לוגיקה למדעי המחשב

ניצן פומרנץ*

25 ביוני 2015

רשימות בקורס לוגיקה למדעי המחשב, סמסטר אביב תשע"ה, אוניברסיטת תל אביב.
טעויות קורות ־ אשמח שתעדכנו אותי עליהן ואשתקנן.

הרצאה 1 ־ 8.3.15

אמיר שפילקה shpilka@post.tau.ac.il
שרייבר 118
שעת קבלה: יום א' 13־12
מתרגלים: לירון כהן, בן לי וולך.
תרגילים שבועיים ־ הגשה בזוגות. חייבים להגיש לפחות 9 תרגילים, והציון יקבע לפי ה־9 הטובים ביותר.
בוחן אמצע יתבסס על התרגילים, אינו חובה ואם מקבלים מעל 75 אז יש בונוס 4 נקודות לציון הסופי. תאריך: תחילת מאי.
מבנה ציון: 90% בחינה ו־10% ש"ב (מגן).

תוכן עניינים

*www.cs.tau.ac.il/~pomerantz

0.1 גיאומטריה אוקלידית

אקסיומות אוקלידס

- דרך כל שתי נקודות עובר ישר אחד בלבד.
- 2 ישרים נחתכים לכל היותר בנק' אחת.
- בהינתן ישר ונק' מחוצה לו, ניתן להעביר מקביל לישר דרך הנק'.
- $\vdots$

בעזרת האקסיומות ניתן להוכיח, בין היתר:

- סכום הזוויות במשולש 180°.
- במשולש שווה שוקיים זוויות הבסיס שוות.
- $\vdots$

אחת השאלות שנשארה פתוחה (ללא תשובה) במשך כ־2000 שנה היא: האם אקסיומת המקבילים "נחוצה"? והאם היא "נכונה"?
נכונות: תלוי.

0.2 טענות וטיעון תקף

טענה $F = m \cdot a$. טענה זו תלויה בעולם.
טענה: אם לכל x, y מתקיים $x \cdot y = y \cdot x$ אז אם $F = m \cdot a$ אז מתקיים $F = a \cdot m$.
זו טענה שנכונותה אינה תלויה בעולם.
אנחנו נרצה להבין אילו טענות תלויות בעולם ואילו טענות מהוות "טיעונים תקפים".

הגדרה 0.1 טיעון הוא תקף אם בכל פעם שההנחות נכונות גם המסקנה נכונה.

דוגמאות:

- כל החייזרים בכיתה לובשים שחור.
- אם היום יום שני אז מחר יום רביעי.
- כל עורב הוא שחור. שחור הוא צבע. לכן עורב הוא צבע. יש כפל משמעות.

דוגמה לטיעון לא תקף: אין אדם בלי חסרונות. ~~לדני~~ למיצי יש חסרונות, לכן ~~דני~~ מיצי בן אדם.
בקורס נלמד לזהות טיעונים תקפים ונלמד איך להוכיח תקפות של טיעונים.

0.3 אינדוקצית מבנה

דוגמה: איך מתארים קבוצה? למשל ע"י רשימת איבריה.
איך נתאר את קב' קרובי המשפחה שלנו? תיאור ע"י רשימת איברי הקבוצה, קצת מסובך.
שיטה אחרת: משפחה גרעינית: אני, אחיי, אחיותי, הוריי, ילדיי, אשתי.
כלל: אם פלוני/ת הורה, ילד, אח, אחות, בן/בת זוג של מישהו בקבוצה אז הוא גם בקבוצה.
קבוצת קרובי המשפחה שלי היא קבוצת האנשים המינימלית שמכילה את המשפחה הגרעינית (בסיס) וסגורה להפעלת הכלל.
B - קבוצת בסיס. F - אוסף פונקציות. רצינו לבנות קבוצה המכילה את B וסגורה לפעולות ב־F.
דוגמה: $B = \{0\}$, $F = \{+1\}$ ו־$\mathbb{N}$ סגורה ל־F שמכילה את B.

0.3.1 בניית קבוצה באינדוקציה

Ω קבוצה (עולם)
$B \subseteq \Omega$ קבוצת בסיס
F קבוצת פונקציות כך שכל $f_{n,i} \in F$ היא פונקציה $f_{n,i} : \Omega^n \to \Omega$
נסמן ב־$X_{B,F}$ את הקבוצה המוגדרת באינדוקציה ע"י B ו־F. $X_{B,F}$ ההיא הקבוצה המקיימת את הדרישות הבאות:

1. $B \subseteq X_{B,F}$
2. לכל $f_{n,i} \in F$ ולכל $x_1, ..., x_n \in X_{B,F}$ גם $f_{n,i}(x_1, ..., x_n) \in X_{B,F}$
3. $X_{B,F}$ מינימלית

משפט 0.2 קיימת קבוצה $X_{B,F}$ המקיימת 1,2 ו־3.

הוכחה: תהי $Y = \{A \,|\, A \subseteq \Omega \text{ and satisfies } 1{,}2\}$. למשל $\Omega \in Y$.
נגדיר כעת: $X = \bigcap_{A \in Y} A$.
נטען ש־X מקיימת את 1,2. כיוון שלכל $A \in Y$ מתקיים $B \subseteq A$ הרי $B \subseteq X$ לכן X מקיימת את 1.
לגבי 2: תהי $f_{n,i} \in F$ פונקציה כלשהי. יהיו $x_1, ..., x_n \in X$, נרצה להוכיח ש־$f_{n,i}(x_1, ..., x_n) \in X$.
מההגדרה, לכל $A \in Y$ חייב להתקיים $x_1, ..., x_n \in A$ ו־A מקיימת את 2. לכן $f_{n,i}(x_1, ..., x_n) \in A$ ואז $f_{n,i}(x_1, .., x_n) \in \bigcap_{A \in Y} A = X$.
ראינו כי X מקיימת את 1,2. מינימליות: נובע מההגדרה כי אם T מקיימת את דרישות 1,2 אז $X \subset T$.
(יחידות: אותו הדבר)
אם X' מקיים 1,2,3 אזי מהגדרה $X \subset X'$ ולכן או $X \subsetneq X'$(בסתירה למינימליות X') או $X = X'$. ■

הערה 0.3 $X_{B,F}$ יקרא הסגור של B תחת הפעולות ב־F.

משפט 0.4 משפט ההוכחה באינדוקציה
אם A קבוצה המקיימת:

1. $B \subset A$
2. לכל $f_{n,i} \in F$ ולכל $x_1, ..., x_n \in A$ מתקיים $f_{n,i}(x_1, .., x_n) \in A$

אזי $X_{B,F} \subset A$.

הערה 0.5 בתיכון, רוצים להראות שאיזושהי טענה מתקיימת למספרים הטבעיים.

$$\mathbb{N} \subset A = \{\text{all elements that the claim is true for}\}$$

בהוכחה באינדוקציה אנו מראים:

1. $0 \in A$ (0 מקיים את הטענה)
2. שאם n מקיים את הטענה אז כך גם $n+1$.

ומכאן מסיקים שהסגור $X_{\{0\},\{+1\}} \supset A$.

0.3.2 סדרת יצירה/בניה

דוגמה: $B = \{0\}$, $F = \{+1\}$. סדרה יצירה עבור 2: $0, 0+1, 0+2$.

הגדרה 0.6 סדרת יצירה עבור $a \in X_{B,F}$ היא סדרה סופית $a_1, .., a_k$ כך שמתקיים:

1. $a = a_k$
2. כל a_i מקיים $a_i \in B$ או התקבל מהפעלת פונקציה ב־F על איברים קודמים בסדרה.

הערה 0.7 סדרת יצירה תמיד סופית.

משפט 0.8 $a \in X_{B,F}$ אם ורק אם יש ל־a סדרת יצירה.

הוכחה: $\Leftarrow$: נגדיר

$$Y = \{a \,|\, \text{a has a creation series}\}$$

נראה כי $X_{B,F} \subset Y$ ע"י אינדוקצית מבנה.
צ"ל ש־$B \subset Y$. יהי $b \in B$; סדרת היצירה של b היא b.
כעת צריך להראות סגירות Y תחת F.
אז צ"ל אם $f_{n,i} \in F$ ו־$x_1, ..., x_n \in Y$ אזי $f_{n,i}(x_1, ..., x_n) \in Y$.
אכן, יהיו $x_1, ..., x_n \in Y$ ו־$f_{n,i} \in F$; נבנה את סדרת היצירה. כיוון ש־$x_1, .., x_n \in Y$, יש להם סדרות יצירה:

$$x_1^1, .., x_{m_1}^1, ..., x_1^n, .., x_{m_n}^n, f_{n,i}(x_1, ..., x_n)$$

כש־$x_1^1, .., x_{m_1}^1$ סדרת יצירה של x_1. קל לוודא שזוהי סדרת יצירה ל־$f_{n,i}(x_1, ..., x_n)$.
ממשפט ההוכחה באינדוקציה נובע כי־$X_{B,F} \subset Y$. לכן, לכל איבר ב־$X_{B,F}$ יש סדרת יצירה.
$\Rightarrow$: נסמן ב־X_nאת קבוצת האיברים להם יש סדרת יצירה באורך n. נראה כי

$$\bigcup_{n \in \mathbb{N}} X_n \subset X_{B,F}$$

נוכיח זאת באינדוקציה על הטבעיים. ואז: X_1= קבוצת האיברים להם יש סדרת יצירה באורך 1. דהיינו, $X_1 = B$.
נניח שהראינו כי $X_1, ..., X_n \subset X_{B,F}$ ונראה זאת ל־X_{n+1}.
יהי $a \in X_{n+1}$. ל־a סדרת יצירה באורך $n+1$: $x_1, ..., x_n, a$. נובע ש־$x_n \in X_n$ ובאופן כללי, $x_i \in X_i$.
בפרט, מהנחת האינדוקציה, $x_1, ..., x_n \in X_{B,F}$. כעת אם $a \in B$ אז בוודאי $a \in X_{B,F}$.
אחרת, a התקבל מהפעלת $f \in F$ על איברים קודמים בסדרה. כיוון שכל איברי הסדרה הקודמים ל־a ב־$X_{B,F}$ ו־$X_{B,F}$ סגורה להפעלת f; נקבל כי $a \in X_{B,F}$ כנדרש. ■

דוגמה: שפת ה־aba. $\Omega = \{a, b\}^*$
עבור קבוצה Σ נסמן

$$\Sigma^* = \{\text{Finite words created by } \Sigma\}$$

$$\{a, b\}^* = \{\varepsilon, a, b, aa, ab, ba, bb, ...\}$$

$$\{a\}^* = \{\varepsilon, a, aa, aaa, ...\}$$

אז עבור Ω כנ"ל ו־$B = \{ab\}$ נגדיר פעולות:

- $f_1(w) = waba$
- $f_2(w)$=מחיקת רצף aa ימני ביותר וכתיבת b במקומו. אם אין רצף כזה אז $f_2(w) = w$. למשל $f_2(aaaa) = aab$
- $f_3(w)$=מחיקת רצף ימני ביותר של bbb.

דוגמה: נראה כי abb נמצאת בשפה:

$$ab, \underbrace{ababa}_{f_1(ab)}, \underbrace{abababa}_{f_1(ababa)}, \underbrace{ababbba}_{f_2(abababa)}, \underbrace{abaa}_{f_3(ababbba)}, \underbrace{abb}_{f_2(abaa)}$$

דוגמה: הראו כי aba לא בשפה. איך מראים שאיבר אינו ב־$X_{B,F}$?
רעיון: מוצאים תכונה שמפרידה את האיבר מאברי $X_{B,F}$.
תכונה: ב־w מספר אי זוגי של a. טענה ברורה: ל־aba אין את התכונה.
תהי

$$Y = \{w \,|\, \text{There is an odd number of } as \text{ in } w\}$$

ברור כי $aba \notin Y$.

טענה 0.9 $X_{B,F} \subset Y$.

הוכחה: $B \subset Y$ כי $ab \in Y$.
תהי $w \in Y$. צריך להראות ש־$f_1(w), f_2(w), f_3(w) \in Y$.
$f_1(w) = waba$. בגלל ש־ אי זוגי+2=אי זוגי נקבל ש־$f_1(w) \in Y$. באופן דומה עבור f_2, f_3
לכן לפי משפט האינדוקציה $X_{B,F} \subset Y$. ■

חלק I
תחשיב הפסוקים

תאור לא פורמלי:
אותיות:

$$P_0, P_1, ...$$

קשרים:

$$\wedge, \vee, \neg, \rightarrow, \leftrightarrow$$

הרצאה 2 - 15.3.15
מהם נבנה ביטויים מורכבים.
ביטוי: סדרה סופית של סימנים: $\Sigma = \{(,), \wedge, \vee, \neg, \Rightarrow, \Leftrightarrow\} \cup \{P_i \,|\, i \in \mathbb{N}\}$. קבוצת הביטויים תהיה: Σ^*.
נגדיר כעת את אוסף הביטויים החוקיים, בהגדרה אינדוקטיבית.
<u>בסיס:</u> פסוקים / נוסחאות אטומיות: $B = \{P_i \,|\, i \in \mathbb{N}\}$
פעולות: $F = \{F_\wedge, F_\vee, F_\neg, F_\Rightarrow, F_\Leftrightarrow\}$, כאשר:

$$\begin{aligned} F_\wedge(a,b) &= (a \wedge b) \\ F_\vee(a,b) &= (a \vee b) \\ F_\neg(a) &= (\neg a) \\ &\vdots \end{aligned}$$

קבוצת הביטויים החוקיים (WFF - Well Formed Formulas): הסגור של B ביחס ל־F.

דוגמאות:

- $(P_1 \wedge P_2)$ ביטוי חוקי. הסבר $P_1, P_2 \in B$ ואז הסדרה היא

$$P_1, P_2, F_\wedge(P_1, P_2)$$

- $P_1(\Rightarrow P_2$ אינו ביטוי חוקי
- $P_1 \Rightarrow\Rightarrow P_2$ אינו ביטוי חוקי

טענה 0.10 כל ביטוי חוקי (WFF) הוא פסוק אטומי או מתחיל ב־) ונגמר ב־(.

הוכחה: תהי $Y \subset \Sigma^*$ הקב' המכילה את B ואת כל הביטויים שמתחילים ב־) ונגמרים ב־(. נרצה להראות ש־$X_{B,F} \subset Y$. ברור כי $B \subset Y$ (לפי ההגדרה).
נשאר להראות סגירות תחת F: בודקים כל אחת מהפונקציות ורואים שכן.
ממשפט ההוכחה באינדוקציה $WFF = X_{B,F} \subset Y$. ■

לפי הטענה נוכל להסיק ששתי הדוגמאות הנ"ל אכן אינן ביטויים חוקיים. נוכיח טענה פשוטה נוספת שתשמש אותנו בהמשך:

טענה 0.11 בכל ביטוי חוקי $\#_(= \#_)$.

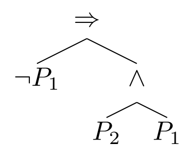
הוכחה: Y= קבוצת כל הביטויים e כך ש־$\#_((e) = \#_)(e)$. ברור ש־$B \subset Y$.
סגירות תחת F: יהיו $\alpha, \beta \in Y$. למשל אם ב־α יש n סוגריים מכל סוג וב־β יש k סוגריים מכל סוג, אז ב־$(\alpha \wedge \beta)$ יש $n+k+1$ סוגריים מכל סוג.
באותו אופן לכל יתר הפונקציות. ■

הערה 0.12 $(P_1 \wedge P_2)$ ו־$(P_2 \wedge P_1)$ הם ביטויים **שונים**.

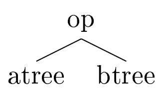
1 עצי יצירה (גזירה)

$$((\neg P_1) \Rightarrow (P_2 \wedge P_1))$$

עבור פסוק זה עץ הגזירה יהיה:



הגדרה 1.1 לפסוק אטומי P_i נתאים את העץ $\dot{P}_i$. לפסוק $(\alpha\, op\, \beta)$ נתאים את העץ



לפסוק $(\neg\alpha)$ יתאים העץ

משפט 1.2 משפט הקריאה היחידה
לכל $\alpha \in WFF$ מתקיים בדיוק אחד מהבאים:

1. α פסוק אטומי
2. קיימים פסוקים יחידים $\beta, \gamma \in WFF$ כך ש־$\alpha = (\beta \wedge \gamma)$
3. קיימים פסוקים יחידים $\beta, \gamma \in WFF$ כך ש־$\alpha = (\beta \vee \gamma)$
4. קיימים פסוקים יחידים $\beta, \gamma \in WFF$ כך ש־$\alpha = (\beta \Rightarrow \gamma)$
5. קיימים פסוקים יחידים $\beta, \gamma \in WFF$ כך ש־$\alpha = (\beta \Leftrightarrow \gamma)$
6. קיים פסוק יחיד $\beta \in WFF$ כך ש־$\alpha = (\neg\beta)$

משפט 1.3 ניסוח שקול של משפט הקריאה היחידה
לכל פסוק $\alpha \in WFF$ מתקיים שני הבאים:

1. אם יש פסוקים $\beta, \gamma \in WFF$ ו־$op \in \{\wedge, \vee, \neg, \rightarrow, \leftrightarrow\}$ כך ש־$\alpha = (\beta\, op\, \gamma)$אז לכל זוג פסוקים β', γ' ו־$op' \in \{\wedge, \vee, \neg, \rightarrow, \leftrightarrow\}$ אם $\alpha = (\beta'\, op'\, \gamma')$ אז בהכרח $\beta = \beta'$, $op = op'$, $\gamma = \gamma'$.
2. אם יש פסוק $\beta \in WFF$ כך ש־$\alpha = \neg\beta$ אין פסוקים $\gamma, \delta \in WFF$ ו־$op \in \{\wedge, \vee, \neg, \rightarrow, \leftrightarrow\}$ כך ש־$\alpha = (\gamma\, op\, \delta)$ וגם אם $\varphi \in WFF$ מקיים $\alpha = (\neg\varphi)$ אז $\varphi = \beta$.

אלגוריתם לבדיקה האם $\alpha \in \Sigma^*$ הוא ב־WFF?

1. אם α פסוק אטומי אז נאמר $\alpha \in WFF$. אם לא, ממשיכים.
2. אם α מתחיל ב־(ונגמר ב־) אז נמחק אותם ונמשיך ל־3. אחרת נאמר ש־α אינו ב־WFF.
3. אם הסימן הראשון הוא $\neg$נמשיך ל־4. אחרת ל־5.
4. נמחק את $\neg$ ונחזור ל־1.
5. נעבור על הפסוק משמאל לימין עד שמספר הסוגריים השמאליים יהיה שווה למספר הימניים (נמצא את "האיבר השמאלי"). נקודת השוויון היא מיד לאחר הסוגר הימני שמשיג את השוויון:

$$...)|\cdot...$$

אם הגענו לקשר דו מקומי $(\wedge, \vee, \neg, \rightarrow, \leftrightarrow)$ נמחק אותו ונריץ שוב את האלגוריתם עבור סדרת הסימנים משמאל לקשר וסדרת הסימנים מימין לקשר.
אם לא הגענו לקשר דו מקומי או שאין נקודת שוויון נאמר ש־α אינו ב־WFF. אם הביטוי הימני או השמאלי לא ב־WFF נאמר ש־α אינו ב־WFF. לבסוף נודיע ש־$\alpha \in WFF$.

הוכחה: תרגיל. אפשר באינדוקציה על מספר הסימנים ולהראות שלפסוק שמתקבל באלגוריתם יש סדרת יצירה. ■

דוגמה: הפסוק: $(P_1 \wedge P_2)$. 1 לא מתקיים, עוברים ל־2. אז $P_1 \wedge P_2$ ונעבור ל־3. נעבור ישר ל־5. שולחים את P_1, P_2 ל־1.

1.1 סדר קדימויות על קשרים

- $\neg$
- $\wedge, \vee$
- $\Rightarrow, \Leftrightarrow$

דוגמה: הביטוי

$$\neg P_1 \Rightarrow P_2 \wedge P_3$$

מתאים לביטוי

$$((\neg P_1) \Rightarrow (P_2 \wedge P_3))$$

הערה 1.4 צריך לנהוג בזהירות!

$$(P_1 \Rightarrow P_2) \Rightarrow P_3$$
$$\neq$$
$$P_1 \Rightarrow (P_2 \Rightarrow P_3)$$

$$P_1 \wedge P_2 \wedge P_3$$
$$\neq$$
$$((P_1 \wedge P_2) \wedge P_3)$$
$$\neq$$
$$(P_1 \wedge (P_2 \wedge P_3))$$

הגדרה 1.5 $WFF_{\{\neg,\Rightarrow\}}$[1]
בסיס: $B = \{P_i \mid i \in \mathbb{N}\}$
פעולות: $F = \{F_\neg, F_\Rightarrow\}$
$WFF_{\{\neg,\Rightarrow\}}$ הוא הסגור.

