לוגיקה למדעי המחשב - הרצאה 10

מטרתנו כעת לענות בצורה אפקטיבית האם $T \vdash_{FOL} A$ כאשר T ו-A פסוקים. כזכור,

$$T \vdash^t_{FOL} A \quad \Leftrightarrow \quad T\{d_1/x_1, d_1/x_2, \ldots\} \vdash^t_{FOL} A\{d_1/x_1, d_1/x_2, \ldots\}$$

כאשר $x_1, x_2, \ldots$ הם המשתנים החופשיים ב-T ו-$d_1, d_2, \ldots$ קבועים חדשים שאינם מופעים ב-$T \cup \{A\}$. עבור v-נביעה,

$$T \vdash^v_{FOL} \quad \Leftrightarrow \quad \forall T \vdash^v_{FOL} \forall A$$

כאשר $\forall A$ הוא סגור של A ו-$\forall T$ היא קבוצת סגורים של כל איברי T. שקילויות אלו מאפשרות לעבור מנביעה עבור נוסחאות כלשהן לנביעה עבור פסוקים.

<u>טענה</u>: $T \vdash_{FOL} A$ אמ"ם $T \cup \{\neg A\}$ אינה ספיקה.

התכנית

1. רדוקציה של בעית ספיקות תורה של פסוקים כלשהם לבעית ספיקות תורה של פסוקים בצורה פרנקסית נורמלית. פסוק A הוא בצורה פרנקסית נורמלית אם $A = Q_1 x_1 Q_2 x_2 \ldots Q_n x_n . \psi$ עבור $Q_1, Q_2, \ldots, Q_n$ כמתים כלשהם ו-ψ נוסחא ללא כמתים.
2. רדוקציה של בעית ספיקות תורה של פסוקים בצורה פרנקסית נורמלית לבעית ספיקות של תורה של פסוקים אוני-ברסליים בעזרת סקולמיזציה. פסוק אוניברסלי הוא פסוק מהצורה $\forall x_1 \forall x_2 \ldots \forall x_n . \psi$ כאשר ב-ψ לא מופעים כמתים ו-$x_1, x_2, \ldots, x_n$ הם המשתנים החופשיים המופיעים ב-ψ.
3. משפט הרברנד - נותן רדוקציה מבעית ספיקות תורה T של פסוקים אוניברסליים ב-FOL לבעית ספיקות בתחשיב הפסוקים.

שלב 1 - צורה פרנקסית נורמלית

<u>משפט החלפת אקויולנטים</u>:

אם $T \vdash^v_{FOL} A \leftrightarrow A'$ ו-φ' התקבלה מ-φ ע"י החלפת מופע אחד או יותר של A ב-A' אז $T \vdash^v_{FOL} \varphi \leftrightarrow \varphi'$.
הוכחה - באינדוקציה על מבנה φ, כתרגיל.

<u>הערה</u>: המשפט אינו נכון עבור t-נביעה. לדוגמא, $(x = x) \leftrightarrow (x = 1) \vdash^t_{FOL} (x = x) \leftrightarrow (x = 1)$ אבל $(x = x) \leftrightarrow (x = 1) \not\vdash^t_{FOL} \forall x\,(x = x) \leftrightarrow \forall x\,(x = 1)$.

<u>מסקנה</u>: אם A ו-A' שקילויות לוגיות אז אפשר להחליף אחת בשניה בכל קונטקסט.

<u>שקילויות חשובות</u>:

(1) $\forall x A \equiv \neg \exists x \neg A \qquad \exists x A \equiv \neg \forall x \neg A \qquad \neg \exists x A \equiv \forall x \neg A \qquad \neg \forall x A \equiv \exists x \neg A$

(2) $\exists x \exists y A \equiv \exists y \exists x A \qquad \forall x \forall y A \equiv \forall y \forall x A$

(3) אם y אינו חופשי ב-A: $\exists y A \equiv A \qquad \forall y A \equiv A$

(4) אם x אינו חופשי ב-A אך חופשי להצבה במקום y ב-A (כלל α):
$\exists y A \equiv \exists x A\,(x/y) \qquad \forall y A \equiv \forall x A\,(x/y)$

(5) $\exists x\,(A \vee B) \equiv \exists x A \vee \exists x B \qquad \forall x\,(A \wedge B) \equiv \forall x A \wedge \forall x B$

(6) אם x אינו חופשי ב-A אז:

(i)	$\forall x\left(A\wedge B\right)\equiv A\wedge\forall xB$	$\exists x\left(A\wedge B\right)\equiv A\wedge\exists xB$
(ii)	$\forall x\left(A\vee B\right)\equiv A\vee\forall xB$	$\exists x\left(A\vee B\right)\equiv A\vee\exists xB$
(iii)	$\forall x\left(A\rightarrow B\right)\equiv A\rightarrow\forall xB$	$\exists x\left(A\rightarrow B\right)\equiv A\rightarrow\exists xB$
(iv)	$\forall x\left(B\rightarrow A\right)\equiv\left(\exists xB\right)\rightarrow A$	$\exists x\left(B\rightarrow A\right)\equiv\left(\forall xB\right)\rightarrow A$

