

לוגיקה למדמ"ח – שיעור 10

משפט ההצבה

$$M, v \models \varphi\left\{\frac{t}{x}\right\} \Leftrightarrow M, v\{x=v(t)\} \models \varphi$$

φ - נוסחא, x - משתנה, t - שם עצם חופשי להצבה במקום x ב- φ .

למת עזר

אם s, t ש"ע, x משתנה, v הצבה במבנה $M = \langle D, I \rangle$: $v' = v\{x=v(t)\}$. אז: $v'[s] = v\left\{\frac{t}{x}\right\}$.

הוכחת הלמה

באינדוקציה על מבנה s .

-אם $s=c$ (קבוע):

$$s\left\{\frac{t}{x}\right\} = s = c \Rightarrow v[c] = I[c], \quad v'[c] = I[c]$$

$$v'[s] = v\left\{\frac{t}{x}\right\} = I[c]$$

-אם $s=y$ (משתנה שונה מ- x):

$$s\left\{\frac{t}{x}\right\} = y\left\{\frac{t}{x}\right\} = y$$

$$v'[y] = v[y]$$

$$v\left\{\frac{t}{x}\right\} = v[y] = v'[y] = v'[s]$$

-אם $s=x$:

$$s\left\{\frac{t}{x}\right\} = x\left\{\frac{t}{x}\right\} = t$$

$$v\left\{\frac{t}{x}\right\} = v[t]$$

$$v'[s] = v'[x] = v[t]$$

לפי הגדרת v'

ולכן השוויון מתקיים

זה היה הבסיס (ש"ע הבסיסיים – קבועים ומשתנים). מעבר:

נניח $s = p(s_1, \dots, s_n)$ כאשר s הוא סימן פונקציה n-מקומי, $s_1, \dots, s_n$ ש"ע פשוטים יותר מ- s . כעת:

$$s\left\{\frac{t}{x}\right\} = f\left(s_1\left\{\frac{t}{x}\right\}, \dots, s_n\left\{\frac{t}{x}\right\}\right)$$

$$v\left[s\left\{\frac{t}{x}\right\}\right] = f^I\left[v\left[s_1\left\{\frac{t}{x}\right\}\right], \dots, v\left[s_n\left\{\frac{t}{x}\right\}\right]\right] = f^I\left[v'[s_1], \dots, v'[s_n]\right] = f^I[v'[s_1], \dots, v'[s_n]] = v'[s]$$

↑ הפירוש של f במטא שפה
↑ הפעלה במטא שפה
↑ ל.ה.א.

ובזה נגמרת הוכחת הלמה.

הוכחת המשפט

עכשיו עוברים לדבר העיקרי, עבור נוסחאות (ושוב זה יהיה דומה, נראה את זה בצורה אינד' על מבנה הנוסחא). באינדוקציה על מבנה φ .

1. נניח $\varphi = p(s_1, \dots, s_n)$ כאשר p סימן יחס n-מקומי.

$$\varphi\left\{\frac{t}{x}\right\} = p\left(s_1\left\{\frac{t}{x}\right\}, \dots, s_n\left\{\frac{t}{x}\right\}\right)$$

$$M, v \models \varphi\left\{\frac{t}{x}\right\} \Leftrightarrow \langle v[s_1\left\{\frac{t}{x}\right\}], \dots, v[s_n\left\{\frac{t}{x}\right\}] \rangle \in p^I \Leftrightarrow \langle v'[s_1], \dots, v'[s_n] \rangle \in p^I \Leftrightarrow$$

$$\Leftrightarrow M, v' \models p(s_1, \dots, s_n)$$

↑ הגדרת סיפוק
↑ סימן ל- $[I, p]$ זה במטא שפה הפירוש של p
↑ לפי למת העזר

נעבור לנוסחאות יותר מורכבות:

2. קשרים. צריך להוכיח עבור: $\varphi = \neg \psi$, $\varphi = \psi_1 \rightarrow \psi_2$, $\varphi = \psi_1 \wedge \psi_2$, $\varphi = \psi_1 \vee \psi_2$. אנחנו נראה רק עבור "או".