2 טיעון תקף

הגדרה 2.1 (תזכורת) טיעון תקף:
טענה שמסקנתה נכונה בכל פעם שההנחות נכונות.

דוגמה (אינטואיציה) $((P_1 \wedge P_2) \Rightarrow P_1)$

מה שיעניין אותנו כדי לדעת האם ביטוי "נכון" או לא, זה רק האם ה"הנחות" $(P_1, ..., P_j)$ "נכונות" או לא. דהיינו, האם P_i נכון או לא נכון.

בהגדרת הסמנטיקה בתחשיב הפסוקים נשתמש בסימון הבא:

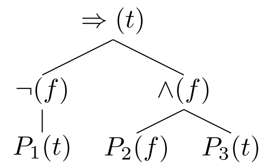
$$t : true$$
$$f : false$$

נרצה ליצור קשר בין "ערך האמת" של פסוק α לערכי האמת של המשתנים.

[1] באותו אופן מוגדרות $WFF_{\{\neg,\wedge\}}$ או $WFF_{\{\wedge,\vee\}}$

2.1 הגדרת ערך האמת

אינטואיציה: $((\neg P_1) \Rightarrow (P_2 \wedge P_1))$



ערכי האמת יחלחלו במעלה עץ היצירה, בהתאם לאופן בו הקשרים פועלים.

2.1.1 טבלאות האמת של הקשרים

$\alpha = (\neg P_1)$

$\mathbf{P_1}$	$(\neg \mathbf{P_1})$
f	t
t	f

, אז $\alpha = (P_1 \wedge P_2)$

$\mathbf{P_1}$	$\mathbf{P_2}$	$(\mathbf{P_1} \wedge \mathbf{P_2})$
f	f	f
f	t	f
t	f	f
t	t	t

...

הגדרה 2.2 השמה[2] היא פונקציה

$$v : \{P_i \mid i \in \mathbb{N}\} \to \{t, f\}$$

הגדרה 2.3 בהינתן השמה $v : \{P_i \mid i \in \mathbb{N}\} \to \{f, t\}$, נגדיר את ערך האמת[3]

$$\bar{v} : WFF \to \{t, f\}$$

יהי $\alpha \in WFF$

- אם α פסוק אטומי, נגדיר $\bar{v}(\alpha) = v(\alpha)$
- אם $\alpha = (\beta\, op\, \gamma)$ אז (עבור TT_{op} טבלת האמת של op)

$$\bar{v}(\alpha) = TT_{op}\left(\bar{v}(\beta), \bar{v}(\gamma)\right)$$

- אם $\alpha = (\neg\beta)$ אז $\bar{v}(\alpha) = TT_{\neg}\left(\bar{v}(\beta)\right)$

משפט 2.4 משפט הגדרת ערך האמת:
ערך האמת (כמו שהגדרנו אותו) מוגדר היטב, ובפרט יחיד.

טענה 2.5 אם כל המשתנים המופיעים ב־α הם מהקבוצה $\{P_1, ..., P_n\}$ ו־v, z השמות המסכימות על משתנים אלו (דהיינו, $\forall 1 \le i \le n,\ v(P_i) = z(P_i)$), אזי

$$\bar{v}(\alpha) = \bar{z}(\alpha)$$

הוכחה: באינדוקציה. ■

עכשיו אפשר להגדיר את טבלת האמת של כל פסוק α. אם ב־α מופיעים המשתנים $P_1, ..., P_n$ אז בטבלה יש 2^n שורות.

$\mathbf{P_1}$	...	$\mathbf{P_n}$	α
f	...	f	f
	$\vdots$		$\vdots$
t	...	t	t

אפשר לשאול, האם כל טבלת אמת ניתנת למימוש ע"י פסוק ב־WFF?

[2] אלכס (מרצה אחר) קורא להשמה סביבה

[3] אלכס מסמן $[|\alpha|]_v$ וארנון מסמן $v(\alpha)$ ולא מבדיל בין השמה לערך האמת

2.2 שלמות פונקציונלית

קבוצת קשרים היא שלמה (פונקציונלית)[4] אם ניתן להביע בעזרתה כל טבלת אמת.

טענה 2.6 $\{\neg,\wedge,\vee\}$ שלמה פונקציונלית.

הוכחה: (סקיצה) למשל אם בטבלה יש 3 עמודות, ובשורה מסוימת מופיע $P_1=t,P_2=t,P_3=f$ ו־$\alpha=t$ נתאים לשורה את הביטוי

$$((P_1\wedge P_2)\wedge(\neg P_3))$$

לכל שורה בטבלה בה הערך הוא t נגדיר את הפסוק המתאים המקבל את הערך t על השורה הזאת בלבד (הנ"ל). ניקח $\vee$ (בסדר כלשהו) על כל הפסוקים האלו. ■

טענה 2.7 $\{\neg,\wedge\}$ ו־$\{\neg,\Rightarrow\}$ שלמות פונקציונלית.

הוכחה: בתרגיל. ■

דוגמה: $\{\wedge,\vee\}$ לא שלמה פונקציונלית ־ אי אפשר להביע את $\neg$.

3 סימונים ומושגים סמנטיים בסיסיים

- אם $\bar{v}(\alpha)=t$ נסמן $v\models\alpha$ ונאמר כי v מספקת את α.
- נאמר כי α ספיקה, אם יש השמה v כך ש־$v\models\alpha$.
- נאמר כי α טאוטולוגיה אם לכל השמה v מתקיים $v\models\alpha$. למשל:
  - $((P_1\wedge P_2)\Rightarrow P_1)$
  - $(P_1\vee(\neg P_1))$
- α יקרא סתירה אם לא קיימת השמה v כך ש־$v\models\alpha$ ($\neg\alpha$ טאוטולוגיה)
- נאמר כי פסוק α שקול לפסוק β אם לכל השמה v מתקיים

  $$\bar{v}(\alpha)=\bar{v}(\beta)$$

  ונסמן $a\equiv\beta$.
- קבוצת נוסחאות Γ היא ספיקה אם יש השמה v כך שלכל $\alpha\in\Gamma$, $\bar{v}(\alpha)=t$ ונסמן $v\models\Gamma$.

  לדוגמה, הקבוצה $\Gamma=\{P_1,P_2,P_3\}$ היא ספיקה אם $v(P_1)=v(P_2)=v(P_3)=t$ ולכן $v\models\Gamma$, מצד שני הקבוצה $\Gamma=\{P_1,(\neg P_1)\}$ אינה ספיקה, נוכיח זאת:
  תהי v השמה כלשהי, מהגדרת ערך האמת $\bar{v}(\neg P_1)=TT_\neg(\bar{v}(P_1))\neq\bar{v}(P_1)$ כאשר אי השיוויון נובע מהתבוננות בטבלת האמת של $\neg$, ולכן לא ייתכן ששני ערכי האמת הם t ולכן $v\not\models\Gamma$.
- α נובעת סמנטית מ־Γ אם לכל v מתקיים: אם $v\models\Gamma$ אזי $v\models\alpha$ ומסמנים $\Gamma\models\alpha$.

הרצאה 3 ־ 22.3.15 כתב **נדב קרן**

נשים לב כי ישנן שקילויות שהוכחנו במתמטיקה בדידה אשר יש צורך להוכיח אותם מחדש בעולם מונחים זה, לדוגמא נתבונן במקרה הבינארי של כלל דה־מורגן:

$$\begin{aligned}\neg(\alpha\wedge\beta) &\equiv (\neg\alpha)\vee(\neg\beta)\\ \bar{v}(\neg(\alpha\wedge\beta)) &\equiv TT_\neg(\bar{v}(\alpha\wedge\beta))\\ \bar{v}(\neg(\alpha\wedge\beta)) &\equiv TT_\neg(TT_\wedge(\bar{v}(\alpha),\bar{v}(\beta)))\end{aligned}$$

[4] קיצור ש"פ

3.0.1 מסקנות חשובות

1. טאוטולוגיה:

$$((\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma)))$$

2. שקילויות:

$$\begin{aligned}
(\alpha \wedge \beta) \wedge \gamma &\equiv \alpha \wedge (\beta \wedge \gamma) \\
(\alpha \wedge \beta) \vee \gamma &\equiv (\alpha \vee \gamma) \wedge (\beta \vee \gamma) \\
(\alpha \wedge \beta) &\equiv (\beta \wedge \alpha) \\
(\alpha \vee \beta) &\equiv (\beta \vee \alpha) \\
\neg(\neg\alpha) &\equiv \alpha
\end{aligned}$$

3. אם $\Gamma \cup \{\alpha\} \models \beta$ וגם $\Gamma \cup \{\neg\alpha\} \models \beta$ אזי $\Gamma \models \beta$.

4. אם $\Gamma \cup \{\neg\alpha) \models \beta$ וגם $\Gamma \cup \{\neg\alpha) \models \neg\beta$ אזי $\Gamma \models \alpha$. נוכיח:
תהי v, אם $v \models \Gamma$ אזי לא ייתכן $v \models \neg\alpha$ כי אחרת, מההנחה נקבל כי $v \models \beta, (\neg\beta)$, לכן אם $v \models \Gamma$ אזי $v \models \alpha$.

5. אם $\Gamma \cup \{\neg\alpha\} \models \alpha$ אזי $\Gamma \models \alpha$.

6. אם $\alpha \equiv \beta$ אזי $\{\alpha\} \models \beta$.

7. $\models (\alpha \to \beta)$ אם"ם $\{\alpha\} \models \beta$.

8. $\{\alpha_1, \ldots, \alpha_n\}$ ספיקה אם"ם $\alpha_1 \wedge \cdots \wedge \alpha_n$ ספיק.

9. אם $\Gamma_1 \subseteq \Gamma_2$ ו־$\Gamma_1 \models \alpha$ אזי $\Gamma_2 \models \alpha$.

3.1 הצבות

נשים לב שישנם ביטויים, כגון $(\alpha \wedge \beta)$ ו־$(P_1 \wedge P_2)$ שיש ביניהם דימיון, בדוגמא זו, אם נחשוב על α כ־ P_1, ו־β כ־P_2 אז זהו אותו הביטוי. החלפת פסוק אטומי בנוסחא נקראת הצבה.

הגדרה 3.1 תהיינה φ, α נוסחאות ו־P_1 פסוק אטומי, נגדיר כעת את $\varphi(\alpha/P_1)$ על ידי: אם φ הוא פסוק אטומי, אזי

$$\varphi(a/P_1) = \begin{cases} \alpha & \varphi = P_1 \\ \varphi & \varphi \neq P_1 \end{cases}$$

אם $\varphi = (\neg\psi)$ אזי

$$\varphi(\alpha/P_1) = (\neg\psi(\alpha/P_1))$$

ואם $\varphi = (\psi \ op \ \gamma)$ אזי

$$\varphi(\alpha/P_1) = (\psi(\alpha/P_1) \ op \ \gamma(\alpha/P_1))$$

טענה 3.2 לכל $\varphi, \alpha \in WFF$ מתקיים כי $\varphi(\alpha/P_1) \in WFF$

הגדרה 3.3 (לא פורמלית) $\varphi(\alpha_1/P_1,\dots\alpha_n/P_n)$, בסיס: פסוק אטומי, נגדיר באופן דומה להגדרה הקודמת (3.1):

$$\varphi(\alpha_1/P_1,\dots\alpha_n/P_n)=\begin{cases}\alpha_1 & \varphi=P_1\\ \alpha_2 & \varphi=P_2\\ \vdots & \vdots\\ \alpha_n & \varphi=P_n\\ \varphi & otherwise\end{cases}$$

נשים לב כי נחוצה לנו הגדרה שונה עבור הצבה סימולטנית של מספר פסוקים שונים. לדוגמא, אם

$$\varphi=P_1\,,\,\alpha_1=P_2\,,\,\alpha_2=P_3$$

אז לפי ההצבה ב־3.3 נקבל:

$$\varphi(\alpha_1/P_1,\alpha_2/P_2)=\alpha_1=P_2$$

ואילו

$$\big(\varphi(\alpha_1/P_1)\big)(\alpha_2/P_2)=\alpha_2=P_3$$

וקיבלנו תוצאות שונות, מכאן שאין שקילות בין ההצבה שהגדרנו ב־3.3 להצבות חוזרות כפי שהוגדרו ב־3.1! בהצבות מרובות נשתמש רק בהגדרה 3.3

כעת, נשאל את עצמנו מה הקשר בין ערך האמת של $\varphi(\alpha_1/P_1)$ לזה של φ?

בהנתן השמה v נגדיר השמה חדשה v' על ידי:

$$v'(P_1)=\begin{cases}\overline{v}(\alpha_1) & i=1\\ v(P_i) & i\neq 1\end{cases}$$

טענה 3.4 עבור השמה v וההשמה שהגדרנו v', מתקיים כי $\overline{v}'(\varphi)=\overline{v}(\varphi(\alpha_1/P_1))$.

הוכחה: נוכיח באינדוקציית מבנה. נגדיר $Y=\{\psi\big|\overline{v}'(\psi)=\overline{v}(\psi(\alpha_1/P_1)\}$;

<u>בסיס:</u> ψ הוא פסוק אטומי, וישנם שני מקרים אפשריים:

אם $\psi=P_1$, אז:

$$\overline{v}'(\psi)=\overline{v}'(P_1)=v'(P_1)=\overline{v}(\alpha_1)$$

כאשר השיוויון הראשון נובע מכך ש־$\psi=P_1$, השני מהגדרת $\overline{v}'$ והשלישי מהגדרת v'. ונשים לב כי $\overline{v}(\psi(\alpha_1/P_1))=\overline{v}(\alpha_1)$.

אם $\psi\neq P_1$ אז:

$$\overline{v}'(\psi)=v'(\psi)=v(\psi)$$

ומכוון ש־$\psi(\alpha_1/P_1)=\psi\Rightarrow\overline{v}(\psi(\alpha_1/P_1))=\overline{v}(\psi)=v(\psi)$.

נוכיח סגירות:

יהיו $\gamma,\delta\in Y$, אז נוכיח כי $(\neg\gamma)\in Y$ ו־ $(\gamma\ op\ \delta)\in Y$.

$$\begin{array}{rcl}\overline{v}'(\gamma\ op\ \delta) & = & TT_{op}(\overline{v}'(\gamma),\overline{v}'(\delta))\\ (\gamma\ op\ \delta)(\alpha/P_1) & = & (\gamma(\alpha/P_1)\ op\ \delta(\alpha/P_1))\\ & \Downarrow & \\ \overline{v}((\gamma\ op\ \delta)(\alpha/P_1)) & = & \overline{v}(\gamma(\alpha/P_1)\ op\ \delta(\alpha/P_1))=\\ & = & TT_{op}\big(\overline{v}(\gamma(\alpha/P_1),\overline{v}(\delta(\alpha/P_1))\big)\end{array}$$

■

מסקנה 3.5 אם φ הוא טאוטולוגיה, אז כך גם $\varphi(\alpha_1/P_1,\dots,\alpha_n/P_n)$ לכל $\alpha_1\dots,\alpha_n\in WFF$.

3.2 צורות נורמליות (Normal Forms)

הגדרה 3.6 נגדיר את הצורה הנורמלית NNF (Negation Normal Form) באופן אינדוקטיבי כסגור של הבסיס $B=\{P_i|i\in\mathbb{N}\}\cup\{(\neg P_i)\big|i\in\mathbb{N}\}$, והפעולות $F=\{f_\wedge,f_\vee\}$.

טענה 3.7 לכל $\alpha\in WFF$ קיים $\alpha'\in NNF$ כך ש־ $\alpha\equiv\alpha'$.

הוכחה: את טענה זו הוכחנו כאשר הוכחנו כי $\{\wedge,\vee,\neg\}$ היא קבוצת קשרים שלמה, כלומר קיים β המכיל רק את הקשרים $\vee,\wedge,\neg$, כך ש־$\beta\equiv\alpha$, וראינו שניתן לקחת β מהצורה $\bigvee_{i=1}^{2^n}\varphi_i$ כאשר φ_i מהצורה $p_1\wedge\neg p_2\wedge\neg p_3...$ - בפרט β בצורת NNF. ■

הגדרה 3.8 נגדיר את $Conj$ להיות הסגור של הבסיס $B=\{P_i|i\in\mathbb{N}\}\cup\{(\neg P_i)\big|i\in\mathbb{N}\}$ עם הפעולה $F=f_\wedge$.

הגדרה 3.9 נגדיר את הצורה הנורמלית DNF (Disjunctive Normal Form) להיות הסגור של הבסיס $Conj$ עם הפעולה $F=\{f_\vee\}$.

טענה 3.10 לכל $\alpha\in WFF$ קיים $\beta\in DNF$ כך ש־ $\alpha\equiv\beta$.

הגדרה 3.11 נגדיר את $Disj$ להיות הסגור של הבסיס $B=\{P_i|i\in\mathbb{N}\}\cup\{(\neg P_i)\big|i\in\mathbb{N}\}$ עם הפעולה $F=\{f_\vee\}$.

הגדרה 3.12 נגדיר את הצורה נורמלית CNF (Conjunctive Normal Form) כסגור של הבסיס $Disj$ עם הפעולה $F=\{f_\wedge\}$.

טענה 3.13 לכל $\alpha\in WFF$ קיים $\beta\in CNF$ כך ש־ $\alpha\equiv\beta$.

הוכחה: לפי משפט ה־DNF, קיים פסוק γ כך ש־$\gamma\in DNF$ ו־$\neg\alpha\equiv\gamma$. כיוון ש־$\gamma\in DNF$, יש פסוקים $\varphi_1,...,\varphi_k\in Conj$, כך ש־

$$\gamma\equiv\varphi_1\vee...\vee\varphi_k$$

לפי חוקי דה־מורגן ושקילות לוגית

$$\neg\gamma\equiv\neg\varphi_1\wedge...\wedge\neg\varphi_k$$

וגם $\neg\varphi_i\in Disj$ - אז נקבל את הדרוש. ■

הערה 3.14 ניתן לשאול מספר שאלות אלגוריתמיות על ביטויים אלו:
בהנתן פסוק α בעל n משתנים, האם הוא ספיק? ניתן לעבור על 2^n ההצבות הקיימות ולבדוק אותן, השאלה הנשאלת האם יש אפשרות יותר טובה? ($NP=P$?)
כמו כן, בהנתן פסוק α, איך מוצאים פסוק שקול לו α' ב־ $NNF/DNF/CNF$?
מה הסיבוכיות של מציאת DNF מינימלי לפסוק α?

4 הוכחה בתחשיב הפסוקים

4.1 הגדרות וסימונים

באופן אבסטרקטי מערכת הוכחה מורכבת מהבאים:

1. אלפבית (אצלנו הפסוקים $\{P_i\big|i\in\mathbb{N}\}$ והפעולות $\{\wedge\ ,\ \vee\ ,\ \neg\ ,\ \rightarrow\ ,\ \leftrightarrow\}$).
2. נוסחאות מעל האלפבית (אצלנו ה־WFF).
3. קבוצת נוסחאות הנקראות אקסיומות A.
4. כללי היסק F.

פסוק φ הוא יכיח מקבוצת הנחות Γ, אם הוא שייך לסגור של הקבוצה $\Gamma\cup A$ עם הפעולות ב־F.
הוכחה של פסוק φ מהנחות Γ: הצגת סדרת יצירה של φ בשביל להראות שהוא בסגור הנ"ל.

סימונים: עבור מערכת הוכחה S, נסמן $\Gamma \underset{s}{\vdash} \varphi$ אם φ יכיח (ניתן להוכחה) מ־Γ במערכת S.
כמו כן נאמר כי φ משפט של S אם $\underset{s}{\vdash} \varphi$ (כלומר לא נדרשות הנחות נוספות Γ).

4.1.1 תכונות פשוטות של מערכת הוכחה

1. **מונוטוניות:** אם $\Delta \underset{s}{\vdash} \varphi$ ו־$\Delta \subseteq \Gamma$ אזי $\Gamma \underset{s}{\vdash} \varphi$.
2. **קומפקטיות:** אם $\Gamma \underset{s}{\vdash} \varphi$ אז יש $\Delta \subseteq \Gamma$, Δ סופית כך ש־$\Delta \underset{s}{\vdash} \varphi$.
3. **טרנזיטיביות:** אם $\Delta \underset{s}{\vdash} \varphi$ ולכל $\alpha \in \Delta$ מתקיים כי $\Gamma \underset{s}{\vdash} \alpha$ אזי $\Gamma \underset{s}{\vdash} \varphi$.
רעיון ההוכחה: בסדרת היצירה של φ מ־Δ נחליף כל הנחה מ־Δ בסידרת היצירה שלה מ־Γ.

