ((A \to \neg B) \to \neg A)$
N2. $\neg\neg A \to A$
C1. $(A \wedge B) \to A$
C2. $(A \wedge B) \to B$
C3. $A \to (B \to (A \wedge B))$
D1. $A \to (A \vee B)$
D2. $B \to (A \vee B)$
D3. $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$

כלל היסק (קישור **wikipedia**: http://en.wikipedia.org/wiki/Modus_ponens)

$$\frac{A \quad A\to B}{B} \qquad \text{(MP)}$$

<u>הערה</u>: יש לשים לב שאלו למעשה לא אקסיומות אלא תבניות ליצירת אקסיומות. כדי "לייצר" אקסיומה, יש להציב פסוקים כלשהם במקום A, B, C.

<u>הגדרה</u>: הוכחה של פסוק φ מתורה T ב-HPC היא סדרה סופית של פסוקים ש-

- הפסוק האחרון בסדרה הוא φ.
- כל איבר בסדרה הוא אקסיומה של HPC, איבר של T או פסוק שמתקבל משני פסוקים קודמים לו בסדרה בעזרת כלל ההיסק MP.

<u>דוגמא</u>: הוכחה של $p \to p$ מהקבוצה הריקה.

1.	$p \to ((p \to p) \to p)$	מ־I1
2.	$(p \to ((p \to p) \to p)) \to ((p \to (p \to p)) \to (p \to p))$	מ־I2
3.	$(p \to (p \to p)) \to (p \to p)$	מ־1,2 לפי MP
4.	$p \to (p \to p)$	מ־I1
5.	$p \to p$	מ־3,4 לפי MP

<u>הגדרה</u>: $T \vdash_{HPC} \varphi$ אם יש ל-φ הוכחה מ-T.

<u>תרגיל</u>: להוכיח ש-$\vdash_{HPC}$ הוא יחס נביעה.

<u>טענה</u>: $T \vdash_{HPC} \varphi$ אמ"ם קיימת $\Gamma \subseteq T$ סופית כך ש- $\Gamma \vdash_{HPC} \varphi$.

<u>הוכחה</u>: שלא כמו במקרה של $\vdash_{CPL}$ (משפט הקומפקטיות), ההוכחה כאן טריוויאלית.

- נניח $T \vdash_{HPC} \varphi$. אזי מהגדרה, קיימת סדרה סופית של פסוקים שהם הוכחה של φ מ-T. תהי Γ קבוצת איברי הסדרה שהם איברי T. מכיוון שהסדרה סופית, גם Γ סופית וברור כי אותה סדרה של פסוקים מהווה הוכחה של φ מ-Γ, כלומר $\Gamma \vdash_{HPC} \varphi$.
- נניח קיימת $\Gamma \subseteq T$ סופית כך ש- $\Gamma \vdash_{HPC} \varphi$. אזי קיימת סדרה של פסוקים שהם הוכחה של φ מ-Γ. אבל מכיוון ש-$\Gamma \subseteq T$, סדרה זו מהווה גם הוכחה של φ מ-T, כלומר $T \vdash_{HPC} \varphi$.

משפט הנאותות והשלמות

$$\vdash_{CPL} \quad = \quad \vdash_{HPC}$$

כלומר: הגדרת יחס הנביעה של תחשיב הפסוקים בצורה סמנטית שקולה להגדרתו הסינטקטית.

ההוכחה מתחלקת לשני חלקים:

1. **נאותות** (soundness): $T \vdash_{\mathbf{HPC}} \varphi \quad \Rightarrow \quad T \vdash_{\mathbf{CPL}} \varphi$
2. **שלמות** (completeness): $T \vdash_{\mathbf{CPL}} \varphi \quad \Rightarrow \quad T \vdash_{\mathbf{HPC}} \varphi$

לשם הוכחת הנאותות נגדיר קודם הצבה ונוכיח את משפט ההצבה, שבעזרתו נוכל לטעון כי כל אקסיומה היא טאוטולוגיה.

<u>הגדרה</u>: תהי φ נוסחא, p פסוק אטומי ו-A נוסחא כלשהי. $\varphi\{A/p\}$ (הפסוק המתקבל מ-φ ע"י הצבת A במקום p) מוגדר באופן הבא:

$$\varphi\{A/p\} \quad = \quad \begin{cases} A & \varphi = p \\ \varphi & \varphi = q,\ q \neq p \\ \neg\psi\{A/p\} & \varphi = \neg\psi \\ \psi_1\{A/p\} \diamond \psi_2\{A/p\} & \varphi = \psi_1 \diamond \psi_2,\ \diamond \in \{\wedge, \vee, \rightarrow\} \end{cases}$$

באופן דומה מגדירים הצבה סימולטנית: $\varphi\{A_1/p_1, \ldots, A_n/p_n\}$. חשוב לציין שההצבה סימולטנית, כי הצבה לפי הסדר תיתן תוצאה שונה (למשל אם מציבים A_1 במקום p_1 ואז A_2 במקום p_2 כאשר p_2 הוא אחד הפסוקים האטומיים ב-A_1).