אז $\varphi = \psi_1 \vee \psi_2$. מתחיל בדיוק באותה צורה כמו בקודמים – נבדוק תחילה מה זה $\varphi\left\{\frac{t}{x}\right\}$ (שנראה על מה אנחנו מדברים בכלל):

$$\varphi\left\{\frac{t}{x}\right\} = \psi_1\left\{\frac{t}{x}\right\} \vee \psi_2\left\{\frac{t}{x}\right\}$$

כעת:

$$\begin{aligned}
 M, v \models \varphi\left\{\frac{t}{x}\right\} &\Leftrightarrow M, v \models \psi_1\left\{\frac{t}{x}\right\} \vee \psi_2\left\{\frac{t}{x}\right\} \Leftrightarrow^* M, v \models \psi_1\left\{\frac{t}{x}\right\} \text{ ו } M, v \models \psi_2\left\{\frac{t}{x}\right\} \Leftrightarrow \\
 &\Leftrightarrow M, v' \models \psi_1 \text{ ו } M, v' \models \psi_2 \Leftrightarrow M, v' \models \psi_1 \vee \psi_2
 \end{aligned}$$

* (זו שליד אחד ה-) $\Leftrightarrow$ בשרשרת המעברים הקודמים):
שימו לב! זה קצת קל מדי לעשות את המעבר הזה (כלומר עשינו אותו בלי ממש לחשוב הרבה) אבל ניתן לעשות אותו רק כאשר מדובר בנכונות (כאשר יש לנו גם M וגם v). בתקפות זה לא נכון (דיברנו על זה בשיעור שעבר).

3. כעת ניגשים למקרה היותר מסובך, המקרה ש- φ מתקבלת בעזרת כימות. כאן יהיה קשה לעשות את זה על ידי שרשרת של $\Leftrightarrow$ (למרות ששני הכיוונים דומים מאוד). אנחנו נעשה כאן כיוון אחד (והשני – כתרגיל). כמו כן, נעשה רק עבור $\varphi = \forall y \psi$.

i. אפשרות א': x לא חופשי ב- φ (יכול להיות כי $y=x$ או שהוא לא חופשי ב- ψ). אז:

$$\varphi\left\{\frac{t}{x}\right\} = \varphi$$

$$M, v' \models \varphi\left\{\frac{t}{x}\right\} \Leftrightarrow M, v' \models \varphi \Leftrightarrow^* M, v \models \varphi$$

* - לגבי נוסחא, מה שמשנה את ערך האמת זה רק המשתנים החופשיים, v ו- v' נותנות אותו דבר (אותם ערכים) למשתנים החופשיים של φ (למעשה רק ל- x הן נותנות ערך שונה, שהוא לא בין המשתנים החופשיים)

נשים לב שעוד לא השתמשנו בנתון ש- t הוא חופשי להצבה במקום x ב- φ . כעת נשתמש בו, באפשרות ב'.

ii. אפשרות ב': x מופיע חופשי ב- $\varphi = \forall y \psi$.
מזה נובע:

$$y \neq x$$

• x מופיע חופשי ב- ψ

כמו כן, העובדה ש- t הוא חופשי להצבה במקום x ב- φ אומרת ש:

• t חופשי להצבה במקום x ב- ψ

• y אינו מופיע ב- t (אם הוא היה, אז בעקבות ההצבה [x מופיע ב- ψ , אחרת היינו

באפשרות א'] ה- y של t יהפוך להיות קשור וזו הצבה אסורה).

$$\varphi\left\{\frac{t}{x}\right\} = \forall y \varphi\left\{\frac{t}{x}\right\}$$

נזכור שהשוויון האחרון לא נכון תמיד, זה כי $y \neq x$ ועצם זה שעושים את הפעולה זה גם אומר שהוא חופשי להצבה ב- ψ ו- t אינו מכיל את y.