4.2 מערכת הוכחה לתחשיב הפסוקים (Hilbert Propositional Calculus- HPC)

(מערכת זו היא ואריציה על המערכת של מנדלסון־פרגה)
נגדיר את מערכת זו על ידי:

1. אלפבית: הסגור של הבסיס $\{P_i | i \in \mathbb{N}\}$ עם הפעולות $\{\neg\ ,\ \to\ ,\ (\ ,\ )\}$
2. נוסחאות $WFF_{\{\neg,\to\}}$
3. אקסיומות A:

$$A_1: \quad \alpha \to (\beta \to \alpha)$$
$$A_2: \quad (\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$$
$$A_3: \quad (\neg\beta \to \neg\alpha) \to (\alpha \to \beta)$$

4. כללי היסק F: כוללים את Modus Ponens (כלל הניתוק)

$$MP\left((\alpha \to \beta), \alpha\right) = \beta$$
$$MP \quad : \quad \frac{(\alpha \to \beta)\ ,\ \alpha}{\beta} = \frac{\text{already proven}}{\text{formula from MP}}$$

כלומר אם ידוע כי $(\alpha \to \beta)$ וגם α נכון, אזי ניתן להסיק כי β נכון.

הרצאה 4 - 29.3.15

מהי הוכחה? כל נוסחה בהוכחה: אקסיומה, הנחה או מתקבלת מאחד מכללי ההיסק.

הגדרה 4.1 משפט ב־HPC: כל פסוק α כך ש־

$$\underset{HPC}{\vdash} \alpha$$

באופן אחר: בסיס: אקסיומות, פעולה: MP, סגור: משפטים של HPC.

דוגמא:[5]

$$\underset{HPC}{\vdash} (\alpha \to \alpha)$$

$$A_1: \alpha \to ((\alpha \to \alpha) \to \alpha) \tag{1}$$
$$A_2: (\alpha \to ((\alpha \to \alpha) \to \alpha)) \to ((\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)) \tag{2}$$
$$MP(1,2): ((\alpha \to (\alpha \to \alpha)) \to (\alpha \to \alpha)) \tag{3}$$
$$A_1: \alpha \to (\alpha \to \alpha) \tag{4}$$
$$MP: \alpha \to \alpha \tag{5}$$

[5] נסמן $MP(i,j)$ ביצוע הפעולה MP על שורות i ו־j

דוגמא: לכל α,β,

$$\underset{HPC}{\vdash} ((\neg\alpha) \to (\alpha \to \beta))$$

$$\begin{aligned}
A_3 &: \underbrace{(\neg\beta \to \neg\alpha) \to (\alpha \to \beta)}_{E} && (1)\\
A_1 &: E \to (\neg\alpha \to E) && (2)\\
MP(1,2) &: (\neg\alpha \to E) && (3)\\
A_2 &: \left(\underbrace{\neg\alpha}_{x} \to \underbrace{\overbrace{(\neg\beta \to \neg\alpha) \to (\alpha \to \beta)}^{E}}_{(y\to z)}\right) \to \left(\underbrace{(\neg\alpha \to (\neg\beta \to \neg\alpha))}_{(x\to y)} \to \underbrace{(\neg\alpha \to (\alpha \to \beta))}_{(x\to z)}\right) && (4)\\
MP(3,4) &: (\neg\alpha \to (\neg\beta \to \neg\alpha)) \to (\neg\alpha \to (\alpha \to \beta)) && (5)\\
A_1 &: \neg\alpha \to (\neg\beta \to \neg\alpha) && (6)\\
MP(5,6) &: \neg\alpha \to (\alpha \to \beta) && (7)
\end{aligned}$$

דוגמא:[6]

$$\{\neg\alpha\} \vdash (\alpha \to \beta)$$

הוכחה: הוכחה 1 (לעצלנים):
ראינו $\vdash (\neg\alpha \to (\alpha \to \beta))$. נכתוב את ההוכחה שוב. אז נוסיף $\neg\alpha$ (הנחה) ולפי MP $(\alpha \to \beta)$

■

הוכחה: הוכחה 2:

$$\begin{aligned}
A_1 &: && \neg\alpha \to (\neg\beta \to \neg a) && (1)\\
\text{assumption} & && \neg\alpha && (2)\\
MP(1,2) &: && (\neg\beta \to \neg\alpha) && (3)\\
A_3 &: && (\neg\beta \to \neg\alpha) \to (\alpha \to \beta) && (4)\\
MP(3,4) &: && \alpha \to \beta && (5)
\end{aligned}$$

■

מסקנה 4.2 אם $\vdash \neg\alpha$, אזי לכל β: $\{\alpha\} \vdash \beta$

הוכחה: ראינו ש־$\vdash \neg\alpha \to (\alpha \to \beta)$ ונתון $\vdash \neg\alpha$, אז לפי MP $\vdash (\alpha \to \beta)$ כלומר $\{\alpha\} \vdash \beta$. ■

4.3 משפט הדדוקציה

משפט 4.3 לכל קבוצת פסוקים $\Gamma \subset WFF_{\{\neg,\to\}}$, ולכל זוג פסוקים $\alpha,\beta \in WFF_{\{\neg,\to\}}$, מתקיים:
$\Gamma \underset{HPC}{\vdash} (\alpha \to \beta)$ אם ורק אם $\Gamma \cup \{\alpha\} \underset{HPC}{\vdash} \beta$

הוכחה: $\Leftarrow$: נניח $\Gamma \vdash (\alpha \to \beta)$. ממונוטוניות $\Gamma \cup \{\alpha\} \vdash (\alpha \to \beta)$. α הנחה מתוך $\Gamma \cup \{\alpha\}$ ולפי MP: β.
$\Rightarrow$: ההוכחה באינדוקציית מבנה.

$$Y = \left\{\varphi \in WFF_{\{\neg,\to\}} \mid \Gamma \vdash (\alpha \to \varphi)\right\}$$

[6] נשתמש ב־$\vdash$, ואם לא נאמר אחרת אז מתכוונים ל־$\underset{HPC}{\vdash}$

סימון: עבור קבוצת נוסחאות Σ, נסמן $Ded(\Sigma) = \{\psi \mid \Sigma \vdash \psi\}$. נרצה להוכיח ש־$Y$ $Ded(\Gamma \cup \{\alpha\}) \subset Y$.
כזכור $Ded(\Sigma)$ היא קבוצה סגורה; בסיס: אקסיומות, הנחות. פעולה: MP. נראה כי האקסיומות וכן $\Gamma \cup \{\alpha\}$ נמצאים ב־Y. תהי ψ אקסיומה או נוסחה מ־Γ. צ"ל: $\Gamma \vdash (\alpha \to \psi)$:

$$\begin{aligned} A_1: &\quad \psi \to (\alpha \to \psi) \\ \text{axiom or assumption} &\quad \psi \\ MP: &\quad (\alpha \to \psi) \end{aligned}$$

סגירות ל־MP: נניח $\gamma \in Y$, $(\gamma \to \delta)$. צ"ל: $\delta \in Y$.
ידוע ש־$\Gamma \vdash (\alpha \to \gamma)$, $\Gamma \vdash \alpha \to (\gamma \to \delta)$ וצ"ל: $\Gamma \vdash (\alpha \to \delta)$

$$\begin{aligned} A_2: &\quad (\alpha \to (\gamma \to \delta)) \to ((\alpha \to \gamma) \to (\alpha \to \delta)) && (1) \\ \text{known} &\quad \Gamma \vdash \alpha \to (\gamma \to \delta) && (2) \\ MP(1,2): &\quad (\alpha \to \gamma) \to (\alpha \to \delta) && (3) \\ \text{known} &\quad \Gamma \vdash (\alpha \to \gamma) && (4) \\ MP(3,4): &\quad (\alpha \to \delta) && (5) \end{aligned}$$

לכן ממשפט האינדוקציה נקבל $Ded(\Gamma \cup \{\alpha\}) \subset Y$ כדרוש. ■

דוגמא: לכל פסוק $\alpha \in WFF_{\{\neg,\to\}}$ מתקיים $\vdash (\neg\neg\alpha \to \alpha)$
הוכחה: לפי משפט הדדוקציה, די להוכיח $\{\neg\neg\alpha\} \vdash \alpha$. הראינו כבר שלכל γ, δ מתקיים

$$\vdash \neg\gamma \to (\gamma \to \delta)$$

ובפרט,

$$\begin{aligned} &\quad \vdash \neg(\neg\alpha) \to (\neg\alpha \to \neg\neg\neg\alpha) && (1) \\ \text{assumption} &\quad \neg\neg\alpha && (2) \\ MP(1,2): &\quad \neg\alpha \to \neg\neg\neg\alpha && (3) \\ A_3: &\quad (\neg\alpha \to \neg\neg\neg\alpha) \to (\neg\neg\alpha \to \alpha) && (4) \\ MP(3,4): &\quad \neg\neg\alpha \to \alpha && (5) \\ &\quad \Gamma \vdash \neg\neg\alpha \to \alpha && (6) \end{aligned}$$

■

דוגמא: $\vdash (\beta \to \neg\neg\beta)$ לכל β.
הוכחה: תרגיל. ■

4.4 משפט הנאותות ל־HPC

משפט 4.4 משפט הנאותות ל־HPC: לכל קבוצת פסוקים $\Gamma \subset WFF_{\{\neg,\to\}}$ ולכל $\alpha \in WFF_{\{\neg,\to\}}$, אם

$$\Gamma \vdash \alpha$$

אז

$$\Gamma \vDash \alpha$$

מסקנה 4.5 אם Γ ספיקה, אז לא ניתן להוכיח סתירות מ־Γ.

הוכחה: באינדוקציית מבנה;

$$Y = \{\varphi \mid \Gamma \vDash \varphi\}$$

רוצים להראות כי:

$$Ded(\Gamma) \subset Y$$

בסיס: תהי φ אקסיומה. צ"ל: $\varphi \in Y$, דהיינו $\Gamma \vDash \varphi$.

טענה 4.6 כל האקסיומות הן טאוטולוגיות. (בוודאי)

נניח $\varphi \in Y$, $\varphi \to \psi$. נראה ש־$\psi \in Y$. נתון: $\Gamma \vDash (\varphi \to \psi)$, $\Gamma \vDash \varphi$. תהי v השמה כך ש־$v \vDash \Gamma$; מהנתון $v \vDash (\varphi \to \psi)$ ו־$v \vDash \varphi$ אז לפי $TT_{\to}$ חייב להתקיים $v \vDash \psi$. ■

משפט 4.7 משפט הדיכוטומיה (הוכחה לפי מקרים):
לכל קבוצת פסוקים $\Gamma \subset WFF_{\{\neg,\to\}}$ ולכל $\alpha, \beta \in WFF_{\{\neg,\to\}}$, אם

$$\Gamma \cup \{\alpha\} \vdash \beta$$

וגם

$$\Gamma \cup \{\neg\alpha\} \vdash \beta$$

אזי

$$\Gamma \vdash \beta$$

למה 4.8 לכל x, y, z, Γ, אם $\Gamma \vdash (y \to z)$ וגם $\Gamma \vdash (x \to y)$, אזי $\Gamma \vdash (x \to z)$

הוכחה: (של הלמה) בלי משפט הדדוקציה:

$$\begin{array}{rll} A_2: & (x \to (y \to z)) \to ((x \to y) \to (x \to z)) & (1) \\ A_1: & (y \to z) \to (x \to (y \to z)) & (2) \\ & \Gamma \vdash (y \to z) & (3) \\ MP: & x \to (y \to z) & (4) \\ MP: & (x \to y) \to (x \to z) & (5) \\ & \Gamma \vdash (x \to y) & (6) \\ MP: & (x \to z) & (7) \end{array}$$

הוכחה נוספת לפי משפט הדדוקציה: די להוכיח $\Gamma \cup \{x\} \vdash z$, אז:

$$\begin{array}{rcl} \Gamma & \vdash & x \to y \\ \text{assumptions} & & x \\ & & y \\ \Gamma & \vdash & y \to z \\ MP: & & z \end{array}$$

■

הוכחה: הוכחת משפט הדיכוטומיה: לפי משפט הדדוקציה הנתון שקול ל־

$$\Gamma \vdash (\alpha \to \beta)$$

וגם

$$\Gamma \vdash (\neg\alpha \to \beta)$$

הראינו (כתרגיל, בדוגמה למשפט 4.3)

$$\vdash (\beta \to \neg\neg\beta)$$

לפי הלמה

$$\Gamma \vdash (\neg\alpha \to \neg\neg\beta)$$

ולפי A_3 ו־MP נקבל

$$\Gamma \vdash (\neg\beta \to \alpha)$$

לפי הלמה עם $x = \neg\beta, y = \alpha, z = \beta$ נקבל

$$\Gamma \vdash (\neg\beta \to \beta)$$

ואז:

$$\begin{array}{rll}
\text{ex. above} & \vdash (\neg\beta \to (\beta \to \neg(\neg\beta \to \beta))) & (1)\\
A_2: & (\neg\beta \to (\beta \to \neg(\neg\beta \to \beta))) \to ((\neg\beta \to \beta) \to (\neg\beta \to \neg(\neg\beta \to \beta))) & (2)\\
MP(1,2): & (\neg\beta \to \beta) \to (\neg\beta \to \neg(\neg\beta \to \beta)) & (3)\\
MP: & \neg\beta \to \neg(\neg\beta \to \beta) & (4)\\
A_3: & (\neg\beta \to \neg(\neg\beta \to \beta)) \to ((\neg\beta \to \beta) \to \beta) & (5)\\
MP: & (\neg\beta \to \beta) \to \beta & (6)\\
MP: & \beta & (7)
\end{array}$$

■

4.5 משפט השלמות ל־HPC

משפט 4.9 לכל $\Gamma \subset WFF_{\{\neg,\to\}}$ ולכל $\alpha \in WFF_{\{\neg,\to\}}$, אם

$$\Gamma \vDash \alpha$$

אזי

$$\Gamma \underset{HPC}{\vdash} \alpha$$

ניתן לנסח את שני המשפטים יחד:

משפט 4.10 משפט השלמות והנאותות: $\Gamma \vDash \alpha$ אם ורק אם $\Gamma \underset{HPC}{\vdash} \alpha$.

משפט 4.11 ניסוח שקול למשפט השלמות:
אם $\Gamma \nvdash \alpha$ אז $\Gamma \nvDash \alpha$
במילים: אם לא ניתן להוכיח את α מתוך Γ אז יש השמה v כך ש־$v \vDash \Gamma$ (מספקת) אבל $v \nvDash \alpha$

אסטרטגיית ההוכחה: נתחיל מהעובדה $\Gamma \nvdash \alpha$ ונבנה v כנ"ל. אנחנו רוצים להגיע למצב בו ל־Γ יש "בעיה" על כל פסוק אטומי.

4.6 קבוצה עקבית

הגדרה 4.12 קבוצת פסוקים Γ נקראת עקבית אם יש פסוק φ כך ש־$\Gamma\nvdash\varphi$

טענה 4.13 Γ לא עקבית אם ורק אם קיים פסוק φ כך ש־$\Gamma\vdash\varphi$ וגם $\Gamma\vdash\neg\varphi$.

הוכחה:

$$
\begin{array}{llll}
(1) & & \vdash\neg\varphi\to(\varphi\to\beta) & \text{ex. above} \\
(2) & \Gamma & \vdash\neg\varphi & \\
(3) & \Gamma & \vdash\beta & MP(1,2)
\end{array}
$$

כלומר לכל β מתקיים $\Gamma\vdash\beta$. ■

הרצאה 5 - 12.4.15

הערה 4.14 מה הקשר בין עקביות למשפט השלמות:

- נניח כי $\Gamma\nvDash\alpha$
- נקבל כי $\Gamma\cup\{\neg\alpha\}$ עקבית, כי אם $\Gamma\cup\{\neg\alpha\}\vdash\alpha$ אז כיוון ש־$\Gamma\cup\{\alpha\}\vdash\alpha$ ונקבל מדיכוטומיה $\Gamma\vdash\alpha$.

משפט 4.15 כל קבוצה עקבית היא ספיקה
בפרט יש השמה v שמקיימת: $v\vDash\Gamma$, $v\vDash\neg\alpha$ (או $\bar{v}(\alpha)=f$) ובפרט $\Gamma\nvDash\alpha$

אנחנו רוצים של־Γ תהיה "דעה" על כל פסוק אטומי (האם לתת לו ערך t או f?). אם לכל פסוק אטומי P היה מתקיים $P\in\Gamma$ או $\neg P\in\Gamma$ ואז בוודאי ל־P הייתה "דעה" עליו.
רעיון ההוכחה: "ננפח" את Γ כך שנישאר עם קבוצה עקבית וגם לכל P, או $P\in\Gamma$ או $\neg P\in\Gamma$.

הגדרה 4.16 קבוצה עקבית מקסימלית היא קבוצת פסוקים X, עקבית ולא קיימת קבוצה עקבית Y כך ש־$X\subsetneq Y$.

טענה 4.17 Γ עקבית אם ורק אם כל תת קבוצה סופית של Γ גם עקבית.

הוכחה: $\Leftarrow$: ברור. אם $\Gamma\nvdash\alpha$ אז α אינו יכיח מאף תת קבוצה סופית Γ.
$\Rightarrow$: נניח כי Γ אינה עקבית ונראה שיש תת קבוצה סופית $\Gamma'\subset\Gamma$ שאינה עקבית. כיוון ש־Γ אינה עקבית יש β כך ש־$\Gamma\vdash\beta$ וגם $\Gamma\vdash\neg\beta$.
כיוון שהוכחה היא סופית, בהוכחה של β ובהוכחה של $\neg\beta$ השתמשנו במספר סופי של הנחות מתוך Γ. תהי $\Gamma'\subset\Gamma$ תת קבוצה סופית המכילה את ההנחות הנ"ל. אזי

$$\Gamma'\vdash\beta$$

וגם

$$\Gamma'\vdash\neg\beta$$

(אותה הוכחה כמו $\Gamma\vdash\beta$, $\Gamma\vdash\neg\beta$ מקודם)
לכן, לפי טענה שהוכחנו, Γ' אינה עקבית. ■

טענה 4.18 אם X עקבית מקסימלית ו־$X\vdash\varphi$, אזי $\varphi\in X$.

הוכחה: נביט בקבוצה $Y=X\cup\{\varphi\}$. בוודאי $X\subset Y$. לכן, אם Y עקבית אז ממקסימליות של X מתקיים $X=Y$ ובפרט $\varphi\in X$. אכן, נראה כי $Y\nvdash\neg\varphi$.
אם

$$X\cup\{\varphi\}=Y\vdash\neg\varphi$$

כיוון ש־

$$X\cup\{\neg\varphi\}\vdash\neg\varphi$$

ממשפט הדיכוטומיה $X\vdash\neg\varphi$ בגלל שהנחנו $X\vdash\varphi$, לכן X לא עקבית - בסתירה. ■

טענה 4.19 לכל קבוצה עקבית מקסימלית X ולכל פסוק φ מתקיים $\varphi \in X$ או $\neg\varphi \in X$.

הוכחה: אם $X \cup \{\varphi\}$ עקבית אז ממקסימליות X מתקיים $\varphi \in X$ (כמו שכבר ראינו). אם $X \cup \{\varphi\}$ לא עקבית אז בפרט $X \cup \{\varphi\} \vdash \neg\varphi$ ומכאן נובע (ראינו כבר בעזרת משפט הדיכוטומיה) ש-$X \vdash \neg\varphi$. מהטענה הקודמת נובע ש-$\neg\varphi \in X$. ■

טענה 4.20 תהי X עקבית מקסימלית. אזי לכל α, β פסוקים מתקיים $X \vdash (\alpha \to \beta)$ אם ורק אם $\neg\alpha \in X$ או $\beta \in X$.