משפט ההצבה

יהיו φ נוסחא, v השמה, $q_1, \ldots, q_n$ נוסחאות אטומיות שונות זו מזו ו-$A_1, \ldots, A_n$ נוסחאות (לא בהכרח שונות זו מזו). תהי v' השמה המוגדרת באופן הבא:

$$v'(p) \quad = \quad \begin{cases} v(A_i) & p = q_i \text{ (ok because } i \neq j \Rightarrow q_i \neq q_j) \\ v(p) & \text{otherwise} \end{cases}$$

אזי $v'(\varphi) = v(\varphi\{A_1/p_1, \ldots, A_n/p_n\})$.

הוכחה בתרגיל בית.

משפט הנאותות של HPC

אם φ $T\vdash_{\mathbf{HPC}}$ אז $T\vdash_{_{CPL}}\varphi$. צריך להוכיח שאם ל-φ יש הוכחה מ-T אז כל מודל של T הוא גם מודל של φ.

<u>הוכחה</u>: נוכיח באינדוקציה על n, שאם $\varphi_1,\ldots,\varphi_n$ סדרת הוכחה מ-T ב-HPC אז כל מודל של T הוא גם מודל של φ_n.

יהי אז v מודל של T, נראה שהוא גם מודל של φ_n.

- בסיס האינדוקציה: $n=1$, כלומר ה"סדרה" φ_1 היא כבר הוכחה תקינה מ-T ב-HPC. ישנן שתי אפשרויות:
  - $\varphi_1\in T$ ואז ברור כי v הוא מודל של φ_1 כי v הינו מודל של כל איבר ב-T.
  - φ_1 אקסיומה של HPC. ע"י בדיקה של כל אחת מהסכימות אפשר לברר שכולן טאוטולוגיות (ליתר דיוק, האינסט-נציות שלהן טאוטולוגיות), ובפרט, $v\left(\varphi_1\right)=t$, כלומר $v\models\varphi_1$.
- הנחת האינדוקציה: לכל $i<n$ מתקיים שאם $\varphi_1,\ldots,\varphi_i$ סדרת הוכחה מ-T ב-HPC אז v מודל של φ_i.
- מעבר האינדוקציה: נראה כי אם $\varphi_1,\ldots,\varphi_n$ סדרת הוכחה מ-T ב-HPC אז v מודל של φ_n.
  מכיוון ש-φ_n מופיע בסדרת ההוכחה אז ישנן 3 אפשרויות:
  - $\varphi_n\in T$
  - φ_n אקסיומה של HPC
  - φ_n מתקבל משני איברים קודמים בסדרה, φ_i ו-φ_j $(i,j<n)$ ע"י MP.

  הטיפול בשתי האפשרויות הראשונות הוא בדיוק כמו במקרה $n=1$.
  במקרה השלישי: קיימים $i,j<n$ כך ש- $\varphi_j=\varphi_i\rightarrow\varphi_n$. מכיוון ש-$\varphi_1,\ldots,\varphi_i$ ו-$\varphi_1,\ldots,\varphi_j$ הוכחות מ-T ב-HPC שאורכן קטן מ-n, אז לפי הנחת האינדוקציה, v הינו מודל של φ_i ושל φ_j, דהיינו $v\left(\varphi_i\right)=t$ ו-t-$v\left(\varphi_j\right)=v\left(\varphi_i\rightarrow\varphi_n\right)=t$.
  לפי טבלת האמת של $\rightarrow$, יוצא מזה ש- $v\left(\varphi_n\right)=t$, כלומר $v\models\varphi_n$.

<u>וריאציה אחרת של הוכחת משפט הנאותות</u>:

נגדיר $Th_{_{HPC}}\left(T\right)$ (שזה בעצם $\{\varphi|T\vdash_{_{HPC}}\varphi\}$) ע"י:

- אם $\varphi\in T$ אז $\varphi\in Th_{_{HPC}}\left(T\right)$.
- אם φ אקסיומה של HPC אז $\varphi\in Th_{_{HPC}}\left(T\right)$.
- אם $\varphi\in Th_{_{HPC}}\left(T\right)$ ו- $\varphi\rightarrow\psi\in Th_{_{HPC}}\left(T\right)$ אז $\psi\in Th_{_{HPC}}\left(T\right)$.

ואז נוכיח באינדוקציה מבנית על ההגדרה הרקורסיבית הזו של $Th_{_{HPC}}\left(T\right)$, שאם $\varphi\in Th_{_{HPC}}\left(T\right)$ אז $T\vdash_{_{CPL}}\varphi$.