כעת נראה ש: $M, v \models \varphi\left\{\frac{t}{x}\right\} \Rightarrow M, v' \models \varphi$ (כמו שאמרנו – הכיוון ההפוך כתרגיל).

בניח כי $M, w \models \varphi$ לכל y -וריאנט w של v' .

צ"ל: $M, w \models \varphi\{\frac{t}{x}\}$ לכל y -וריאנט w של v .

אז יהי w השמה y -וריאנט של v (כך צפוי שנתחיל). כעת טבלה על מנת לבדוק מה בדיוק כל השמה נותנת למשתנים השונים, ולש"ע t :

	v	$v' = v\{x=v[t]\}$	w	$w' = w\{x=v[t]\}$
x	a	d	a	d
y	b	b	e	e
$z \neq x, y$	c_z	c_z	c_z	c_z
t	d		d	

(z מסמל את כל הערכים שהם לא x או y)

בטור הראשון סימנו את הערכים (c_z מתאר את קבוצת הערכים לשאר המשתנים) בטור השני, v' נותנת ל- x את מה ש- v נותנת ל- t , לשאר המשתנים אותו דבר (זו השמה x -וריאנטית) ומה שהיא נותנת ל- t לא מעניין אותנו כרגע. בטור השלישי, w היא y -וריאנט של v ולכן נותנת לשאר המשתנים אותו ערך (את הערך עבור y סימנו). לגבי הערך של t , הוא כמו של v כיוון ש- y לא מופיע חופשי ב- t . בטור הרביעי, בצורה דומה. נשים לב ש: $w' = w\{x=v[t]\} = w\{x=w[t]\}$.

מהטבלה אנחנו רואים (גילינו) ש- w' היא y -וריאנט של v' . לכן מהנחתנו נובע ש: $M, w' \models \varphi$ כלומר $M, w\{x=v[t]\} \models \varphi$.

ל.ה.א על φ , $M, w \models \varphi\{\frac{t}{x}\}$.

בכך סיימנו את הכיוון הראשון. את הכיוון השני יש לעשות בבית. כנ"ל את 2 הכיוונים עבור $\varphi = \exists y \psi$.

בהוכחה זו עברנו על הרבה הגדרות שראינו בעבר, חשוב לוודא שמבינים אותה. מומלץ כעת לחזור על הכל ולראות שיודעים להוכיח את הכל לבד. זה אולי ארוך אבל לא קשה. בזה אנחנו מסיימים את הנושא הזה (בעתיד כנראה לא נראה הוכחות מפורטות ברמה הזו).

כריעות

אחרי ששיעור קודם הגדרנו סמנטיקה, יחסי נביעה, ספיקות. הבעיה העיקרית שצריך להתמודד איתה: יש לי קבוצה של נוסחאות (T), ונוסחא אחרת (φ) ואנו רוצים לברר האם φ נובעת מ-T או לא. (צריך לברר t-נביעה או v-נביעה, ואם T מורכבת מפסוקים אז זה אותו דבר). נניח ש-T היא סופית. אפשר אפילו להניח ש-T ריקה (אם מדובר על t-נביעה אז לפי משפט הדדקוציה אבל לעשות רדקוציה לנביעה מהקבוצה הריקה, אם מדובר על v-נביעה אז מבצעים סגור ואז משתמשים במשפט הדדקוציה). כלומר אפשר (כלומר מספיק) להסתכל האם נוסחא האם אמת לוגית או לא.

פעם היה לנו אלג' שקבע האם משהו הוא טאו' או לא (כלומר בתחשיב הפסוקים - היו טבלאות אמת). לכן תחשיב הפסוקים הוא כריע (יש גם עניין של יעילות אבל זה לא עניינו). מה קורה עם FOL? התשובה היא לא, אין דרך כזו.

כשאין כריעות אפשר לחפש חצי כריעות - בהנתן קלט יש אלג' שעובד ועובד ואם התשובה היא כן הוא עוצר ואם לא, אז יתכן שהוא לא יעצור (בזמן הריצה אנחנו לא יודעים אם הוא לא עוצר כי הוא לא סיים או כי הוא לא יעצור לעולם). נראה דוגמא ואז את התוצאות.