הוכחה: $\Leftarrow$: לפי טענה 4.19 קודמת $\alpha \in X$ או $\neg\alpha \in X$. אם $\neg\alpha \in X$ אז סיימנו.
אם $\alpha \in X$ אזי

$$\begin{array}{rcl} X & \vdash & (\alpha \to \beta) \\ \text{assumption} & & \alpha \end{array}$$

מ-MP נקבל:

$$X \vdash \beta$$

ולפי טענה 4.18 קודמת $\beta \in X$.
$\Rightarrow$: מקרה ראשון: $\neg\alpha \in X$. ראינו

$$\begin{array}{rcl} & \underset{HPC}{\vdash} & \neg\alpha \to (\alpha \to \beta) \\ \text{assumption} & & \neg\alpha \end{array}$$

וע"י MP נקבל

$$X \vdash (\alpha \to \beta)$$

מקרה שני: $\beta \in X$

$$\begin{array}{rl} A_1: & \beta \to (\alpha \to \beta) \\ \text{assumption} & \beta \\ MP: & (\alpha \to \beta) \end{array}$$

וקיבלנו

$$X \vdash (\alpha \to \beta)$$

■

טענה 4.21 כל קבוצה עקבית מוכלת בקבוצה עקבית מקסימלית.

הוכחה: כיוון ש-WFF בת מניה, ניתן למנות את פסוקי WFF:

$$WFF = \{\varphi_1, \varphi_2, \varphi_3, ...\}$$

נניח כי X קבוצה עקבית. נסמן $X_0 = X$. נגדיר באופן אינדוקטיבי:

$$X_n = \begin{cases} X_{n-1} \cup \{\varphi_n\} & X_{n-1} \cup \{\varphi_n\} \text{ is consistent} \\ X_{n-1} \cup \{\neg\varphi_n\} & else \end{cases}$$

נגדיר כעת

$$Y = \bigcup_{n \in \mathbb{N}} X_n$$

ברור כי $X = X_0 \subset Y$. נראה כי Y עקבית מקסימלית. אם Y אינה עקבית, אז יש $Y' \subset Y$ סופית שאינה עקבית. בפרט יש X_n שאינה עקבית (כי כל $Y' \subset Y$ סופית מוכלת באיזשהו X_n).

למה 4.22 נראה ש־X_n עקבית לכל n, באינדוקציה על n. $n=0$ נתון, נניח ש־X_{n-1} עקבית.

הוכחה: (של הלמה) מקרה ראשון: $X_n = X_{n-1} \cup \{\varphi_n\}$ מהגדרת X_n נקבל כי X_n עקבית.
מקרה שני: $X_{n-1} \cup \{\varphi_n\}$ אינה עקבית. אם גם $X_{n-1} \cup \{\neg\varphi_n\}$ אינה עקבית אז ממשפט הדיכוטומיה נקבל ש־ X_{n-1} אינה עקבית בסתירה. לכן גם במקרה השני $X_n = X_{n-1} \cup \{\neg\varphi_n\}$ עקבית. ∎

הראינו כי Y עקבית ונראה כי היא עקבית מקסימלית. מההגדרה ברור שלכל φ מתקיים $\varphi \in Y$ או $\neg\varphi \in Y$ וכפי שכבר ראינו זה גורר ש־Y עקבית מקסימלית. ∎

הערה 4.23 טיעון שחזור במשך היום: אם $Y \subset Z$, Z עקבית. יהי $\varphi \in Z$. אם $\varphi \notin Y$ אז $\neg\varphi \in Y$ בפרט $\neg\varphi \in Z$ לכן $Z \vdash \varphi, \neg\varphi$ ואז Z לא עקבית בסתירה. לכן $\varphi \in Y$ ו־$Z \subset Y$.

טענה 4.24 כל קבוצה עקבית מקסימלית ספיקה.

הוכחה: תהי X קבוצה עקבית מקסימלית. נגדיר השמה v באופן הבא:

$$v\left(P_i\right) = \begin{cases} t & P_i \in X \\ f & \neg P_i \in X \end{cases}$$

ונראה כי $v \vDash X$. (v מוגדרת היטב כי X עקבית מקסימלית)
נגדיר קבוצת פסוקים T:

$$T = \{\varphi \mid (\varphi \in X \text{ and } \bar{v}(\varphi) = t) \text{ or } (\varphi \notin X \text{ and } \bar{v}(\varphi) = f)\}$$

נוכיח באינדוקציית מבנה כי $WFF \subset T$.
<u>בסיס:</u> פסוקים אטומיים - יהי P_i כלשהו. אם $P_i \in X$ אז $\bar{v}(P_i) = v(P_i) = t$ ולכן $P_i \in T$. אם $P_i \notin X$ אז $\neg P_i \in X$ ונקבל כי $\bar{v}(P_i) = f$ ולכן, שוב $P_i \in T$.
נראה כי T <u>סגורה</u>. יהיו $\alpha, \beta \in T$. צ"ל: $\neg\alpha \in T$ וגם $(\alpha \to \beta) \in T$. נראה כי $\neg\alpha \in T$. נפריד למקרים:

1. אם $\alpha \in X$, $\bar{v}(\alpha) = t$. אז $\neg\alpha \notin X$ (X עקבית). $\bar{v}(\alpha) = t$ ייתן ש־$\bar{v}\left(\neg\alpha\right) = f$. לכן קיבלנו ש־$\neg\alpha \notin X$ וגם $\bar{v}\left(\neg\alpha\right) = f$ ומהגדרת T, $\neg\alpha \in T$.

2. אם $\alpha \notin X$, $\bar{v}(\alpha) = f$. X מקסימלית ולכן $\neg\alpha \in X$ וגם $\bar{v}\left(\neg\alpha\right) = t$. מהגדרת T, $\neg\alpha \in T$.

כעת נראה ש־$(\alpha \to \beta) \in T$. נפריד למקרים:

1. אם $\alpha \in X$.

   (א) אם $\beta \in X$, $\bar{v}(\beta) = t$. מהטענה שהוכחנו $(\alpha \to \beta) \in X$. $\bar{v}\left(\alpha \to \beta\right) = t$ כי $\bar{v}(\alpha) = \bar{v}(\beta) = t$ ולכן $(\alpha \to \beta) \in T$.

   (ב) אם $\beta \notin X$, $\bar{v}(\beta) = f$. מהטענה שהוכחנו נקבל $(\alpha \to \beta) \notin X$, $\bar{v}(\alpha \to \beta) = f$ כי $\bar{v}(\alpha) = t$, $\bar{v}(\beta) = f$ וגם כאן $\alpha \to \beta \in T$.

2. אם $\alpha \notin X$. לכן $\neg\alpha \in X$. מהטענה שהוכחנו, $(\alpha \to \beta) \in X$ ו־$\bar{v}\left(\alpha \to \beta\right) = t$ כיוון ש־$\bar{v}(\alpha) = t$. לכן $\alpha \to \beta \in T$.

ואז $WFF \subset T$ כדרוש. ∎

מסקנה 4.25 מטענות 4.21 ו־4.24, כל קבוצה עקבית היא ספיקה.

הוכחה: של משפט השלמות ($\Gamma \vDash \alpha \Rightarrow \Gamma \vdash \alpha$)
נניח $\Gamma \nvdash \alpha$ אז $\Gamma \cup \{\neg\alpha\}$ עקבית לכן היא ספיקה. בפרט, אם $v \vDash \Gamma \cup \{\neg\alpha\}$ אז $v \vDash \Gamma$ וגם $v \nvDash \alpha$ ולכן $\Gamma \nvDash \alpha$. ∎

מסקנה 4.26 X עקבית אם ורק אם X ספיקה.

הוכחה: $\Leftarrow$: הראינו.
$\Rightarrow$: אם $v \vDash X$, יהי α עם $\bar{v}(\alpha) = f$. ממשפט השלמות נקבל כי $X \nvdash \alpha$ ולכן X עקבית. ∎

משפט 4.27 השלמות והנאותות
$X \vdash \alpha$ אם ורק אם $X \vDash \alpha$.

4.7 משפט הקומפקטיות

משפט 4.28 הקומפקטיות (תחשיב הפסוקים):
X ספיקה אם ורק אם כל תת קבוצה סופית של X ספיקה.

הוכחה: X ספיקה אם ורק אם X עקבית (הוכחנו) אם ורק אם כל תת קבוצה סופית של X עקבית (הוכחנו) אם ורק אם כל תת קבוצה סופית של X ספיקה. ∎

לכל קבוצת פסוקים X נגדיר

$$Ass\left(X\right)=\left\{ v\mid v\vDash X\right\}$$

אלו הקבוצות הסגורות שלנו.

$$Ass(X)=\bigcap_{\varphi\in X}Ass(\varphi)$$

אם X אינה ספיקה $Ass(X)=\emptyset$, אז $\bigcap_{\varphi\in X}Ass(\varphi)=\emptyset$. יש תת קבוצה $X'\subset X$ סופית שאינה עקבית.

$$\bigcap_{\varphi\in X'}Ass(\varphi)=\emptyset$$

4.7.1 שימושים

הגדרה 4.29 גרף $G=(V,E)$ הוא k־צביע אם יש פונקציה $\chi:V\to\{1,...,k\}$ כך שאם יש קשת בין v ל־u אז $\chi(v)\neq\chi(u)$.

משפט 4.30 יהי $G=(V,E)$ גרף אינסופי. אזי G 2־צביע[7] אם ורק אם כל תת גרף סופי שלו הוא 2־צביע. נניח G בן מניה.

הוכחה: נתרגם את השאלה לשאלה בתחשיב הפסוקים. נתאים פסוק אטומי לכל קודקוד ב־G.

$$V\Leftrightarrow\{P_1,P_2,...\}$$

נחשוב על הצבעים כעל הערכים t,f. לכל $e\in E$ נתאים:

$$\varphi_e=(P_i\to\neg P_j)\wedge(\neg P_i\to P_j)$$

כש־$e=(P_i,P_j)$.
$v\vDash\varphi_e$ רק אם v "צובעת היטב" את P_i ו־P_j. נסמן כעת $X=\{\varphi_e\mid e\in E\}$.
נניח שכל תת גרף סופי הוא 2־צביע ונראה שכל תת קבוצה $X'\subset X$ סופית היא ספיקה.
תהא $X'\subset X$ סופית; ניקח

$$V'=\{P_i\mid\ P_i\text{ appears in some }\alpha\in X'\}$$

הגרף המושרה על V'[8] הוא 2־צביע. לכן לכל φ ששני קדקודיו ב־V'מתקיים ש־φ צבועה היטב. נהפוך את הצביעה להשמה $(1\to t,2\to f)$ ונשים לב שההשמה מספקת כל φ_e כנ"ל ולכן את X'. ∎

Syntax		**Semantics**
X consistent	$\Leftrightarrow$	X satisfyable
$X\vdash\alpha$	$\Leftrightarrow$	$X\vDash\alpha$
$\vdash\alpha$	$\Leftrightarrow$	$\vDash\alpha$

הערה 4.31 ראינו כי X עקבית מקסימלית מסתפקת על ידי השמה יחידה.

מאידך, בהינתן השמה v נגדיר $X_v=\{\varphi\mid v\vDash\varphi\}$

טענה 4.32 X_v עקבית מקסימלית.

הרצאה 6 - 19.4.15

[7] הטענה נכונה עבור כל k

[8] שימו לב לאי ההבדלה בין V ל־$\{P_i\}$: העתקה חח"ע ועל בין שתי הקבוצות תעביר תת קבוצה ב־V לתת קבוצה מתאימה ב־$\{P_i\}$

4.8 גדירות

נאמר שקבוצת פסוקים X מגדירה את קבוצת ההשמות המספקות אותה

$$Ass(X) = \{v \mid v \vDash X\}$$

נאמר שקבוצת השמות K היא גדירה אם קיימת קבוצת פסוקים X כך ש־

$$K = Ass(X)$$

דוגמאות: הקבוצות הבאות גדירות

1. $\emptyset$
2. קבוצת כל ההשמות
3. השמות הנותנות ערך t למשתנה אחד לכל היותר
4. $K = \{v\}$

הוכחה:

1. $X = \{p \wedge \neg p\}$ סתירות
2. $X = \{p \vee \neg p\}$ טאוטולוגיות
3. $\{\neg (P_i \wedge P_j) \mid i \neq j\}$, $\{P_i \to \neg P_j \mid i \neq j\}$
4. $\{P_i \text{ or } \neg P_i \text{ according to } v(P_i) \mid i\}$

■

מה עצמת הקבוצות הגדירות? כל K גדירה היא $K = Ass(X)$, $X \subset WFF$. אז עצמת הקבוצות הגדירות $\leq 2^{\aleph_0}$. עצמת קבוצת ההשמות היא $2^{\aleph_0}$. עצמת (קבוצת החזקה) קבוצת כל תת הקבוצות של קבוצת ההשמות היא $2^{2^{\aleph_0}}$.

סימון: Ass = קבוצת כל ההשמות; $\forall P_i,\ v_t(P_i) = t$

טענה 4.33 הקבוצה

$$K_{fin} = \{v \mid v \text{ sets } t \text{ for a finite number of } P_i\text{s}\}$$

אינה גדירה.

הוכחה: תהי X קבוצת פסוקים כך ש־$K_{fin} \subset Ass(X)$. נראה שלכל X כנ"ל $v_t \vDash X$.

תהי $\Sigma = \{P_i \mid i \in \mathbb{N}\}$, נראה כי $\Sigma \cup X$ ספיקה. לפי משפט הקומפקטיות, $\Sigma \cup X$ ספיקה אם ורק אם כל תת קבוצה סופית שלה ספיקה.

תהי $\Sigma' \cup X'$ תת קבוצה סופית. נניח $\Sigma' \subset \{P_1, ..., P_n\}$ ונגדיר את v_nבאופן הבא:

$$v_n(P_i) = \begin{cases} t & 1 \leq i \leq n \\ f & n < i \end{cases}$$

נראה כי $v_n \vDash X' \cup \Sigma'$ נראה אפילו כי $v_n \vDash X \cup \Sigma'$. אכן, $v_n \in K_{fin}$; מהגדרת X, מתקיים ש־$K_{fin} \subset Ass(X)$ ובפרט $v_n \vDash X$.

מהגדרת v_n ברור גם $v_n \vDash \Sigma'$ ולכן $v_n \vDash X \cup \Sigma'$.

הראנו שכל תת קבוצה של $\Sigma \cup X$ ספיקה, ולכן היא בעצמה ספיקה. ההשמה היחידה המספקת את Σ היא v_t ולכן $v_t \vDash X$ ובפרט

$$K_{fin} \subsetneq Ass(X)$$

לכן K_{fin} אינה גדירה. ■

הגדרה 4.34 קבוצת השמות K גדירה באופן סופי אם יש X סופית כך ש־$K = Ass(X)$

משפט 4.35 התנאים הבאים שקולים:

1. K גדירה וגם K^c גדירה
2. K גדירה באופן סופי
3. K גדירה על ידי פסוק יחיד

הוכחה: $1 \Leftarrow 2$: תהיינה X, Y כך ש־

$$\begin{aligned} K &= Ass(X) \\ K^c &= Ass(Y) \end{aligned}$$

ותהא

$$\Sigma = X \cup Y$$

Σ אינה ספיקה (כי אם $v \in K$ אז $v \notin Ass(Y)$ וכנ"ל $v \in K^c$ אז $v \notin Ass(X)$)
לפי משפט הקומפקטיות קיימת $\Sigma' = X' \cup Y'$ סופית, שאינה ספיקה. נראה כי $K = Ass(X')$ וגם $Ass(Y') = K^c$.
ברור כי $K \subset Ass(X')$. נראה כי אין $v \in K^c$ כך ש־$v \models X'$. כיוון ש־$v \in K^c$, $v \models Y'$. אם גם $v \models X'$ אזי

$$v \models X' \cup Y' = \Sigma'$$

בסתירה.
לכן $K \subset Ass(X')$ ובפרט $Ass(X') = K$ לכן K גדירה באופן סופי. ■

הוכחה: $2 \Leftarrow 3$: תהי $K = Ass(X)$ כך ש־$X = \{\varphi_1, .., \varphi_n\}$ויהי

$$\varphi = \varphi_1 \wedge \varphi_2 \wedge ... \wedge \varphi_n$$

קל לראות ש־

$$Ass\left(\{\varphi\}\right) = Ass(X) = K$$

■

הוכחה: $3 \Leftarrow 1$: $K = Ass\left(\{\varphi\}\right)$ אזי $K^c = Ass\left(\{\neg\varphi\}\right)$. ■

תחשיב הפסוקים

- פסוקים אטומים יכולים לקבל t או f
- בנינו נוסחאות מורכבות בעזרת קשרים והפסוקים האטומיים (סינטקס, WFF)
- הגדרנו סמנטיקה (השמות לפסוקים אטומים והרחבה לערך אמת לכל $\varphi \in WFF$)
- מושג ההוכחה: מערכת הוכחה (HPC) לתחשיב הפסוקים
- תכונות של מערכת ההוכחה HPC: נאותות, דדוקציה, דיכוטומיה, שלמות
- אנלוגיה בין סינטקטי לסמנטי $X \vdash \alpha \Leftrightarrow X \models \alpha$
- קופמקטיות
- גדירות

אבל עדיין תחשיב הפסוקים מאוד מוגבל. מה אי אפשר לעשות בתחשיב הפסוקים?

דוגמה:

סוקרטס בן אדם - תכונה שסוקרטס מקיים אותה

כל בן אדם הוא בן תמותה - כל מי שמקיים את התכונה מקיים תכונה אחרת

לכן סוקרטס בן תמותה

דוגמה:

כל מספר טבעי גדול מ-0

הוא עוקב של מספר טבעי אחר

נרצה לתאר יחסים כאלה, ואנחנו לא יכולים לעשות זאת בתחשיב הפסוקים הרגיל.

חלק II

תחשיב היחסים / לוגיקה מסדר ראשון

באנגלית Predicate Calculus / First Order Logic

1 הגדרות ומשפטים בסיסיים

אלפבית: סימנים לוגיים המשותפים לכל השפות

1. משתנים $\{x_i \mid i \in \mathbb{N}\}$
2. סימני עזר: סוגריים),(
3. קשרים בוליאניים $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
4. כמתים $\forall, \exists$

מילון: (סיגנטורה Signature)
המילון מכיל פרמטרים המיוחדים לשפה; תת קבוצה של:

1. סימני קבוע $\{c_i \mid i \in \mathbb{N}\}$
2. סימני יחס $\{R_{n,i} \mid n, i \in \mathbb{N}\}$, כש־$R_{n,i}$ הוא סימן יחס n־מקומי
3. סימני פונקציה $\{f_{n,i} \mid i, n \in \mathbb{N}\}$ ו־$f_{n,i}$ מסמן פונקציה n־מקומית

נאמר כי מילון הוא סופי, אם יש בו מספר סופי של סימונים. נאמר שמילון הוא יחסי אם אם אינו מכיל סימני פונקציה.
האלפבית של השפה איתה עובדים מורכב מהסימונים הלוגיים המשותפים לכל השפות ומהסימנים במילון. בד"כ נסמן מילון באותיות τ, σ וכו'.

הגדרה 1.1 שם עצם (term) מעל מילון σ.
ההגדרה ברקורסיה: <u>בסיס:</u> כל x_i הוא שם עצם. כל $c \in \sigma$ גם שם עצם.
<u>פעולות:</u> לכל $f \in \sigma$ אם f פונקציה n מקומית ו־$t_1, .., t_n$ שמות עצם גם $f(t_1, ..., t_n)$ שם עצם.

משפט 1.2 הקריאה היחידה לשמות עצם:
אם t הוא שם עצם מעל מילון σ אז מתקיים בדיוק אחד מהבאים:

1. $t = x_i$ לאיזשהו משתנה x_i
2. $t = c$ לאיזשהו $c \in \sigma$
3. קיימת פונקציה יחידה $f \in \sigma$ וקיימים $t_1, .., t_k$ שמות עצם יחידים כך ש־f על k משתנים ו־

$$t = f(t_1, ..., t_k)$$

1.1 נוסחאות מעל מילון σ

הגדרה 1.3 נוסחאות אטומיות:
לכל $R \in \sigma$ סימן יחס n־מקומי ולכל $t_1, ..., t_n$ שמות עצם $R(t_1, ..., t_n)$ הוא נוסחה אטומי.

הגדרה 1.4 פעולות:

1. הפעלת קשרים של תחשיב הפסוקים: אם α, β נוסחאות אז גם
   - $(\neg\alpha)$
   - $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$
   - $(\alpha \leftrightarrow \beta)$, $(\alpha \rightarrow \beta)$

2. כמתים: אם α נוסחה ו־x משתנה, אז $(\forall x\,\alpha)$ ו־$(\exists x\,\alpha)$ נוסחאות.