<u>דוגמא</u>: אם p,q סימני יחס חד-מקומיים, אז:

$$(y\neq x)\qquad \forall x\left(q\left(x\right)\wedge\neg\forall x.p\left(x\right)\right)\equiv\forall x\left(q\left(x\right)\wedge\exists x.\neg p\left(x\right)\right)\equiv\forall x\left(q\left(x\right)\wedge\exists y.\neg p\left(y\right)\right)\equiv\forall x\exists y.q\left(x\right)\wedge\neg p\left(y\right)$$

הערה: בדוגמא זו ניתן להגיע גם ל-$\exists y\forall x.q\left(x\right)\wedge\neg p\left(y\right)$, בדרך אחרת.

שלב 2 - סקולמיזציה

משפט: תהי L שפה, T תורה של פסוקים ו-φ פסוק מהצורה $\forall x_1 \ldots \forall x_n \exists y.\psi$ (ψ יכול להכיל כמתים נוספים), אז $T \cup \{\varphi\}$ ספיקה כתורה בשפה L אמ"ם $T \cup \{\forall x_1 \ldots \forall x_n.\psi \{f(x_1, \ldots, x_n)/y\}\}$ ספיקה כתורה בשפה L^* המתקבלת מ-L ע"י הוספת סימן פונקציה n-מקומי חדש f.

סימון: בהנתן השמה v במבנה M, נסמן ב-$v(a/y)$ את ההשמה v' המוגדרת ע"י $v'[y] = a$ ו-$v'[x] = v[x]$ ($x \neq y$).

תזכורת:

1. $M \vDash \varphi \;\Rightarrow\; M \vDash \forall x_1 \ldots \forall x_n \varphi$
2. משפט ההצבה: אם t חופשי להצבה במקום x ב-φ ו-$a = v[t]$ אז $M, v \vDash \varphi\{t/x\} \;\Leftrightarrow\; M, v(a/x) \vDash \varphi$.

הוכחה:
כיוון א': אם $T \cup \{\forall x_1 \ldots \forall x_n.\psi\{f(x_1, \ldots, x_n)/y\}\}$ ספיקה כתורה בשפה L^* אז $T \cup \{\varphi\}$ ספיקה כתורה בשפה L.
הוכח כתרגיל.

כיוון ב': תהי $T \cup \{\varphi\}$ ספיקה ב-L. יהי M מודל כך ש-$M \vDash T \cup \{\varphi\}$ ב-L. אז $M \vDash \forall x_1 \ldots \forall x_n \exists y \psi$, כלומר לכל $\langle a_1, \ldots, a_n \rangle \in D^n$ קיים $a \in D$ כך שלכל השמה v שמקיימת $v[x_i] = a_i$ (לכל $1 \le i \le n$) מתקיים $M, v(a/y) \vDash \psi$. נגדיר אם כן פונקציה $G : D^n \to D$ שעבור כל $\langle a_1, \ldots, a_n \rangle \in D^n$ תחזיר $a \in D$ כלשהו כזה, ואז $M, v(G[v[x_1], \ldots, v[x_n]]/y) \vDash \psi$ לכל השמה v ב-M. נרחיב את M ל-M^* ע"י $I[f] = G$. ברור כעת כי לכל נוסחא A <u>בשפה L</u> אם $M, v \vDash A$ אז $M^*, v \vDash A$, מכיוון ש-f לא מופיע ב-A (השמה ב-M היא גם השמה ב-M^* ולהפך). לכן $M^*, v(G[v[x_1], \ldots, v[x_n]]/y) \vDash \psi$ לכל השמה v ב-M^*. אבל $v[f(x_1, \ldots, x_n)] = I[f][v[x_1], \ldots, v[x_n]] = G[v[x_1], \ldots, v[x_n]]$ ולפי משפט ההצבה $M^*, v \vDash \psi\{f(x_1, \ldots, x_n)/y\}$ לכל השמה v ב-M^*, כלומר $M^* \vDash \psi\{f(x_1, \ldots, x_n)/y\}$. לפי תזכורת 1 נקבל $M^* \vDash \forall x_1 \ldots \forall x_n.\psi\{f(x_1, \ldots, x_n)/y\}$. לשאר הפסוקים (ב-$T$) ברור כי M^* מספק אותם.

דוגמא: $\forall x_1 \forall x_2 \exists y \forall u \exists v.q(x_1, x_2, y, u, v)$ ספיקה אמ"ם $\forall x_1 \forall x_2 \forall u \exists v.q(x_1, x_2, h(x_1, x_2), u, v)$ ספיקה אמ"ם $\forall x_1 \forall x_2 \forall u.q(x_1, x_2, h(x_1, x_2), u, f(x_1, x_2, u))$ ספיקה.