בדרך כשרוצים להראות שנוסחא לא תקפה, מה עושים? נקח תחילה דוגמא ספציפית:

דוגמא

בשיעור שעבר שדיברנו על הקשר בין t-נביעה ל-v-נביעה, ראינו ש:

$$\vdash_{FOL} \forall x(p(x) \rightarrow q(x)) \rightarrow ((\forall x p(x)) \rightarrow \forall x(q(x)))$$

תקף לוגית (אם משהו הוא v-נובע אז הוא t-נובע), וגם אמרנו שההיפך אינו נכון:

$$\vdash_{FOL} ((\forall x p(x)) \rightarrow \forall x(q(x))) \rightarrow \forall x(p(x) \rightarrow q(x))$$

איך נראה שלא? הדרך הכי פשוטה זה לחפש דוגמא נגדית. כאן p ו-q הם פרדיקטים חד מקומים, אך זה כמובן עובד לכל פרדיקט.

אנו מחפשים מבנה שבוא $\forall x p(x)$ לא נכון. כלומר (נתחיל לבנות את המבנה):

D	T
a	$a \in I[p]$

וכעת הבטחנו שחצי שמאל נכון, כעת צד לדאוג שחצי מימין לא יהיה נכון. נצטרך להוסיף מישהו כדי לוודא שצד ימין לא יהיה נכון, ולכן נוסיף איבר b שידווא את זה:

D	T
a	$a \notin I[p]$
b	$b \in I[p], b \notin I[q]$

אז זה המבנה שלנו:

$$D = \{a, b\}, I[p] = \{b\}, I[q] = \emptyset$$

מצב פרדוקסלי

תרגיל ראשון היה להראות שהראשון הוא תקף לוגית והשני לא. השני לכאורה היה יותר קל (היינו צריכים בו למצוא דוגמא נגדית, בראשון כדי להוכיח היינו צריכים: יהי M נבנה נקח השמה, נראה ש... וכו', לא שזה מאוד קשה אבל זה מעצבן יותר מאשר למצוא דוגמא נגדית).

אבל האמת היא שאין דרך למצוא דוגמאות נגדיות באופן כללי - השאלה אם משהו לא תקף לוגית זו בעיה שהיא לא כריעה וגם לא חצי כריעה. אפשר באופן שיטתי לעבור רק על כל המודלים הסופיים. אז נעבור אחד אחד כדי למצוא איפה הוא ספיק, ואם יש סופי נוכל למצוא אותו (כלומר אם יש אחד סופי שמהווה דוגמא נגדית). אבל יש פסוקים שהם ספיקים אבל היחידים שמספקים אותם הם אין סופיים. הדוגמא המפורסמת ביותר למצב כזה: נניח R סימן יחס דו-מקומי. הפסוק:

$$\forall x \neg R(x, x) \wedge \forall x \forall y (R(x, y) \wedge R(y, z) \rightarrow R(x, z)) \wedge \forall x \exists y R(x, y)$$

זה הוא פסוק ספיק - יש לו מודל, אבל לא מודל סופי.

הטענה היא שהפסוק הזה ספיק, כלומר שלילתו היא אינה אמת לוגית (אפשר להפריך אותה).

1. אומר ש-R אי רפלקסיבי במובן החזק
2. אומר ש-R הוא טרנזיטיבי
3. לכל אחד יש יותר גדול (אנחנו מודים שעלינו על זה ש: $R=<$)

אז הוא ספיק בטבעיים.

כמו כן, כל מודל של הדבר הזה חייב להיות אין סופי. למה?