הסגור של הנוסחאות האטומיות תחת הפעולות האלה הוא הנוסחאות מעל σ.

משפט 1.5 משפט הקריאה היחידה לנוסחאות מעל σ:
אם α נוסחה אז מתקיים בדיוק אחד מהבאים:

- αנוסחה אטומית: קיים $R \in \sigma$ יחיד וכו'
- $\alpha = (\neg\beta)$ β יחיד
- $a = (\beta\, op\, \gamma)$ כש־$op \in \{\wedge, \vee, \to, \leftrightarrow\}$, β, γ יחידים ו־op יחיד.
- $a = \exists x\, \beta$ כש־x, β יחידים
- $\alpha = \forall x\, \beta$ כש־x, β יחידים

דוגמאות

- $\sigma = \{c, f(), R_1(), R_2(,)\}$, x, y משתנים.
- $f(c), f(x), x, c$ שמות עצם
- $R_1(f(x))$: נוסחה אטומית
- $R_2(x, f(c))$: נוסחה אטומית
- נוסחה:

$$((\exists y\, R_1(f(y))) \to (\forall x\, R_2(f(x), c)))$$

מאידך:

- $(R_1(f(x)) \wedge f(c))$ - לא נוסחה ($f(c)$ אינו נוסחה אטומי)
- $(\forall c\, R_1(f(c)))$ - לא נוסחה כי c אינו משתנה (מכמתים רק משתנים)
- $\forall x\, R_1(x)$ - חסרים סוגריים

הערה 1.6 לשם הנוחות נשמיט סוגריים. סדר קדימויות:

1. כמתים
2. קשרים לפי סדר קדימויות בתחשיב הפסוקים

1.2 משתנים חופשיים וקשורים

נגדיר את המושגים משתנה חופשי (free) ומשתנה קשור (bound).

הגדרה 1.7 עבור שם עצם t, $FV(t)$ מוגדר באופן הבא:

- אם $t = c$ אז $FV(t) = \emptyset$
- אם $t = x$ (x משתנה) אז $FV(t) = \{x\}$
- אם $t = f(t_1, ..., t_n)$ אז $FV(t) = FV(t_1) \cup FV(t_2) \cup ... \cup FV(t_n)$

הגדרה 1.8 עבור נוסחה φ, $FV(\varphi)$ מוגדר באופן הבא:

- אם $\varphi = R(t_1, ..., t_n)$ אז $FV(\varphi) = FV(t_1) \cup ... \cup FV(t_n)$
- אם $\varphi = (\neg\alpha)$ אז $FV(\varphi) = FV(\alpha)$
- אם $\varphi = (\alpha\, op\, \beta)$ אז $FV(\varphi) = FV(\alpha) \cup FV(\beta)$
- אם $\varphi = Qx\,\alpha$ כש־$Q \in \{\forall, \exists\}$, $FV(\varphi) = FV(\alpha) \setminus \{x\}$

דוגמה:

$$FV\left(\left(\forall x\, R(x)\right)\to R_2(x)\right)=FV\left(\forall x\, R(x)\right)\cup FV\left(R_2(x)\right)=\emptyset\cup\{x\}=\{x\}$$

כי

$$FV\left(\forall x\, R(x)\right)=FV\left(R(x)\right)\setminus\{x\}=\underbrace{FV\left(x\right)}_{\{x\}}\setminus\{x\}=\emptyset$$

$$FV\left(R_2(x)\right)=FV(x)=x$$

הערה 1.9 כיוון שביטויים מהצורה

$$\left(\left(\forall x\,\varphi(x)\right)\to\alpha(x)\right)$$

"מבלבלים", נראה שלנוסחה

$$\left(\left(\forall y\,\varphi(y)\right)\to\alpha(x)\right)$$

יש אותה משמעות סמנטית. אז נוכל לשנות שם למשתנים קשורים כדי שיהיו שונים משמות המשתנים החופשיים.

הגדרה 1.10 x חופשי ב־φ אם $x\in FV(\varphi)$

הגדרה 1.11 נוסחה φ תיקרא סגורה אם $FV(\varphi)=\emptyset$

הגדרה 1.12 שם עצם t יקרא סגור אם $FV(t)=\emptyset$

1.3 מבנה

הגדרה 1.13 מבנה עבור מילון σ:
מבנה M מורכב מהאובייקטים הבאים:

1. תחום D^M קבוצה לא ריקה.
2. פירוש של סימנים מ־σ:
   (א) לכל סימן קבוע $c\in\sigma$ מתאים איבר $c^M\in D^M$
   (ב) לכל סימן יחס $R\in\sigma$ n־מקומי מתאים יחס n־מקומי מעל D^M
   $$R^M\subset\underbrace{D^M\times...\times D^M}_{n\text{ times}}$$
   (ג) לכל סימן פונקציה $f\in\sigma$ n־מקומי מתאימים פונקציה
   $$f^M\,:\,\left(D^M\right)^n\to D^M$$

ומסמנים $M=\left(D^M,C_0^M,...,f_0^M,...,R^m,...\right)$

הרצאה 7 - 26.4.15

כדי להגדיר ערכי אמת צריך לדעת את ערכי המשתנים החופשיים

הגדרה 1.14 השמה:

$$v\,:\,\{x_i\}\to D^M$$

כדי להגדיר ערכי אמת צריכים: מבנה M, השמה v.

לכל $d\in D^M$ נסמן

$$v\left({}^{d}/{}_{x_i}\right)\left(x_j\right)=\begin{cases}v(x_j) & j\neq i\\ d & j=i\end{cases}$$

1.3.1 ערך של שם עצם תחת השמה v במבנה M

אם $c_i \in \sigma$

- $s = c_i$ אז $\bar{v}(s) = c_i^M$
- $s = x_i$ אז $\bar{v}(s) = v(x_i)$

אם $s = f\left(s_1, .., s_n\right)$ כש־$f \in \sigma$, אז $\bar{v}(s) = f^M(\bar{v}(s_1), ..., \bar{v}(s_n))$

דוגמה שנעבוד איתה: $\sigma = \{c_0, c_1, f_1(,), f_2(,), R(,)\}$, $M = (\mathbb{N}, 0, 1, +, \times, \leq)$
אז נסמן $s = f_1\left(f_2\left(f_1(c_1, c_1), x_1\right) x_2\right)$, $v(x_1) = 5,\ v(x_2) = 7$

$$\begin{aligned} \bar{v}\left(f_1(c_1, c_1)\right) &= f_1^M(c_1^M, c_1^M) = 1 + 1 = 2 \\ \bar{v}\left(f_2\left(f_1(c_1, c_1), x_1\right)\right) &= f_2^M\left(f_1\left(c_1, c_1\right), \bar{v}(x_1)\right) = 2 \times 5 = 10 \\ \bar{v}(s) &= 10 + 7 = 17 \end{aligned}$$

1.4 הגדרת ערך האמת בלוגיקה מסדר ראשון

יהיו M מבנה, v השמה.

1. **נוסחאות אטומיות:** $\varphi = R\left(s_1, ..., s_n\right)$ כש־$R \in \sigma$; אז $\bar{v}(\varphi) = t$ אם ורק אם $(\bar{v}(s_1), ..., \bar{v}(s_n)) \in R^M$
   נחזור לדוגמה: $\varphi = R\left(f_1(c_1, c_1), x_2\right)$ במבנה שהגדרנו קודם.
   - אם $v(x_2) = 6$ אז $\bar{v}(\varphi) = t$
   - אם $v(x_2) = 1$ או $v(x_2) = 0$ אז $\bar{v}(\varphi) = f$
2. **קשרים לוגיים:** אם $\varphi = (\alpha\, op\, \beta)$ כש־$op \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ או $\varphi = (\neg\alpha)$ אז ערך האמת של φ יקבע לפי טבלת האמת של הקשר הרלוונטי:

$$\bar{v}\left(\varphi\right) = TT_{op}\left(\bar{v}(\alpha), \bar{v}(\beta)\right)$$

3. **כמתים:** $\varphi = \exists x_i\ \alpha$ או $\varphi = \forall x_i\ \alpha$

- $\bar{v}(\exists x_i\ \alpha) = t$ אם ורק אם יש $d \in D^M$ כך שעבור $u = v\left({}^{d}/_{x_i}\right)$ מתקיים $\bar{u}(\alpha) = t$.
- $\bar{v}\left(\forall x_i\ \alpha\right) = t$ אם ורק אם לכל $d \in D^M$ עבור $u = v\left({}^{d}/_{x_i}\right)$ מתקיים $\bar{u}(\alpha) = t$

משפט 1.15 אם u, v השמות כך שלכל $x \in FV(\varphi)$, $v(x) = u(x)$ אז $\bar{v}(\varphi) = \bar{u}(\varphi)$

הגדרה 1.16 פסוק: נוסחה ללא משתנים חופשיים

מסקנה 1.17 יהי φ פסוק. אם קיימת השמה v כך ש־ $\bar{v}(\varphi) = t$ אזי לכל השמה u, $\bar{u}(\varphi) = t$

מסקנה 1.18 ערך האמת של פסוק תלוי רק במבנה

דוגמה

$$\varphi = \forall x\ \exists y\ R\left(f_2(c, y), x\right)$$

יהי $d \in \mathbb{N}$ כלשהו. צ"ל: אם $v(x) = d$, אז

$$\bar{v}\left(\exists y\, R\left(f_2(c_1, y), x\right)\right) = t$$

נביט בהשמה המקיימת:

- $v(x) = d$ (קבוע כבר)

- $v(y) = d$ (נבחר ערך ל־y)

$$\bar{v}\left(R\left(\underbrace{f_2(c_1,y)}_{d},x\right)\right) = \bar{v}\left(R(d,d)\right) = t$$

דוגמה

$$\alpha = (\forall x\, R(x,x)) \to R\left(f_1(x,c_1),x\right)$$

$$FV(\alpha) = \{x\}$$

נשים לב ש־x מימין ל־$\to$ אינו מכומת. תהא v השמה ונניח ש־$v(x) = 7$.
$\bar{v}(\alpha) = f$

הערה 1.19 באותו מילון עם המבנה $(\mathbb{N},0,1,+,\times,<)$, $\bar{v}(\alpha) = t$. למה זה נכון?
מהו $\bar{v}\left(\forall x\, R(x,x)\right)$ (אצלנו $R = {}^{"}<{}^{"}$) צריך להביט לכל $d \in \mathbb{N}$ על ערך האמת של $R(x,x)$ תחת ההשמה $v\left({}^{d}/_{x}\right)$

$$R^M\left(d,d\right) = f$$

לכן $\bar{v}\left(R(x,x)\right) = f$ לפי $TT_{\to}$ ואז $\bar{v}\left(\forall x\, R(x,x) \to ...\right) = t$.

2 מושגי יסוד סמנטיים

נדבר על שני מונחים שונים בהקשר של נביעה:

- t־נביעה ($truth$)
- v־נביעה ($valid$)

הגדרה 2.1 t־נביעה:

- מבנה M והשמה v מספקים את φ אם $\bar{v}(\varphi) = t$. נסמן $M,v \vDash \varphi$.
- φ ספיקה במבנה M אם יש השמה v כך ש־$M,v \vDash \varphi$. במקרה זה נאמר כי (M,v) הוא t־מודל של φ.
- תהי Γ קבוצת נוסחאות. אז
  - Γ מסתפקת במבנה M תחת השמה v אם לכל $\varphi \in \Gamma$ מתקיים $M,v \vDash \varphi$ ונסמן $M,v \vDash \Gamma$.
  - Γ ספיקה במבנה M אם יש v כך ש־$M,v \vDash \Gamma$, ואומרים ש־(M,v) הוא t־מודל של Γ.
- φ (Γ) ספיקה אם יש מבנה M בו φ ספיקה.
- נסמן $\Gamma \overset{t}{\vDash} \varphi$ אם כל t־מודל של Γ הוא גם t־מודל של φ. במילים אחרות, $\Gamma \overset{t}{\vDash} \varphi$ אם לכל M,v כך ש־$\bar{v}(\alpha) = t$, לכל $\alpha \in \Gamma$, מתקיים גם $\bar{v}(\varphi) = t$

$$M,v \vDash \Gamma \Rightarrow M,v \vDash \varphi$$

- φ היא t־שקולה ל־ψ אם $\{\varphi\} \overset{t}{\vDash} \psi$ וגם $\{\psi\} \overset{t}{\vDash} \varphi$
- נאמר כי φ היא t־תקפה אם $\emptyset \overset{t}{\vDash} \varphi$

הגדרה 2.2 v־נביעה:

- φ (Γ) נכונה במבנה M אם לכל השמה v, $M,v \vDash \varphi$, ומסמנים $M \vDash \varphi$. M יקרא v־מודל של φ.

- φ (Γ) היא v־ספיקה אם יש לה v־מודל.
- φ נקראת v־תקפה אם φנכונה בכל מבנה. נסמן $\overset{v}{\models}\varphi$
- $\Gamma\overset{v}{\models}\varphi$ אם כל v־מודל של Γ הוא גם v־מודל של φ.
- φ הוא v־שקול ל־ψ אם $\{\varphi\}\overset{v}{\models}\psi$ וגם $\{\psi\}\overset{v}{\models}\varphi$

דוגמאות:

- $\varphi = R(x,x)$. ברור כי ל־φ יש t־מודל: $D^M = \{0,1\}$, $R^M = \{(0,0),(0,1)\}$, $v(x)=0$
  ל־φ יש גם v־מודל: כל מבנה בו R יחס רפלקסיבי. (אמ"מ)
- $\varphi = (\forall x_3 \forall x_4\ R(x_3,x_4)) \vee \neg R(x_1,x_2)$. בכל מבנה M יש v כך ש־$M,v\models\varphi$.
  אם $R^M=\emptyset$ (או $R^M = D^M\times D^M$) אז M הוא v־מודל של φ.
-

$$\begin{aligned}\alpha &= \forall x,y,z\ ((R(x,y)\wedge R(y,z))\to R(x,z))\\ \beta &= \forall x,y,z,w\ ((R(x,y)\wedge R(y,z)\wedge R(z,w))\to R(x,w))\end{aligned}$$

מתקיים $\{\alpha\}\overset{v}{\models}\beta$

טענה 2.3

1. אם φ v־תקפה אז כך גם $\exists x\,\varphi$, $\forall x\,\varphi$
2. אם $\forall x\,\varphi$ v־תקפה אז φ v־תקפה
3. φ ו־ψ הן t־שקולות אם ורק אם לכל M,v מתקיים $\bar{v}(\varphi)=\bar{v}(\psi)$

הוכחה: תרגיל ("ההוכחה טריוויאלית") ■

הערה 2.4 אם $M,v\models\varphi$ אז בוודאי $M,v\not\models\neg\varphi$; מאידך φ וגם $\neg\varphi$ יכולות להיות ספיקות ב־M.
אם $M\models\varphi$ אז בוודאי $M\not\models\neg\varphi$ אבל אם $M\not\models\neg\varphi$ לא בהכרח $M\models\varphi$.

טענה 2.5

1. אם $\Gamma\overset{t}{\models}\varphi$ אז $\Gamma\overset{v}{\models}\varphi$ (הכיוון השני לאו דווקא נכון)
2. אם Γ מכילה רק פסוקים אז אם $\Gamma\overset{v}{\models}\varphi$ אז $\Gamma\overset{t}{\models}\varphi$
3. $\overset{v}{\models}\varphi$ אם ורק אם $\overset{t}{\models}\varphi$ ולכן נדבר רק על תקפות באופן כללי
4. אם ב־Γ יש רק פסוקים אז $\Gamma\overset{t}{\models}\varphi$ אם ורק אם $\Gamma\overset{v}{\models}\varphi$
5. $\Gamma\cup\{\varphi\}$ t־ספיקה אם ורק אם $\Gamma\overset{t}{\not\models}\neg\varphi$

הוכחה:

1. נניח כי $M\models\Gamma$, תהי v השמה כלשהי. $M,v\models\Gamma$ כי $M\models\Gamma$ ומהנתון (משתמשים ב־$\Gamma\overset{t}{\models}\varphi$) מתקיים $M,v\models\varphi$. לכן φ מסתפקת תחת כל השמה ב־M ולכן $M\models\varphi$.
2. נניח $M,v\models\Gamma$. צ"ל: $M,v\models\varphi$. כיוון שב־Γ יש רק פסוקים, מתקיים שערך האמת לא תלוי בהשמה ולכן לכל השמה u מתקיים $M,u\models\Gamma$. דהיינו, $M\models\Gamma$. מהנתון $M\models\varphi$ ובפרט $M,v\models\varphi$
3. נובע מ־א,ב (בקבוצה הריקה אין נוסחאות)
4. נובע מ־א,ב

5. $\Gamma\cup\{\varphi\}$ ־t־ספיקה, אז יש M,v כך ש־$M,v\vDash\Gamma\cup\{\varphi\}$ בפרט $M,v\nvDash\neg\varphi$ וגם $M,v\vDash\Gamma$ ולכן $\Gamma\not\vDash\neg\varphi$

■

הרצאה 8 ־ 3.5.15

תכנית השיעור:

1. נדבר בקצרה על מושגים סמנטיים
2. הצבה של שמות עצם במשתנים
3. צורות נורמליות: Prenax Normal Form
4. גדירות יחסים במבנה

טענה 2.6 φ t־שקולה ל־ψ אם ורק אם $(\varphi\leftrightarrow\psi)$ תקפה.

הוכחה: מיידית מ־t שקילות וטבלת האמת של $\leftrightarrow$. ■

מה לגבי v־שקילות? נניח φ ו־ψ v־שקילות ־ האם $\psi\leftrightarrow\varphi$ תקפה?

דוגמה: $\varphi=R(x)$, $\psi=\forall x\,R(x)$; נשים לב ש־φ ו־ψ v־שקולות. מאידך, $R(x)\leftrightarrow\forall x\,R(x)$ אינה תקפה.

טענה 2.7 $R(x)\overset{v}{\vDash}\forall x\,R(x)$

הוכחה: יהי M מבנה כך ש־$M\vDash R(x)$. תהא v השמה. $\bar v\left(R(x)\right)=t$, $\bar v\left(\forall x\,R(x)\right)$ אם ורק אם לכל d $\bar v\left({}^{d}/_{x}\right)\left(R(x)\right)=t$ וכו'. ■

הגדרה 2.8 עבור נוסחה φ עם משתנים חופשיים $x_1,...,x_n$, הסגור האוניברסלי של φ מסומן $\varphi^{\forall}$ הוא הפסוק $\forall x_1\forall x_2....\forall x_n\varphi$

טענה 2.9 $\varphi^{\forall}$ מסתפק ב־M אם ורק אם M v־מודל של φ

הוכחה: מיידי. ■

טענה 2.10 $\Gamma\overset{v}{\vDash}\varphi$ אם ורק אם $\Gamma^{\forall}\overset{v}{\vDash}\varphi^{\forall}$ אם ורק אם $\Gamma^{\forall}\overset{t}{\vDash}\varphi^{\forall}$, כש־$\Gamma^{\forall}=\left\{\alpha^{\forall}\mid\alpha\in\Gamma\right\}$

2.1 הצבה של שם עצם למשתנה

יהי x משתנה ו־r שם עצם.

אינטואיציה: רוצים להחליף "כל" מופע של x ב־r. צריך להגדיר בזהירות בגלל האפשרות ש־x קשור.

הגדרה 2.11 החלפת משתנה בשם עצם, עבור שמות עצם
יהיו r,s שמות עצם. שם העצם $s\left[{}^{r}/_{x}\right]$ מוגדר באופן הבא:

1.
   (א) אם $s=c$ אז $s\left[{}^{r}/_{x}\right]=s$
   (ב) אם $s=y$ אז אם $y\neq x$ $s\left[{}^{r}/_{x}\right]=s$ ואם $y=x$ אז $s\left[{}^{r}/_{x}\right]=r$
2. אם $s=f\left(s_1,...,s_n\right)$ אז $s\left[{}^{r}/_{x}\right]=f\left(s_1\left[{}^{r}/_{x}\right],...,s_n\left[{}^{r}/_{x}\right]\right)$

לפי משפט הקריאה היחידה אפשר לראות ש־$s\left[{}^{r}/_{x}\right]$ מוגדר היטב.