הערות חשובות:

1. תהליך סילוק הכמתים הישיים (כמתי $\exists$) נקרא סקולמיזציה. הפסוק המתקבל ב-φ בתהליך זה מסומן ע"י $Sk(\varphi)$, והתורה המתקבלת מ-T - $Sk(T)$.
2. $Sk(\varphi)$ לא נקבע באופן יחיד ע"י φ אלא תלוי בבחירת סימני הפונקציה.
3. $Sk(\varphi)$ לא שקול ל-φ! הם אפילו לא באותה שפה.
4. כל מודל $\langle D, I \rangle$ של תורה T בשפה L עם סיגנטורה σ ניתן להרחיב למודל $\langle D, I^* \rangle$ של $Sk(T)$ ו-$I = I^*/\sigma$.
5. אם $\langle D, I^* \rangle$ מודל של $Sk(T)$ אז $\langle D, I^*/\sigma \rangle$ הוא מודל של T (בשפה L עם סיגנטורה σ).
6. סימני פונקציה שמכניסים בתהליך סקולמיזציה נקראים פונקציות סקולם (למרות שהם לא פונקציות אלא סימני פונקציה).

שלב 3 - משפט הרברנד

<u>הגדרה</u>: אינסטנציה של נוסחא φ היא נוסחא מהצורה $\varphi\{t_1/x_1,\ldots,t_n/x_n\}$ כאשר t_i חופשי להצבה במקום x_i ב-φ (לכל $1\le i\le n$). אינסטנציה סגורה: אינסטנציה שהיא פסוק.

<u>הגדרה</u>: אם $\psi=\forall x_1\ldots\forall x_n\varphi$ (וב-φ אין כמתים) אז φ היא המטריצה של ψ.

<u>משפט הרברנד</u>: תהי T תורה אוניברסלית בשפה L שיש בה קבוע אחד לפחות. אז T ספיקה כתורה ב-FOL אמ"ם T^*, קבוצת האינסטנציות הסגורות של המטריצות של איברי T, ספיקה כתורה ב-CPL (מסתכלים על נוסחאות אטומיות של FOL כעל פסוקים אטומיים ב-CPL). הערה: אם אין ב-L קבועים אז נגדיר את T^* כקבוצת האינסטנציות הסגורות של T בשפה $L^*=L\cup\{c\}$ ואז T ספיקה כתורה ב-L אמ"ם T ספיקה כתורה ב-L^* (להוכיח כתרגיל).

<u>טענה 1</u>: יהי M מבנה עבור שפה L. נגדיר השמה פסוקית v_M ע"י:

$$v_M\left[p\left(s_1,\ldots,s_n\right)\right] = \begin{cases} t & M\vDash p\left(s_1,\ldots,s_n\right) \\ f & M\nvDash p\left(s_1,\ldots,s_n\right) \end{cases}$$

אז לכל פסוק A ללא כמתים מתקיים $M\vDash A$ אמ"ם $v_M[A]=t$. הוכחה כתרגיל.

<u>טענה 2</u>: אם $M=\langle H(L),I\rangle$ מבנה הרברנד עבור שפה L ו-v השמה במבנה אז $M,v\vDash\forall x\varphi$ אמ"ם לכל ש"ס s מתקיים $M,v\vDash\varphi\{s/x\}$. מסקנה: אם $\forall x\varphi$ פסוק אז $M\vDash\forall x\varphi$ אמ"ם $M\vDash\varphi\{s/x\}$ לכל ש"ס s. הוכחה בתירגול.

<u>הוכחת משפט הרברנד</u>:

<u>כיוון א'</u>: $\forall x_1\ldots\forall x_n A\vdash_{FOL} A^*$ לכל אינסטנציה סגורה A^* של A. מכאן שכל מודל M של T הוא גם מודל של T^*. לפי טענה 1, v_M היא השמה פסוקית שמספקת את T^* במובן של CPL.

<u>כיוון ב'</u>: תהי T^* ספיקה במובן של CPL ותהי v השמה פסוקית כך ש-$v[\psi]=t$ לכל $\psi\in T^*$. יהי כמו כן $M=\langle H(L),I\rangle$ מבנה הרברנד עבור L כך ש-$p(s_1,\ldots,s_n)\in HB(M)$ אמ"ם $v[p(s_1,\ldots,s_n)]=t$ (כלומר $\langle s_1,\ldots,s_n\rangle\in I[p]$ אמ"ם $v[p(s_1,\ldots,s_n)]=t$). מטענה 1, $M\vDash\psi$ עבור כל $\psi\in T^*$, כלומר $M\vDash T^*$. נראה ש-$M\vDash T$. יהי $\varphi\in T$, אז $\varphi=\forall x_1\ldots\forall x_n A$ כאשר ב-A אין כמתים. ממסקנה של טענה 2, $M\vDash\varphi$ אמ"ם $M\vDash A^*$ לכל אינסטנציה סגורה A^* של A. אבל כל A^* הוא איבר ב-T^* ולכן $M\vDash A^*$. מכאן ש-$M\vDash\varphi$ במובן של FOL, ולכן $M\vDash T$ (במובן של FOL).