יש בתחום a_0 (יש לפחות איבור אחד, נסמן אותו כ), ממנו יש את a_1 וכך הלאה:

$$a_0 \stackrel{R}{\rightarrow} a_1 \stackrel{R}{\rightarrow} a_2 \stackrel{R}{\rightarrow} a_3 \stackrel{R}{\rightarrow} a_4 \stackrel{R}{\rightarrow} \dots$$

עד כה השתמנו רק בנתון האחרון. וזה לא מספיק. צריך להראות שלא חזרנו לראשון, וזה נובע לפי האי-רפלקסיביות והטרנזיטיביות.

להראות שמהו הוא כן תקף לוגית זה דווקא כן חצי כריע.

במודלים - אם שניהם היו חצי כריעות, היה אלג שמכריע (הרצה במקביל והראשון שעוצר). אז אפשר היה לבוא בכיוון אחר: מזה שהבעיה של תקפות לא כריעה, אך היא חצי כריעה, נובע שבעיית אי תקפות אינה אפילו חצי כריעה.

לסיכום: מספיק לדבר על הוכחת פסוקים (ראינו רדוקציה לזה), ומספיק לדבר על יכולת ההוכחה / הפרכה של אמת לוגית. כעת:

- האם כן תקף לוגית (שקול גם לא-ספיקות, על ידי $\neg$) זה חצי כריע.
- האם לא תקף לוגית (שקול גם לספיקות, על ידי $\neg$) אפילו לא חצי כריע.

תחשיבים

יש הרבה תחשיבים ב-FOL אנחנו לומדים שניים מהם:

- הילבט (הרחבה מתחשיב הפסוקים)
- דדקוציה טבעית (הרחבה מתחשיב הפסוקים)

בתוכנות מחשב בדרך כלל לא עובדים איתם (זה לא נוח לעבודה עם מחשב, שם יש שיטות יותר יעילות).
כעת כשעוברים על שניהם, מומלץ להתסכל על הדף שחולק השיעור.

דדקוציה טבעית

נוספו בסך הכל 4 כללים, עבור "לכל" ול"קיים", כלל הכנסה וכלל סילוק לכל אחד.
יש לנו כאן כמה הגבלות לגבי משתנים חופשיים וקשורים, והסילוק של "קיים" אף נראה מאוד מוזר.

נקח דוגמא על מנת להסביר מה הולך. נקח תרגיל המתמטיקה (שלא אמורה להיות בעיה להוכיח אותו, מצד שני הוא בחדו"א), נראה מה ההוכחה שלנו ואז נראה שהוכחנו את זה בדדקוציה טבעית למעשה.

$$\lim_{n \rightarrow \infty} a_n + b_n = a + b \quad \text{אז} \quad \lim_{n \rightarrow \infty} a_n = a, \quad \lim_{n \rightarrow \infty} b_n = b \quad \text{המשפט: אם}$$

אז איך היינו מוכיחים תרגיל כזה? ככה:

הוכחה:

יהי $\epsilon > 0$.

$$\begin{aligned} & \text{קיים } N \text{ כך שכל } n > N: |a_n - a| < \frac{\epsilon}{2} \quad \text{קיים } N' \text{ כך שכל } n > N': |b_n - b| < \frac{\epsilon}{2} \\ & \text{נקח } N'' = \max(N, N') \text{ אז לכל } n > N'': |(a_n + b_n) - (a + b)| < \epsilon \end{aligned}$$

וכעת להוכחה בדדקוציה טבעית (נראה רק סכימה, בתרגול נראה הוכחה דומה מלאה):
הנחות:

$$\forall \epsilon (\epsilon > 0 \rightarrow \exists N \forall n (n > N \rightarrow |a_n - a| < \epsilon))$$

$$\forall \epsilon (\epsilon > 0 \rightarrow \exists N \forall n (n > N \rightarrow |b_n - b| < \epsilon))$$

ונרצה להראות:

$$\forall \epsilon (\epsilon > 0 \rightarrow \exists N \forall n (n > N \rightarrow |(a_n + b_n) - (a + b)| < \epsilon))$$

הערות:

- יהי מרמז על שימוש בכלל הכנסה של לכל בסוף.
- בעברית כתבנו N ו- N' , אבל נשים לב בפורמלי (כלומר ב-2 ההנחות המוצרנות) יש גם ל- a וגם ל- b . למה אנחנו השתמשנו בשני סימונים שונים? כי בין קשורים אי אפשר לעשות מקסימום. בעברית אנחנו זמינית הופכים אותו לחופשי.