הגדרה 2.12 הצבת שם עצם למשתנה עבור נוסחאות
יהי r שם עצם, φ נוסחה. אז $\varphi\left[{}^{r}/_{x}\right]$ מוגדרת באופן הבא:

1. אם $\varphi=R\left(s_1,...,s_n\right)$ אז $\varphi\left[{}^{r}/_{x}\right]=R(s_1\left[{}^{r}/_{x}\right],...,s_n\left[{}^{r}/_{x}\right])$
2. אם $\varphi=\varphi_1\,op\,\varphi_2$ (או $\varphi=\neg\varphi_1$) אז $\varphi\left[{}^{r}/_{x}\right]=\varphi_1\left[{}^{r}/_{x}\right]op\,\varphi_2\left[{}^{r}/_{x}\right]$ (או $\neg\varphi_1\left[{}^{r}/_{x}\right]$)
3. $\varphi=Qy\,\psi$ (כש־$Q\in\{\forall,\exists\}$)
   (א) אם $y=x$ אז $\varphi\left[{}^{r}/_{x}\right]=\varphi$
   (ב) אם $y\neq x$ אז $\varphi\left[{}^{r}/_{x}\right]=Qy\,\psi\left[{}^{r}/_{x}\right]$

הערה 2.13 בעצם $\varphi\left[{}^{r}/_{x}\right]$ מתקבלת מ־φ ע"י החלפת כל המופעים החופשיים של x ב־r.

דוגמה: $r_1 = f(x_1, x_2)$, $r_2 = x_3$, $\varphi = R(x_3)$, $\psi = \forall x_3\, \varphi$ ו־$\alpha = \forall x_1\, \varphi$
אז:

$$\begin{aligned} r_1\left[{}^{r_2}/_{x_3}\right] &= f(x_1, x_2) \\ \varphi\left[{}^{r_1}/_{x_3}\right] &= R\left(f(x_1, x_2)\right) \\ \alpha\left[{}^{r_1}/_{x_3}\right] &= \forall x_1\, R\left(f(x_1, x_2)\right) \\ \psi\left[{}^{x_1}/_{x_3}\right] &= \psi \end{aligned}$$

הערה 2.14 בדוגמה שראינו $\alpha\left[{}^{r_1}/_{x_3}\right]$ נוצר מופע קשור חדש של x_1. יש הרבה מקרים בהם היינו רוצים להימנע מכך.

הגדרה 2.15 r חופשי להצבה ב־x בנוסחה φ אם:

1. $\varphi = R\left(s_1, .., s_n\right)$ אזי r חופשי להצבה ב־x עבור φ
2. אם $\varphi = \varphi_1\, op\, \varphi_2$ (או $\varphi = \neg\varphi_1$) אז r חופשי להצבה ב־x עבור φ רק אם r חופשי להצבה ב־x עבור φ_1 וגם עבור φ_2 (או עבור φ_1 בלבד במקרה של $\varphi = \neg\varphi_1$)
3. $\varphi = Qy\, \psi$
   (א) אם x אינו מופע ב־φ אז r חופשי להצבה ב־x בנוסחה (לא מתבצעות הצבות)
   (ב) אם x אינו חופשי ב־φ אז r חופשי להצבה (לא מתבצעות הצבות)
   (ג) $x \in FV(\varphi)$ אז r חופשי להצבה אם:
      i. $y \notin FV(r)$
      ii. r חופשי להצבה ב־x עבור ψ

טענה 2.16 r חופשי להצבה ב־x עבור נוסחה φ אם ורק אם לאף משתנה $y \in FV(r)$ לא נוצר מופע קשור חדש.
הערה: צריך להגדיר מהם מופע קשור ומופע חופשי (יותר עדין ממשתנה קשור / חופשי)

טענה 2.17 יהיו r, s שמות עצם ו־v השמה. נגדיר השמה חדשה: $u = v\left[{}^{\bar{v}(r)}/_{x}\right]$. כלומר:

$$u(y) = \begin{cases} v(y) & y \neq x \\ \bar{v}(r) & y = x \end{cases}$$

אז

$$\bar{u}(s) = \bar{v}\left(s\left[{}^{r}/_{x}\right]\right)$$

טענה 2.18 r שם עצם, v השמה ו־$y \notin FV(r)$ (y לא מופיע ב־r) אזי $\bar{v}(r) = \bar{u}\left(r\left[{}^{y}/_{x}\right]\right)$ כאשר $u = v\left[{}^{v(x)}/_{y}\right]$.

טענה 2.19 שינוי שם משתנה קשור
תהי φ נוסחה כך ש־y לא מופיע ב־φ אז $\exists x\, \varphi$ (באותו אופן $\forall x\, \varphi$) t־שקולה לנוסחה $\exists y\, \varphi\left({}^{y}/_{x}\right)$ (ובאותו אופן $\forall y\, \varphi\left({}^{y}/_{x}\right)$)

הוכחה: ההוכחה מיידית מטענה 2.18 ■

הטענה מאפשרת להחליף שם למשתנים קשורים ולקבל נוסחאות שקולות. בפרט, בהינתן נוסחה φ ניתן לקבל (ע"י אלגוריתם יעיל) נוסחה ψ השקולה ל־φ בה לאף משתנה חופשי אין מופע קשור.

2.2 צורות קנוניות

הגדרה 2.20 Prenax Normal Form - PNF
נוסחאות ב־PNF הן מהצורה $Q_1x_1...Q_nx_n\,\varphi$ (כש־φ חסרת כמתים)

הגדרה אינדוקטיבית: נוסחה חסרת כמתים:
בסיס: נוסחאות אטומיות; פעולות: קשרים; סגור: נוסחאות חסרות כמתים.
PNF:
בסיס: נוסחאות חסרות כמתים; פעולות: כמתים; סגור: PNF.

משפט 2.21 משפט ה־PNF
לכל נוסחה מעל מילון σ קיימת נוסחת PNF מעל σ t־שקולה לה.

הוכחת המשפט בהמשך. הפעלה של העברת נוסחה לנוסחת PNF נקראת חילוץ כמתים.

טענה 2.22

1. $\forall x\,(\varphi\wedge\psi)$ t־שקולה ל־$\forall x\,\varphi\wedge\forall x\,\psi$
2. $\exists x\,(\varphi\vee\psi)$ t־שקולה ל־$\exists x\,\varphi\vee\exists x\,\psi$
3. אם $x\notin FV(\psi)$ אזי $(\forall x\,\varphi)\vee\psi$ t־שקולה ל־$\forall x\,(\varphi\vee\psi)$
4. אם $x\notin FV(\psi)$ אזי $\exists x\,(\varphi\wedge\psi)$ t־שקולה ל־$(\exists x\,\varphi)\wedge\psi$
5. $\neg\forall x\,\varphi\equiv\exists x\,\neg\varphi$, $\neg\exists x\,\varphi\equiv\forall x\,\neg\varphi$ ($\equiv$ זה t־שקילות)

הערה 2.23 $\forall x\,(\varphi\vee\psi)$ לאו דווקא שקולה ל־$\forall x\,\varphi\vee\forall x\,\psi$
דוגמה: φ: x זוגי, ψ x אי זוגי. $\exists x\,\varphi\wedge\exists x\,\psi$ נכון אבל $\exists x\,(\varphi\wedge\psi)$ לא נכון

הוכחה: הוכחת משפט ה־PNF:
בתור התחלה נתרגם כל נוסחה לנוסחה מעל הקשרים $\vee,\wedge,\neg$ והכמתים $\forall,\exists$. אם φ נוסחה אטומית, אז היא כבר ב־PNF.
המקרה המעניין: φ_1,φ_2 נוסחאות, ψ_1,ψ_2 ב־PNF ו־$\varphi_1\equiv\psi_1$, $\varphi_2\equiv\psi_2$. אז

$$\exists\forall\exists\forall\alpha_1\equiv\varphi=\varphi_1\,op\,\varphi_2\equiv\exists\forall\exists\forall\alpha_2$$

$$\varphi\equiv\exists\forall\exists\forall\alpha$$

טענה:

$$\varphi\equiv\psi_1\,op\,\psi_2$$

נשנה את שמות המשתנים הקשורים ב־ψ_1 למשתנים שלא מופיעים ב־ψ_2 ואחר כך נעשה אותו הדבר ל־ψ_2.
כעת לפי הטענה הקודמת על שקילויות ניתן להוציא את כל הכמתים החוצה. ■

2.3 גדירות יחסים במבנה

$$\sigma_{arith}=\langle c_0,c_1,+,\times,<,=\rangle$$

מבנה: הטבעיים. $\varphi_{even}(x)=\exists y\,(y\cdot(c_1+c_1)=x)$, $\varphi_{odd}(x)=\neg\varphi_{even}(x)$
$\varphi_{prime}(x)=\forall x\,(divide(y,x)\to((y=x)\vee(y=c_1)))$, $divide(y,x)=\exists z\,(y\times z=x)$

הגדרה 2.24 יהיה σ מילון, M מבנה עבורו. תהי $\varphi(x_1,..,x_n)$ נוסחה מעל σ עם $FV(\varphi)=\{x_1,...,x_n\}$ (אולי ב־φ יש משתנים קשורים נוספים) אזי φ מגדירה ב־M את היחס הבא:

$$R_\varphi\subset\underbrace{D^M\times...\times D^M}_{n\,\text{times}}$$

כך ש־$(d_1,...,d_n)\in R_\varphi$ אם ורק אם ההשמה v המקיימת $v(x_1)=d_1,...,v(x_n)=d_n$. מקיימת $\bar{v}(\varphi)=t$.
יחס R יקרא גדיר ב־M אם קיימת נוסחה φ כך ש־$R=R_\varphi$.

הרצאה 9 - 10.5.15

שאלה ממבחן סמסטר א':
נתון המילון: $\Sigma = \{+, \times, =\}$[9] עם מבנה $\mathbb{R}$, $+$ חיבור ו־$\times$ כפל.
הוכיחו:

1. המספר 0 גדיר (יש נוסחה φ שהאיבר היחיד המספק אותה הוא 0; או היחס החד מקומי $\{0\}$ גדיר).
2. המספר a גדיר אם ורק אם היחס $x < a$ גדיר
3. המספר $\sqrt{2}$ גדיר (ב־$\mathbb{R}$)
4. אם יחס חד מקומי סופי P גדיר ב־$\mathbb{R}$ אז המספר המקסימלי שמקיים את P, גדיר.
5. אם יחס חד מקומי סופי P גדיר ב־$\mathbb{R}$ אזי כל מספר שמקיים את P גדיר.

פתרון

.1

$$\varphi_0(x) \ : \ \forall y\ (x + y = y)$$

0 נייטרלי לחיבור

לפני פתרון ב', נגדיר את היחס $x \leq y$:

$$\varphi_{\leq}(x,y) \ : \ \exists z\ (x + z \times z = y)$$

$(x,y) \in \varphi_{\leq}$ אם ורק אם $x \leq y$ כי הנוסחה אומרת שיש מספר אי שלילי (z^2) כך ש־$x + z^2 = y$. אז נגדיר:

$$\varphi_{<}(x,y) \quad : \quad \exists z \ \left(\neg\varphi_0(z) \land \left(x + z^2 = y\right)\right)$$

או

$$\varphi_{<}(x,y) \quad : \quad \varphi_{\leq}(x,y) \land \neg(x = y)$$

2. נניח a גדיר. נניח φ_a נוסחה המגדירה את a. נציג נוסחה המגדירה את $< a$:

$$\varphi_{<a}(x) \quad : \quad \exists y\ (\varphi_{<}(x,y) \land \varphi_a(y))$$

נניח $\varphi_{<a}(x)$ גדיר.

$$\varphi_a(x) = (\neg\varphi_{<a}(x)) \land (\forall z\, (\neg\varphi_0(z) \to \forall y\ (y + z \times z = x \to \varphi_{<a}(y))))$$

הסבר: a הוא המספר היחיד המקיים a לא קטן מ־a וגם לכל מספר חיובי ממש (z^2), $a - z^2$ קטן מ־a.

3. נגדיר את 1.

$$\varphi_1 \quad : \quad \forall y\, (x \times y = y)$$

$$\varphi_2(y) \quad : \quad \exists z\ (\varphi_1(z) \land (z + z = y))$$

ואז

$$\varphi_{\sqrt{2}}(x) \quad : \quad \exists y\ (\varphi_2(y) \land (x \times x = y) \land \exists z\ (x = z \times z))$$

.4

$$\varphi_{maxP}(x) \quad : \quad \varphi_P(x) \land (\forall y\ (\varphi_P(y) \to \varphi_{\leq}(y,x)))$$

כאשר φ_P הנוסחה המגדירה את P. x מקיים את P וכל מספר אחר המקיים את P קטן או שווה לו. מהסופיות נקבל שאכן קיים מקסימום.

[9] כשכותבים = מתכוונים ליחס השוויון ואין צורך לפרש אותו

5. נוכיח באינדוקציה על מספר המספרים הממשיים המקיימים את P.

בסיס: $|P|=1$ (נסמן ב־$|P|$ את מספר הממשיים המקיימים את P). תהא φ_P הנוסחה המגדירה את P. בגלל שיש רק מספר אחד שמקיים אותה נקבל ש־φ_P מגדירה אותו.

נניח שהוכחנו את הטענה לכל יחס P' המקיים $|P'|\leq n$. נוכיח את הטענה ליחס המקיים $|P'|=n+1$. יהי a איבר כלשהו $a\in P'$. אם $a=maxP'$ [10], אז ראינו כי a גדיר. אם a אינו המקסימלי, אז נגדיר יחס חדש $R(x)=\varphi_{P'}(x)\wedge(\neg\varphi_{maxP'}(x))$. נשים לב שביחס R יש בדיוק n איברים, כי פרט ל־$maxP'$ כל איברי P' ביחס ואין אחרים. נשים לב כי $a\in R$ (כי הוא לא היה המקסימלי). כיוון ש־R גדיר ו־$|R|=n$, ניתן להגדיר את איבריו לפי הנחת האינדוקציה, ולכן a גדיר.

3 בדיקת ספיקות

בשיעור הזה ננסה להבין איך בודקים **האם קבוצת נוסחאות ספיקה**.

- **פסוק:** נוסחה ללא משתנים חופשיים.
- **פסוק/נוסחה אוניברסלי:** $\forall x_1 ... \forall x_n\,\varphi$ כש־φ חסרת כמתים.
- **פסוק/נוסחה יישי:**[11] $\exists x_1 ... \exists x_n\,\varphi$ כש־φ חסרת כמתים.

הצעד הראשון בבדיקה האם נוסחה φ ספיקה היא תרגום φ לנוסחה אוניברסלית באופן המשמר ספיקות.

טענה 3.1 יהי σ מילון, אזי $\exists x\,\varphi(x)$ ספיקה מעל σ אם ורק אם $\varphi\left[c/x\right]$ ספיקה מעל המילון $\sigma'=\sigma\cup\{c\}$, כאשר c סימון קבוע חדש.

הוכחה: $\Leftarrow$: נניח $\exists x\,\varphi(x)$ ספיקה. כלומר, יש $M,v\vDash\exists x\,\varphi(x)$. לפי הגדרת ערך אמת מתקיים שיש $d\in D^M$ כך ש־$M,v\left[d/x\right]\vDash\varphi(x)$ ונראה כעת כי $\varphi\left[c/x\right]$ ספיקה.

יהי M' המבנה הזהה ל־M פרט לכך ש־$c^{M'}=d$. (c לא מפורש ב־M כי $c\notin\sigma$) וניקח $v'=v\left[d/x\right]$ (אפשר גם $v'=v$ כי x לא מופיע ב־$\varphi\left[c/x\right]$)

לפי הגדרת הסמנטיקה בגלל ש־$v'(c)=d$ ולפי טענה שהוכחנו, $\bar{v}'\left(\varphi\left[c/x\right]\right)=\bar{v}'\left[d/x\right]$, במבנה M'. ולכן $M',v'\vDash\varphi\left[c/x\right]$.

$\Rightarrow$: נניח M' מבנה עבור σ' ו־v' השמה כך ש־$M',v'\vDash\varphi\left[c/x\right]$. יהי M הצמצום של M ל־σ. אזי $M,v'\vDash\exists x\,\varphi(x)$ כי יהי $D^M=D^{M'}\ni d=c^{M'}$. לפי הגדרת ערך אמת

$$M,v\left[d/x\right]\vDash\varphi(x)$$

■

טענה 3.2 פסוק

$$\forall y_1 ... \forall y_n \exists x\,\varphi(x,y_1,...,y_n)$$

ספיק אם ורק אם הפסוק

$$\forall y_1 ... \forall y_n\,\varphi(f(y_1,...,y_n),y_1,...,y_n)$$

ספיק מעל מילון $\sigma'=\sigma\cup\{f\}$ כאשר f סימון פונקציה n־מקומית חדש.

הוכחה: בדומה למה שעשינו קודם. ■

משפט 3.3 סקולם ($Skolem$)
קיים אלגוריתם שלכל פסוק φ בונה פסוק אוניברסלי ψ כך ש־φ ספיק אם ורק אם ψ ספיק.
ψ עשוי להיות מעל מילון שונה.

הוכחה:

- מוצאים φ' שקולה ל־φ בצורת PNF.
- מסלקים כמתים יישיים ($\exists$) אחד אחרי השני, משמאל לימין ע"י הוספת סימני פונקציות חדשים או קבועים למילון.

■

[10] כתיב מקוצר, ראינו כבר איך להגדיר
[11] מלשון יש

דוגמאות

1. $\exists x\, \varphi(x) \rightsquigarrow \varphi(c)$ כש־c סימן קבוע חדש
2. $\forall x \exists y\, \varphi(x,y) \rightsquigarrow \forall x\, \varphi(x, f(x))$
3.

$$\begin{aligned}\forall x_1 \exists y_1 \forall x_2 \exists y_2\, \varphi(x_1,x_2,y_1,y_2) \\ \rightsquigarrow \forall x_1 \forall x_2 \exists y_2\, \varphi(x_1,x_2,f_1(x_1),y_2) \\ \rightsquigarrow \forall x_1 \forall x_2\, \varphi(x_1,x_2,f_1(x_1),f_2(x_1,x_2))\end{aligned}$$

הערה 3.4 האם φ שקולה ל־ψ? לאו דווקא, בהרבה מקרים הן אפילו לא מוגדרות מעל אותו מילון!

הערה 3.5 האם הטרנספורמציה שומרת על תקפות? לאו דווקא. ניקח

$$\varphi = \forall x \exists y\ (R(x) \vee \neg R(y)) \equiv \forall x\, R(x) \vee \exists y\, \neg R(y) \equiv \forall x\, R(x) \vee \neg \forall y\, R(y)$$

ו־

$$\psi = \forall x\ (R(x) \vee \neg R(f(x)))$$

הערה 3.6 המילה המעניינת והחשובה במשפט היא אלגוריתם. בלעדיה הטענה טריוויאלית.

חזרה לשאלת הספיקות. דבר על פסוקים ללא משתנים וללא כמתים.

דוגמה:

1. $R(a, f(a)) \wedge \neg R(b,c)$
2. $\neg R(a, f(a)) \wedge \neg R(f(b), c)$ ספיק (למשל $R = \emptyset$)
3. א$\wedge$ב

נראה כעת תרגום של נוסחה חסרת משתנים (וכמתים) לתחשיב הפסוקים באופן ששומר ספיקות / תקפות.
כיוון שעצמת קבוצת הנוסחאות האטומיות בת מניה, ניתן להתאים לכל נוסחה אטומית מעל σ פסוק אטומי P_i בתחשיב הפסוקים.
למשל $\sigma = \langle a,b,c,f,R \rangle$

$$\underbrace{R(a,a)}_{P_1}, \underbrace{R(a,b)}_{P_2}, \ldots$$

$$\underbrace{R(a,f(a))}_{P_3}, \underbrace{R(b,f(a))}_{P_4}, \ldots$$

למשל אם $R(a,f(a)) \rightsquigarrow P_1$ ו־$R(b,c) \rightsquigarrow P_2$ אזי $R(a,f(a)) \wedge \neg R(b,c) \rightsquigarrow P_1 \wedge \neg P_2$
אם φ נוסחה חסרת משתנים וכמתים, נסמן ב־$\hat{\varphi}$ את הנוסחה שהתאמנו לה בתחשיב הפסוקים. (מגדירים באינדוקציה כמו שצריך).

טענה 3.7

1. φ ספיקה אם ורק אם $\hat{\varphi}$ ספיקה.
2. φ תקפה אם ורק אם $\hat{\varphi}$ תקפה.

הוכחה: נראה את 1. $\Leftarrow$: יהי M מבנה המספק את φ. נגדיר השמה בתחשיב הפסוקים, w. אם לפסוק האטומי P_i התאמנו נוסחה אטומית α אזי $w(P_i)=t$ אם ורק אם $M\vDash\alpha$. אם ל־P_i לא הותאם α נגדיר $w(P_i)=f$.

כעת, ניתן להוכיח (למשל באינדוקצית מבנה) כי $\bar{w}(\hat{\varphi})=t$. נניח כי $\{P_i \mid i\in I\}$ אלו הפסוקים האטומיים שהותאמו לנוסחאות אטומיות. נסמן ב־T את קבוצת כל הנוסחאות מעל P_i הנ"ל שערך האמת שלהם זהה לערך האמת של הנוסחה המתאימה בתחשיב היחסים. באינדוקציה אפשר להראות שכל הנוסחה ב־$\{P_i \mid i\in I\}$ גם ב־T.

$\Rightarrow$: נניח $\hat{\varphi}$ ספיקה ונראה כי φ ספיקה. תהי w השמה המספקת את $\hat{\varphi}$ו־$\bar{w}(\hat{\varphi})=t$. נגדיר מבנה M באופן הבא: $D^M=Term$ (קבוצת שמות העצם מעל המילון שלנו)

עבור קבוע $c\in\sigma$ נפרש $c^M=c$. איך נגדיר את f^M, יהי $s_1,...,s_n\in D^M$ ונגדיר

$$f^M(s_1,...,s_n)=\underbrace{f(s_1,...,s_n)}_{\in Term=D^M}$$

אינטואיטיבית: w אומרת אילו נוסחאות אטומיות צריכות להתקיים במבנה M אותו אנו מחפשים.

נותר לפרש יחסים. יהי $R\in\sigma$. נגדיר את R^M. נגדיר $(s_1,...,s_n)\in R^M$ אם ורק אם: יהי P_i הפסוק האטומי (תחשיב פסוקים) המתאים לנוסחה האטומית $R(s_1,..,s_n)$. אזי $(s_1,...,s_n)\in R^M$ אם ורק אם $w(P_i)=t$ וכעת ניתן להוכיח באינדוקצית מבנה כי $M\vDash\varphi$. ■

דוגמה: $\neg R(a,f(a))\wedge\neg R(f(b),c)$. סימני קבוע: a,b,c, סימן פונקציה: $f(\cdot)$, יחס דו מקומי: $R(\cdot,\cdot)$.

$$\begin{aligned} R(a,f(a)) &\rightsquigarrow P_1\\ R(f(b),c) &\rightsquigarrow P_2\\ &\vdots \end{aligned}$$

אז $\hat{\varphi}=\neg P_1\wedge\neg P_2$. $w(P_1)=f,\ w(P_2)=f$.

ניקח M: $D^M=Term$= כל שמות העצם. $c^M=c$, $f^M(b)=f(b)$, $a^M=a$, $f^M(a)=f(a)$. אז $(a,f(a))\notin R^M$

$$R(a,f(a))\rightsquigarrow P_1,\ w(P_1)=f$$

ו־$(f(b),c)\notin R^M$ וכו'.

הגדרה 3.8 מבנה הרברנד Herbrand

M הוא מבנה הרברנד מעל מילון σ אם:

1. לכל $a\in D^M$ יש שם עצם s ללא משתנים כך ש־$s^M=a$
2. לכל שני שמות עצם שונים $(s_1\neq s_2)$, $s_1^M\neq s_2^M$

במבנה הרברנד איברים מהתחום מתאימים לשמות עצם באופן חח"ע ועל.

דוגמה $\sigma=\langle c_0,succ\rangle$, $M=\langle\mathbb{N},0,+1\rangle$. M הוא מבנה הרברנד עבור σ. ($succ$ היא פונקציה חד מקומית)

הרצאה 10 - 17.5.15

דוגמה: $\sigma=\langle c_0,succ,pred\rangle$, $M=\langle\mathbb{N},0,+1,-1\rangle$. $pred(succ(c_0))=0+1-1=0$

טענה 3.9 אם במילון σ יש סימן קבוע, אז קיים מבנה הרברנד ל־σ.

3.1 תכונות של מבנה הרברנד

יהי σ מילון, H מבנה הרברנד עבורו.

1. יש שם עצם r מעל משתנים $x_1,...,x_n$. נניח כי:

$$\begin{aligned} v(x_1) &= d_1\Leftrightarrow s_1\\ &\vdots\\ v(x_n) &= d_n\Leftrightarrow s_n \end{aligned}$$

אז לכל השמה v מתקיים

$$\bar{v}(r)=r\left[{}^{s_1}/_{x_1},...,{}^{s_n}/_{x_n}\right]^M$$

(s_i הם שמות העצם המתאימים ל־$v(x_i)$)

2. φ נוסחה, $FV(\varphi)=\{x_1,...,x_n\}$. אז $H,v\vDash\varphi$ אם ורק אם
$$H\vDash\varphi\left[{}^{s_1}/_{x_1},...,{}^{s_n}/_{x_n}\right]$$
כש־
$$\begin{aligned} v(x_1) &= d_1 \Leftrightarrow s_1 \\ &\vdots \\ v(x_n) &= d_n \Leftrightarrow s_n \end{aligned}$$

3. $\exists x\,\varphi(x)$ נכון ב־H אם ורק אם יש שם עצם r כך ש־$\varphi\left[{}^{r}/_{x}\right]$ נכון ב־H.
4. $\forall x\,\varphi(x)$ נכון ב־H אם ורק אם לכל שם עצם r, $\varphi\left[{}^{r}/_{x}\right]$ נכון ב־H.

תזכורת בהינתן השמה v, שם עצם s ומשתנה x הגדרנו:
$$v'=v\left[{}^{\bar{v}(s)}/_{x}\right]$$
והוכחנו ש־
$$\bar{v}\left(r\left[{}^{s}/_{x}\right]\right)=\bar{v'}(r)$$
וכנ"ל לנוסחאות. **הוכחה:** תרגיל. ∎

משפט 3.10 משפט הרברנד
יהי σ מילון ללא סימן $=$. פסוק אוניברסלי φ מעל σ ספיק אם ורק אם הוא ספיק במבנה הרברנד.

הגדרה 3.11 (Ground Instance) יהי $\alpha=\forall x_1...\forall x_n\,\varphi(x_1,...,x_n)$ פסוק אוניברסלי. נוסחה המתקבלת על ידי הצבת שמות עצם סגורים למשתנים $x_1,...,x_n$ נקראת ground instance של α.
$$GrIns(\alpha)=\left\{\varphi\left[{}^{s_1}/_{x_1},...,{}^{s_n}/_{x_n}\right]\ \mid s_1,...,s_n\in\overline{Term}\right\}$$
כש־$\overline{Term}$ - קבוצת שמות העצם הסגורים.

משפט 3.12 σ מילון ללא $=$. Γ קבוצת פסוקים אוניברסלית מעל σ. הטענות הבאות שקולות:

1. Γ ספיקה
2. Γ ספיקה במבנה הרברנד
3. $GrIns(\Gamma)$ ספיקה
$$GrIns(\Gamma)=\bigcup_{\varphi\in\Gamma}GrIns(\varphi)$$
4. $GrIns(\Gamma)$ ספיקה במבנה הרברנד

הוכחה: 1⇔4 לפי תכונה 4 של מבנה הרברנד. 2⇐1 ו־4⇐3 מיידי לפי הגדרה. 1⇐3 פשוט.
נשאר להראות את $3\Leftarrow$4. ∎

טענה 3.13 (נניח שב־σ אין שוויון) אם Λ קבוצת פסוקים ללא משתנים וללא כמתים, אז Λ ספיקה אם ורק אם היא ספיקה במבנה הרברנד.

הוכחה: $\Rightarrow$: ברור.
$\Leftarrow$: יהי M מבנה ל־Λ. נגדיר H כמו בשבוע שעבר:
$$D^H=\overline{Term}$$
פירוש פונקציות וקבועים באופן הטבעי. נותר לפרש סימני יחס. עבור $R\in\sigma$
$$\left(t_1^H,...,t_n^H\right)\in R^H\Leftrightarrow R(t_1,...,t_n)^M=t$$
מכאן נובע (באינדוקציה) שלכל נוסחה ללא משתנים וללא כמתים φ, $\varphi^M=\varphi^H$. ∎

טענה זו מוכיחה מיידית את $3\Leftarrow$4. המשפט שהוכחנו עכשיו הוא הכללה של משפט הרברנד, ולכן בפרט הוכחנו את משפט הרברנד.

4 בדיקת תקפות

בהינתן פסוק φ נראה תהליך שעוצר אם φ תקף (ואומר φ תקף), אחרת עשוי לרוץ לעד.
φ תקף $\Leftrightarrow$ $\neg\varphi$ לא ספיק.
נעביר את $\neg\varphi$ לצורה אוניברסלית (סקולמיזציה). נקבל פסוק אוניברסלי ψ. לפי המשפט שראינו, ψ אינו ספיק אם ורק אם $GrIns(\psi)$ אינה ספיקה במבנה הרברנד.
בשבוע שעבר ראינו דרך לתרגם נוסחאות ללא משתנים וללא כמתים לתחשיב הפסוקים באופן משמר ספיקות. נקרא לקבוצה Γ.
לפי משפט הקומפקטיות בתחשיב הפסוקים, Γ ספיקה אם ורק אם כל תת קבוצה סופית שלה ספיקה.
הפרוצדורה תעבור על כל תתי הקבוצות הסופיות עד שתמצא אחת שאינה ספיקה ואז תכריז ש־φ תקף.

4.1 משפט הקומפקטיות בתחשיב היחסים

משפט 4.1 משפט הקומפקטיות עבור נוסחאות מעל מילון ללא $=$:

1. Γ ספיקה אם ורק אם כל תת קבוצה סופית שלה ספיקה.
2. $\Gamma \overset{t}{\vDash} \varphi$ אם ורק אם קיימת תת קבוצה סופית $\Delta \subseteq \Gamma$, כך ש־$\Delta \overset{t}{\vDash} \varphi$.
3. $\Gamma \overset{v}{\vDash} \varphi$ אם ורק אם קיימת תת קבוצה סופית $\Delta \subseteq \Gamma$, כך ש־$\Delta \overset{v}{\vDash} \varphi$.

הוכחה: 1: נוכיח תחילה למקרה ש־Γ ללא משתנים וללא כמתים. נניח שכל תת קבוצה סופית של Γ ספיקה. ראינו דרך לתרגם פסוק φ לפסוק $\hat{\varphi}$ בתחשיב הפסוקים, באופן המשמר ספיקות:

$$\Gamma \mapsto \hat{\Gamma} = \{\hat{\varphi} \mid \varphi \in \Gamma\}$$

$\hat{\Gamma}$ ספיקה אם ורק אם Γ ספיקה.
$\hat{\Gamma}$ אם ורק אם כל תת קבוצה סופית $\hat{\Delta} \subseteq \hat{\Gamma}$ ספיקה.
$\hat{\Delta} \subseteq \hat{\Gamma}$ ספיקה אם ורק אם $\Delta \subseteq \Gamma$ ספיקה.
כיוון שהוכחנו שכל תת קבוצה סופית של Γ ספיקה, כל $\hat{\Delta} \subseteq \hat{\Gamma}$ ספיקה.
כעת נעבור למקרה של Γ כללית של פסוקים.

- Γ ספיקה אם ורק אם Γ_{skolem} המתקבלת מ־Γ אחרי תהליך סקולם (לכל פסוק ב־Γ), ספיקה.
- Γ_{skolem} קבוצת פסוקים אוניברסלית והוא ספיקה אם ורק אם $GrIns(\Gamma_{skolem})$ ספיקה.
- $GrIns(\Gamma_{skolem})$ ספיקה אם ורק אם כל תת קבוצה סופית שלה ספיקה.

נראה כעת שאם כל תת קבוצה סופית של Γ ספיקה אזי גם כל תת קבוצה סופית של $GrIns(\Gamma_{skolem})$ ספיקה.
תהא $\Delta \subseteq GrIns(\Gamma_{skolem})$ סופית ונראה שהיא ספיקה. יש $\Sigma \subseteq \Gamma_{skolem}$ סופית כך ש־$\Delta \subseteq GrIns(\Sigma)$.
יש $\Lambda \subseteq \Gamma$ סופית כך ש־$\Sigma = \Lambda_{skolem}$; Λ ספיקה ולכן Σ ספיקה.
לפי משפט הרברנד $GrIns(\Sigma)$ ספיקה, וכיוון ש־$\Delta \subseteq GrIns(\Sigma)$ נקבל ש־Δ ספיקה.
כעת עבור Γ כללית של נוסחאות:
נרצה לתרגם קבוצת נוסחאות לקבוצת פסוקים באופן ששומר ספיקות. נציג מספר בן מניה של קבועים חדשים וכל מופע חופשי של x_i נחליף ב־c_i. ברור שהתהליך שומר ספיקות. ■

הוכחה: 2: $\Rightarrow$: ברור. $\Leftarrow$: נניח $\Gamma \overset{t}{\vDash} \varphi$. אזי $\Gamma \cup \{\neg\varphi\}$ לא ספיקה. לפי סעיף א' יש תת קבוצה סופית $\Delta \cup \{\neg\varphi\}$ שאינה ספיקה. כלומר $\Delta \overset{t}{\vDash} \varphi$. ■

הוכחה: 3: 2: $\Rightarrow$: ברור. $\Leftarrow$: נניח $\Gamma \overset{v}{\vDash} \varphi$ $\Leftrightarrow$ (ראינו בעבר) $\Gamma^{\forall} \overset{v}{\vDash} \varphi^{\forall}$ $\Leftrightarrow$ ($\Gamma^{\forall}$ פסוקים) $\Gamma^{\forall} \overset{t}{\vDash} \varphi^{\forall}$ $\Leftrightarrow$ (סעיף ב') $\Delta^{\forall} \overset{t}{\vDash} \varphi^{\forall}$ $\Leftrightarrow$ (ראינו בעבר) $\Delta \overset{v}{\vDash} \varphi$. ■

4.1.1 דוגמה לשימוש במשפט הקומפקטיות

הרצאה 11 - 31.5.15

$\sigma = \langle E(\cdot,\cdot)\rangle$; E יחס דו מקומי. נשים לב שמבנה הוא פשוט גרף. $V = D^M$ ומופיעה קשת (i,j) אם ורק אם $E(i,j)$.

טענה 4.2 לא ניתן בלוגיקה מסדר ראשון להגדיר את אוסף הגרפים הקשירים.

טענה 4.3 לא קיימת נוסחה $\varphi(x,y)$ מעל σ המסתפקת אם יש מסלול בין x ל־y.

הוכחה: נניח בשלילה שיש φ כנ"ל. תהי ψ_k נוסחה האומרת שאין מסלול באורך k בין x ל־y.
למשל:

$$\begin{aligned}\psi_1 &= \neg E\,(x,y)\\ \psi_2 &= \neg\exists z\;(E(x,z)\wedge E(z,y))\end{aligned}$$

נראה כי

$$\Gamma=\{\varphi\}\cup\{\psi \mid k=0,1,...\}$$

ספיקה ומכאן נקבל סתירה כי מבנה המספק את φ מכיל מסלול בין x ל־y, מאיד לפי $\{\psi \mid k=0,1,...\}$ המסלול אינו סופי, בסתירה.

לפי משפט הקומפקטיות, Γ ספיקה אם ורק אם כל תת קבוצה סופית ספיקה. תהי $\Gamma'\subset\Gamma$ סופית.
בה"כ,

$$\Gamma'\subset\{\varphi\}\cup\{\psi_1,..,\psi_n\}$$

ניקח מבנה שייצג גרף שרשרת באורך מעל n, ואז בין שני הקצוות לא קיים מסלול באורכים $1,...,n$ אבל קיים מסלול כלשהו. זוהי השמה שמספקת את $\{\varphi\}\cup\{\psi_1,..,\psi_n\}$, לכן גם את Γ' ולכן Γ ספיקה. ■

בש"ב: $\exists x\,\varphi$ תקף אם ורק אם לאיזשהו n יש $t_1,...,t_n$ שמות עצם סגורים כך ש־

$$\varphi\left[{}^{t_1}\!/x\right]\vee...\vee\varphi\left[{}^{t_n}\!/x\right]$$

תקף. תרגיל זה משתמש במשפט הקומפקטיות.

משפט 4.4 "היורד" (Downward - Löwenheim–Skolem)
φ ספיקה אם ורק אם φ ספיקה במבנה סופי או בן מניה.

הוכחה: מיידי ממשפט הרברנד. ■

משפט 4.5 "העולה" (Upward - Löwenheim–Skolem)
אם φ ספיקה במבנה אינסופי, אז לכל עוצמה אינסופית λ יש מבנה מעוצמה λ המספק את φ.

הוכחה: רעיון ההוכחה (אינטואיציה): נגדיר מספר קבועים בעוצמה λ, וזה יכריח את המבנה שלנו להיות גדול. ואז משתמשים במשפט הקומפקטיות... ■

4.2 לוגיקה מסדר ראשון עם סימן $=$

$$\sigma=\langle c_0,c_1,...,f_1,...,R_1,...\rangle$$

$$(,),\exists,\forall,\rightarrow,\neg,\wedge,\vee,\leftrightarrow$$

סימן נוסף: $=$
יש הרבה ספרים בהם סימן $=$ הוא חלק מהשפה - נמצא בכל מילון ותמיד מפורש כשיוויון. בפרט כשיש שוויון, גם $(t_1=t_2)$ פסוק אטומי.
רעיון לטיפול ב־$=$: להגדיר מבנה בו האיברים הם מחלקות שקילות של שמות עצם סגורים בהתאם למבנה M, כך ש־$(t_1\sim t_2)$ אם $(t_1=t_2)^M=t$.

משפט 4.6 קיים אלגוריתם שעבור נוסחה φ בונה נוסחה ψ ללא שיוויון כך ש־φ ספיקה אם ורק אם ψ ספיקה.

תכונות השוויון:

- שוויון הוא יחס שקילות
- שוויון הוא יחס קונגרואציה (Congruent): כלומר נשמר תחת כל נוסחה; למשל אם R הוא יחס דו מקומי אז

$$\begin{array}{l} x_1 = x_2 \\ y_1 = y_2 \end{array} \Rightarrow R(x_1,y_1) \leftrightarrow R(x_2,y_2)$$

אסטרטגיה: נגדיר יחס חדש E שיהיה יחס שקילות ויחס קונגרואציה (ניתן אוסף נוסחאות שמסתפק רק ל־E כנ"ל).
אחרי כן, נחליף כל פסוק אטומי מהצורה $(x=y)$ ב־$E(x,y)$. לבסוף נראה שהנוסחה שמתקבלת ספיקה אם ורק אם הנוסחה המקורית ספיקה.
נרצה שלא יהיו סימני פונקציה כדי שיהיה נוח לעבוד.

טענה 4.7 יש אלגוריתם שבהינתן נוסחה φ בונה נוסחה φ' ללא סימני פונקציה כך ש־φ ספיקה אם ורק אם φ' ספיקה.