- שימוש בידע של "לכל" זה לעבור למקרים פרטיים. אנחנו עברנו מהנתון למקרה הפרטי של $\frac{\epsilon}{2}$.

השתמשנו בכלל סילוק של "לכל". מחקנו את ה"לכל" מהראשון והצבנו $\frac{\epsilon}{2}$ במקום ϵ . זה חוקי כי

אין קשירה בהצבה. השתמשנו במודוס פוננס - כלל הסילוק של גרירה (כי ידוע לנו ש- $\frac{\epsilon}{2} > 0$). אז

אחר שימוש ב- 2 הכללים וידע בסיסי על חילוק, קיבלנו ידע מהצורה של קיים:

$$\exists N \forall n (n > N \rightarrow |a_n - a| < \frac{\epsilon}{2})$$

$$\exists N \forall n (n > N \rightarrow |b_n - b| < \frac{\epsilon}{2})$$

איך משתמשים בידע הזה. זה אומר לנו שיש כזה. טוב אז נקח אותו ונתן לו שם (לעיתים קרובות זה אותו שם עצמו). אז כעת:

$$\forall n (n > N \rightarrow |a_n - a| < \frac{\epsilon}{2})$$

ופה N הוא משתנה חופשי שיש לו את התכונה הזו. אז אנו מנחים ש-N הוא משהו שיש לו את ההנחה הזו. על סמך שתי ההנחות האלה, נראה מה שכתוב במסגרת מרובעת.

עכשיו לשימוש בנתון השני, שהוא כעת (גם אצלנו סילקנו וכו'):

$$\exists N \forall n (n > N \rightarrow |b_n - b| < \frac{\epsilon}{2})$$

אבל אנחנו לא יכולים לבחור שוב את N כי הוא כבר תפוס, הוא מופיע בהנחות שלנו, הוא כבר לא משתנה חופשי. אז מה נעשה? נקח משתנה אחר, אנחנו הצענו N'. נוסיף הנחה שלישית ונקבל בסך הכל:

$$\epsilon > 0$$

$$\forall n (n > N \rightarrow |a_n - a| < \epsilon)$$

$$\forall n (n > N' \rightarrow |b_n - b| < \epsilon)$$

כששני האחרונים יסיימו את תפקידם, זה כאילו הנחנו רק את הראשון.

עכשיו עם קצת ידע במספרים, נרצה להראות כי:

$$(*) \exists N \forall n (n > N \rightarrow |(a_n + b_n) - (a + b)| < \epsilon)$$

אז נרצה להראות שקיים, ואנחנו נראה אותו: $N'' = \max(N, N')$ (בעיקרון אפשר גם בשלילה, להניח

שאין ואז להגיע לסתירה). ה-t שלנו שאנחנו רוצים להציב ב- (*) [בשביל הקיים]: $t = \max(N, N')$.

נפעיל את כלל הסילוק של "לכל" על שתי ההנחות השניות. כעת נוסיף עוד הנחה: $n > N''$. כעת צריך להראות את צד ימין של (*) [כלומר את $|(a_n + b_n) - (a + b)| < \epsilon$]. נסיים כאן.

במה התשמחנו בהוכחה?

בהוכחה הזו השתמשנו בכל 4 הכללים החדשים שלנו, וגם בכלל הגרירה (באחרים לא השתמשנו כי הם לא מופיעים בנוסחא שלנו). נזכור שכשהוכחנו שמהו הוא קיים, השימוש הוא להוסיף הנחה חדשה עם משתנה חדש (כלומר שהוא לא מופיע כמשתנה חופשי בהנחות שעדיין קיימות).

בתרגול נראה הוכחה מלאה ומסודרת של משפט מחדו"א. כאן ראינו את הרעיון.

פה הוספנו עוד 4 אקסיומות ועוד כלל היסק חדש - כלל ההכללה.

מי מתאים למי?

נזכר התחשיבים האלה אמורים להיות עבור הוכחות של נוסאות מתוך הנחות (קבוצת נוסחאות).

בהילברט יש את כלל הכללה, לכן הוא מכון ל- v -נביעה (ספרים שעובדים עם הילברט בדרך כלל עובדים רק עם v -נביעה)
ב- $NDFOL$, יש לנו כלל הכנסה של גרירה, והוא לא נכון עבור v -נביעה, ולכן ND מכון עבור t -נביעה.

המשפטים המקשרים הם השניים הבאים.

משפט הנאותות והשלמות של $NDFOL$:

$$T \vdash_{NDFOL} \varphi \Leftrightarrow T \vdash_{FOL}^t \varphi$$

(כאשר $T \vdash_{NDFOL} \varphi$ מוגדר כצפוי – אם יש $I \subseteq T$ סופית כך שיש סדרת סקוונטים... וכו')

משפט הנאותות והשלמות של $HFOL$:

$$T \vdash_{HFOL} \varphi \Leftrightarrow T \vdash_{FOL}^v \varphi$$

(כאשר $T \vdash_{HFOL} \varphi$ מוגדר כצפוי – יש סדרת הוכחה... וכו')

כמה מילים על האקיומות של $HFOL$:

מה הכוונה ב"כל האינסטנסיות של האקסיומות של HPC "?

לדוגמא:

$$(T \vdash) \quad \varphi \rightarrow (\psi \rightarrow \varphi)$$

(זה לא מדויק, כי פי ופסי הם משתנים עבור נוסחאות, ולכן זה במטא שפה וכו')

אז יש לנו אותן סכמות, כל סכימה שהופיעה ב- HPC תהיה סכימה ב- $HFOL$ רק שעכשיו אנחנו מציבים דברים מתוך השפה הרלוונטית.

כדי להראות נאותות נראה שכל האקסיומות שומרות על נכונות, ואז שכללי ההיסק משמרים את זה. בעמוד הבא נראה סכימה של ההוכחה של הנאותות.

משפט הנאותות של HFOL

המשפט: $T \vdash_{HFOL} \varphi \Rightarrow T \vdash_{FOL}^v \varphi$

סכימת ההוכחה

באינדוקציה על אורך סדרה של הוכחה (בדיוק כמו שעשינו עבור HPC).
אם φ שייך ל-T אז ברור. אם φ אקסיומה אז φ תקפה – כלומר צריך להראות שהיא תקפה! ואז באה ההוכחה לכל אחת האקסיומות (אנחנו נעשה אחת).
אחרי זה בא שלב האינדוקציה: שתי אפשרויות - עבור MP, ועבור כלל ההיסק החדש – ההכללה.

האסקיומה עבורה אנו נראה תקפות:

נראה ש: $M \models \forall x A \rightarrow A\{\frac{t}{x}\}$ (זו אחת האקסיומות החדשות שלנו ב-HFOL) לכל מבנה M עבור

השפה. כלומר לכל M ולכל v : $M, v \models \forall x A \rightarrow A\{\frac{t}{x}\}$.

יהיו M, v מבנה השמה בו.

אם $M, v \models \forall x A$ אז $M, v \models A\{\frac{t}{x}\}$.

נניח ש- $M, v \models \forall x A$. נראה ש- $M, v \models A\{\frac{t}{x}\}$ ושוב הגרירה תהיה נכונה. כדי להוכיח את זה, אנחנו

מכניסים לתמונה את משפט ההצבה. $M, v \models A\{\frac{t}{x}\}$ אם"ם $M, v\{x=v[t]\} \models A$. אבל $v\{x=v[t]\}$ היא

x-וריאנט של v (כי זה רק עדכון של v על ידי שינוי של x) ולכן כיוון ש- $M, v \models A\{\frac{t}{x}\}$

$M, v\{x=v[t]\} \models A$.