רעיון: פונקציה היא בעצם יחס. כלומר, לכל f n־מקומית אפשר להגדיר יחס $n+1$ מקומי מתאים

$$f(x_1,..,.x_n)=y \iff R_f(x_1,...,x_n,y)$$

רעיון האלגוריתם: נניח שיש לנו "הרבה" סימני קבוע חדשים. כל פעם שיש מופע $f(t_1,...,t_n)$ בתוך יחס R. נחליף את $f(t_1,...,t_n)$ במשתנה חדש y ונוסיף $(f(t_1,...,t_n)=y)\wedge$.[12]

הגדרה 4.8 יחס E נקרא יחס קונגרואנציה אם:

1. E יחס שקילות:

$$Equivalence(E) \;:\; (\forall x\, E(x,x)) \wedge (\forall x,y\, E(x,y)\to E(y,x)) \wedge \forall x,y,z\; (E(x,y)\wedge E(y,z)\to E(x,z))$$

2. לכל יחס R מתקיימת הנוסחה $Cong(E,R)$; אם R יחס k־מקומי אז

$$Cong(E,R) \;:\; \forall x_1,...,x_k \forall y_1,...,y_k\; (E(x_1,y_1)\wedge ... \wedge E(x_k,y_k)\wedge (R(x_1,...,x_k)\to R(y_1,...,y_k)))$$

הוכחה: הוכחת המשפט - סילוק =:
אלגוריתם: בהינתן φ נחליף כל מופע של פסוק אטומי $(x=y)$ ב־$E(x,y)$ (ובאופן כללי $(t_1=t_2)$ ב־$E(t_1,t_2)$). נניח שקיבלנו נוסחה φ'.
בשלב שני נגדיר

$$\psi = \varphi' \wedge Equivalence(E) \wedge \bigwedge_R Cong(E,R)$$

נטען ש־φ ספיקה אם ורק אם ψ ספיקה.
$\Leftarrow$: נניח φ מסתפקת במבנה M. נפרש ב־M את E כיחס שוויון (נקבל מבנה $\hat{M}$). קל לוודא כי φ מסתפקת ב־$\hat{M}$.
$\Rightarrow$: נניח שיש מבנה $\hat{M}$ בו ψ מסתפקת. נגדיר מבנה חדש עבור φ.

$$D^M = \left\{ [a] \;\mid a \in D^{\hat{M}} \right\}$$

אלה הן מחלקות השקילות של E ב־$D^{\hat{M}}$.

$$f\left([a_1],...,[a_n]\right)^M = \left[f^{\hat{M}}(a_1,...,a_n) \right]$$

[12] הבהרה במודל

ונאמר כי

$$([a_1], ..., [a_n]) \in R^M \iff (a_1, ..., a_n) \in R^{\hat{M}}$$

עבור בחירה כלשהי של נציגים.
כיוון ש־E יחס קונגרואנציה ההגדרה טובה.
לכל השמה $\hat{v}$ ב־$D^{\hat{M}}$ נגדיר השמה v ב־D^M ע"י

$$v(x) = [\hat{v}(x)]$$

ולהפך, לכל השמה v מעל D^M נגדיר $\hat{v}$ שתקיים $\hat{v}(x) \in v(x)$
כעת נטען שלכל נוסחה α מתקיים שאם $\hat{\alpha}$ זה התרגום של α ללא שוויון, אז $M, v \vDash \alpha$ אם ורק אם $\hat{M}, \hat{v} \vDash \hat{\alpha}$.
נוכיח באינדוקצית מבנה: בסיס: עבור נוסחה מהצורה $\alpha = (x = y)$

$$\hat{\alpha} = Equivalence(E) \wedge E(x, y)$$

אז$\hat{M}, \hat{v} \vDash \hat{\alpha}$ אם ורק אם $(\hat{v}(x), \hat{v}(y)) \in E^{\hat{M}}$ אם ורק אם $[\hat{v}(x)] = [\hat{v}(y)]$ אם ורק אם $M, v \vDash (x = y)$.
ונוסחה מהצורה: $\alpha = R(x_1, ..., x_n)$

$$\hat{\alpha} = (Cong(E, R) \wedge Equivalence(E) \wedge R(x_1, .., x_n))$$

הנוסחה $Cong(E, R)$ אומרת שהגדרת R^M טובה וקונסיסטנטית.
מעבר האינדוקציה:

- קשרים: סטנדרטי לגמרי.
- כמתים: נניח $\alpha = \forall x\, \beta$. אז $M, v \vDash \alpha$ אם ורק אם לכל $[a]$

$$M, v\, [{}^{[a]}/_{x}] \vDash \beta$$

אם ורק אם

$$\hat{M}, \hat{v}\, [{}^{a}/_{x}] \vDash \hat{\beta}$$

אם ורק אם $\hat{M}, \hat{v} \vDash \forall x\, \hat{\beta}$.

■

מסקנה 4.9 משפט הקומפקטיות למילון עם שוויון.

משפט 4.10 לא קיים אלגוריתם לבעיית התקפות (משפט *Church*) (מאידך, ראינו פרוצדורה שאומרת "כן" לנוסחאות תקפות, ולא ועצרת כשהנוסחה אינה תקפה).

4.3 בעיית התקפות אינה כריעה

הגדרה 4.11 בעיית העצירה: בהינתן מכונת טיורינג, צריך להכריע האם המכונה עוצרת על הקלט הריק.

משפט 4.12 לא קיים אלגוריתם לבעיית העצירה [מודלים חישוביים].

הגדרה 4.13 בעיית הריצוף: קלט: "לבנים" 1×1 עם צדדים צבועים (מספר סופי של סוגי לבנים).
מטרה: לרצף את הרביע הראשון; צלעות משיקות צבועות באותו הצבע.
השאלה ־ האם קיים ריצוף כזה?

משפט 4.14 אין אלגוריתם לבעיית הריצוף (ע"י רדוקציה לבעיית העצירה).

הוכחה: הוכחת משפט Church (ע"י רדוקציה לבעיית הריצוף):
בהינתן קלט לבעיית הריצוף: $T_1, T_2, ..., T_k$, נגדיר מילון σ:

$$\sigma = \langle c, Succ, R_1(\cdot, \cdot), ..., R_k(\cdot, \cdot) \rangle$$

R_i "יקודד" את המקומות בהם ריצפנו ב־T_i.

1.

$$\forall x,y\bigvee_{i=1}^{k}R_i(x,y)$$

2. לכל $i\neq j$

$$\forall x,y\,R_i(x,y)\to\neg R_j(x,y)$$

3. לכל T_i נגדיר Top_i,$Right_i$:

$$\begin{aligned}Top_i &= \{j\mid T_j \text{ can be placed above } T_i\}\\ Right_i &= \{j\mid T_j \text{ can be placed to the right of } T_i\}\end{aligned}$$

4. אז לכל i

$$\forall u,v\,R_i(u,v)\to\left(\bigvee_{j\in Top_i}R_j(u,Succ(v))\wedge\bigvee_{j\in Right_i}R_j(Succ(u),v)\right)$$

נגדיר את φ להיות ה־$\wedge$ של כל הנוסחאות הנ"ל. נשים לב: φ שקולה לפסוק אוניברסלי.

נטען ש־φ ספיק אם ורק אם יש ריצוף.

אם יש ריצוף:

$$M=\left\langle\mathbb{N},0,+1,..,R_i^M,..\right\rangle$$

כש־R_i^M כל המקומות בהם ריצפנו ב־T_i; קל לוודא ש־φ מסתפקת.

אם φ ספיקה: לפי משפט הרברנד היא מסתפקת במבנה הרברנד. מבנה הרברנד כשיש קבוע ופונקציה חד מקומית יחידה הוא $\mathbb{N}$, וניתן לראות שהמבנה מגדיר ריצוף. ■

4.3.1 מילון עבורו ניתן להכריע את בעיית התקפות

מילון σ יקרא מונאדי אם במילון יש רק יחסים חד מקומיים (בלי פונקציות ובלי שוויון).

משפט 4.15 משפט המבנה הקטן

אם נוסחה φ המוגדרת מעל מילון מונאדי ספיקה, אז היא ספיקה במבנה סופי (אם יש בה k יחסים היא ספיקה במבנה בגודל 2^k, k יכול להיות עצמה אינסופית).

הוכחה: נניח $\sigma=\langle P_1,..,P_k\rangle$ יחסים חד מקומיים.

נניח M מבנה בו φ מסתפקת. נגדיר יחס שקילות על M:[13]

$$a\sim b\iff(\forall P_i\,a\in P_i\Leftrightarrow b\in P_i)$$

יש לכל היותר 2^k מחלקות שקילות ונגדיר מבנה חדש $\hat{M}$ שאיבריו הם מחלקות השקילות הנ"ל ונפרש את P_i באופן הטבעי.

$[a]\in P_i^{\hat{M}}$ אם ורק אם $a\in P_i^M$; ומוכיחים באינדוקצית מבנה ש־φ מסתפקת ב־$\hat{M}$. ■

5 מערכת הוכחה ללוגיקה מסדר ראשון

הרצאה 12 - 7.6.15 **תזכורת (תחשיב הפסוקים):** 3 אקסיומות, כלל היסק $MP=\frac{\alpha,\alpha\to\beta}{\beta}$.

הגדרה 5.1 אקסיומות למערכת הוכחה[14]

A_1: $\alpha\to(\beta\to\alpha)$

A_2: $(\alpha\to(\beta\to\gamma))\to((\alpha\to\beta)\to(\alpha\to\gamma))$

A_3: $(\neg\beta\to\neg\alpha)\to(\alpha\to\beta)$

A_4: $\forall x\,\alpha(x)\to\alpha\left[{}^{t}/{}_{x}\right]$ לכל שם עצם t החופשי להצבה ב־x ב־α

A_5: $\forall x\,(\varphi\to\psi)\to(\varphi\to\forall x\,\psi)$ כאשר x אינו חופשי ב־φ

דוגמאות:

- $\forall x\,(\varphi\vee\psi)\to\varphi\vee\forall x\,\psi$ כאשר x אינו חופשי ב־φ
- $\forall x\,(\varphi\to\psi)\to(\varphi\to\forall x\,\psi)$

הגדרה 5.2 כללי היסק

- $$MP\quad:\quad\frac{(\alpha\to\beta)\,,\,\alpha}{\beta}$$
- $$Gen\quad:\quad\frac{\varphi(x)}{\forall x\,\varphi(x)}$$

הערה 5.3

- לא נבדיל בין נוסחאות שהתקבלו משינוי שם משתנה
- נאמר כי $\Gamma\underset{HC}{\vdash}\alpha$ אם α יכיח במערכת ההוכחה הנ"ל, מקבוצת נוסחאות Γ.
- HC היא מערכת הוכחה מעל $\{\neg,\to,\forall\}$
- לא מטפלים בשוויון; לא ניתן להוכיח במערכת ההוכחה הזאת $x=x$. אם רוצים לטפל בשוויון מוסיפים אקסיומות שמבטאות את העובדה ש־$=$ הוא יחס שקילות וקונגרואנציה.

5.1 משפטי השלמות והנאותות

משפט 5.4 הנאותות
אם $\Gamma\underset{HC}{\vdash}\alpha$ אז $\Gamma\overset{v}{\vDash}\alpha$

משפט 5.5 השלמות
אם $\Gamma\overset{v}{\vDash}\alpha$ אז $\Gamma\underset{HC}{\vdash}\alpha$

משפט 5.6 ניסוח שקול למשפט השלמות
אם Γ עקבית (יש פסוק שלא יכיח מ־Γ) אז יש מבנה בו היא נכונה.

[13] שימו לב זו הגדרה ולא נוסחה במילון

[14] תזכורת: זו סכמה לאקסיומות; כלומר האקסיומות הן כל ההצבות האפשריות של נוסחאות במקומות המתאימים

הוכחה: של משפט הנאותות
באינדוקצית מבנה מראים

$$\left\{\alpha \mid \Gamma \underset{HC}{\vdash} \alpha\right\} \subset \left\{\beta \mid \Gamma \overset{v}{\vDash} \beta\right\}$$

- בסיס:
  - אקסיומות ־ תקפות
  - הנחות ־ ברור
- פעולות:
  - MP: ברור
  - Gen: ברור. אם $\Gamma \overset{v}{\vDash} \beta$ אז גם $\Gamma \overset{v}{\vDash} \beta^{\forall}$.

■

טענה 5.7 נניח ש־α $\underset{HPC}{\vdash}$. לכל הצבה של נוסחאות ב־FOL למשתנים האטומים ב־α (נקרא לנוסחה החדשה $\hat{\alpha}$) מתקיים $\underset{HC}{\vdash} \hat{\alpha}$

הוכחה: תהי $\alpha_1, ..., \alpha_n = \alpha$ סדרת ההוכחה של α. אזי "$\hat{\alpha}_1, ..., \hat{\alpha}_n$" הוכחה של $\hat{\alpha}$ ב־HC. ■

5.2 משפט הדדוקציה

בתחשיב הפסוקים: אם $\Gamma, \alpha \underset{HPC}{\vdash} \beta$ אז $\Gamma \underset{HPC}{\vdash} (\alpha \rightarrow \beta)$
מה קורה בלוגיקה מסדר ראשון? נניח $R(x) \vdash \forall x\, R(x)$; מאידך $R(x) \rightarrow \forall x\, R(x)$. אם α פסוק הכל בסדר.

משפט 5.8 משפט הדדוקציה ל־HC
אם $\Gamma, \alpha \underset{HC}{\vdash} \beta$ ויש הוכחה של β מ־Γ, α שבה לא הפעלנו את Gen על אף משתנה חופשי ב־α, אז $\Gamma \underset{HC}{\vdash} (\alpha \rightarrow \beta)$.

הוכחה: באינדוקציה על אורך ההוכחה ("הטובה") של β מ־Γ, α. כלומר, נראה שאם $\beta_1, ..., \beta_n = \beta$ הוכחה של β מ־Γ, α בו לא הופעל כלל Gen על אף משתנה חופשי של α.
אזי לכל i, $\Gamma \vdash (\alpha \rightarrow \beta_i)$
φ: אקסיומה או הנחה מ־Γ או α. לפי A_1 $\varphi \rightarrow (\alpha \rightarrow \varphi)$ ואז $MP: \ \frac{\varphi, \varphi \rightarrow (\alpha \rightarrow \varphi)}{\alpha \rightarrow \varphi}$
נניח β_i התקבל מהפעלת MP; $\beta_j \rightarrow \beta_i$ ו־β_j הופיעו קודם בהוכחה.
לפי הנחת האינדוקציה $\alpha \rightarrow (\beta_j \rightarrow \beta_i)$ ואז $\alpha \rightarrow \beta_j$.
לפי A_2 ופעמיים MP נקבל $\alpha \rightarrow \beta_i$.
כעת נניח ש־β_i התקבל מהפעלת Gen על β_j. נאמר $\beta_i = \forall y\, \beta_j$ כאשר y אינו חופשי ב־α. לפי הנחת האינדוקציה, הוכחנו $\Gamma \underset{HC}{\vdash} (\alpha \rightarrow \beta_j)$. לפי Gen נקבל $\forall y\, (\alpha \rightarrow \beta_j)$
לפי A_5

$$\forall y\, (\alpha \rightarrow \beta_j) \rightarrow \left(\alpha \rightarrow \underbrace{\forall y\, \beta_j}_{\beta_i}\right)$$

כי y לא חופשי ב־α. MP וסיימנו. ■

5.3 משפט הדיכוטומיה

בתחשיב הפסוקים: אם $\Gamma, \alpha \underset{HPC}{\vdash} \beta$ וגם $\Gamma, \neg\alpha \underset{HPC}{\vdash}$ אז $\Gamma \underset{HPC}{\vdash} \beta$.
מה קורה בלוגיקה מסדר ראשון?

משפט 5.9 משפט הדיכוטומיה ב־HC
אם $\Gamma, \alpha \underset{HC}{\vdash} \beta$ וגם $\Gamma, \neg\alpha \underset{HC}{\vdash} \beta$ וניתן לכתוב כל אחת מההוכחות ללא הפעלת כלל Gen על אף משתנה חופשי ב־α, אז $\Gamma \underset{HC}{\vdash} \beta$.

הוכחה: אנו עומדים בתנאי משפט הדדוקציה ולכן $\Gamma \underset{HC}{\vdash} \alpha \to \beta$, $\Gamma \underset{HC}{\vdash} \neg\alpha \to \beta$
כעת, $(\alpha \to \beta) \to ((\neg\alpha \to \beta) \to \beta)$. מתקבל מהצבה לטאוטולוגיה פסוקית

$$((p \to q) \to ((\neg p \to q) \to q))$$

יכיח ב־HC (לפי טענה שהוכחנו). כעת נשתמש ב־MP פעמיים ונקבל הוכחה של β מ־Γ. ■

משפט 5.10 יהי c סימן קבוע שלא מופיע ב־Γ או ב־α. אז אם $\Gamma \underset{HC}{\vdash} \alpha\left[{}^{c}/_{x}\right]$ אז $\Gamma \underset{HC}{\vdash} \forall x\, \alpha(x)$.

הוכחה: באינדוקציה על אורך ההוכחה של $\alpha\left[{}^{c}/_{x}\right]$ מ־Γ. יהי y משתנה שלא מופיע בהוכחה של $\alpha\left[{}^{c}/_{x}\right]$ מ־Γ (ולא מופיע ב־α)
תהא $\alpha_1, ..., \alpha_n$ סדרת ההוכחה של $\alpha\left[{}^{c}/_{x}\right]$ מ־Γ. תהא $\hat{\alpha}_1, ..., \hat{\alpha}_n$ סדרת הנוסחאות המתקבלת ע"י החלפת כל מופע של c ב־y.
נראה באינדוקצית מבנה כי $\hat{\alpha}_1, ..., \hat{\alpha}_n$ הוכחה של $\alpha\left[{}^{y}/_{x}\right]$.

- אם זו אקסיומה: מיידי.
- הנחה מ־G: לא מכילה את c ולכן לא השתנתה
- MP: פשוט
- Gen: $\alpha_i = \forall z\, \alpha_j$. אז $\hat{\alpha}_i = (\forall z\, \alpha_j)\left[{}^{y}/_{c}\right] = \forall z\ (\alpha_j\left[{}^{y}/_{c}\right]) = \forall z\, \hat{\alpha}_j$

הראינו $\Gamma \underset{HC}{\vdash} \alpha\left[{}^{y}/_{x}\right]$. לפי Gen $\Gamma \vdash \forall y\, \alpha\left[{}^{y}/_{x}\right]$ שקול (החלפת שם) ל־$\forall x\, \alpha(x)$. ■

תזכורת: הוכחת משפט השלמות ב־HPC: בתחשיב הפסוקים הוכחנו שאם Γ עקבית אז Γ ספיקה.

- שלב 1: כל Γ עקבית מוכלת ב־Γ' עקבית מקסימלית (לכל φ, $\varphi \in \Gamma'$ או $\neg\varphi \in \Gamma'$)
- שלב 2: כל קבוצה עקבית מקסימלית, ספיקה. וההשמה מתקבלת ע"י בחירת הפסוקים המתאימים.

ב־HC האסטרטגיה דומה, אבל ההגדרות קצת שונות.

- נראה שאם Γ עקבית מעל σ אז היא מוכלת ב־Γ' (עקבית) מעל $\Sigma \supset \sigma$ שהיא שלמה ובעלת תכונת הנקין.
- נראה שכל קבוצה עקבית שלמה בעלת תכונת הנקין, ספיקה.

הגדרה 5.11 קבוצת נוסחאות Γ (אולי מעל $\sigma \subset \Sigma$) היא שלמה עבור מילון σ אם לכל פסוק φ מעל σ מתקיים $\varphi \in \Gamma$ או $\neg\varphi \in \Gamma$.

הערה 5.12 כשמוכיחים את משפט השלמות די לדבר על קבוצת פסוקים Γ כי $\Gamma \overset{v}{\vDash} \alpha$ אם ורק אם $\Gamma^{\forall} \overset{v}{\vDash} \alpha$ וברור שאם $\Gamma^{\forall} \underset{HC}{\vdash} \alpha$ אז $\Gamma \underset{HC}{\vdash} \alpha$.

משפט 5.13 אם Γ עקבית מעל σ אז יש $\Gamma \subset \Gamma'$ עקבית ושלמה מעל σ.

נוכיח למקרה σ סופי או בן מניה. **הוכחה:** יש מספר בן מניה של פסוקים מעל σ: $\{\varphi_1, \varphi_2, ...\}$

נגדיר באינדוקציה: $\Gamma_0 = \Gamma$

אם $\Gamma \cup \{\varphi_n\}$ עקבית אז $\Gamma_n = \Gamma_{n-1} \cup \{\varphi_n\}$; אחרת $\Gamma_n = \Gamma_{n-1} \cup \{\neg\varphi_n\}$

לבסוף $\Gamma' = \bigcup_m \Gamma_m$

ברור כי Γ' שלמה, נראה כי היא עקבית (יש β שלא יכיח ממנה). אם Γ' אינה עקבית, אז יש n כך ש-Γ_n אינה אינה עקבית.

נראה באינדוקציה על i שכל Γ_i עקבית. עבור $i = 0$, $\Gamma_0 = \Gamma$. נניח כי Γ_i עקבית. אם $\Gamma \cup \{\varphi_{i+1}\}$ עקבית אז Γ_{i+1} עקבית. נראה שלא יתכן שגם $\Gamma_i \cup \{\varphi_{i+1}\}$ וגם $\Gamma_i \cup \{\neg\varphi_{i+1}\}$ לא עקביות.

יהי β כלשהו. אם שתי הקבוצות אינן עקביות אז $\Gamma_i \cup \{\varphi_{i+1}\} \vdash \beta$ וגם $\Gamma_i \cup \{\neg\varphi_{i+1}\} \vdash \beta$.

כיוון ש-φ_{i+1} פסוק, נקבל לפי משפט הדיכוטומיה, $\Gamma_i \underset{HC}{\vdash} \beta$ בסתירה לעקביות Γ_i. ■

הגדרה 5.14 ל-Γ יש את תכונת הנקין (*Henkin*) עבור מילון σ אם לכל פסוק $\varphi \in \Gamma$ מעל σ מהצורה $\varphi = \neg\forall x\,\psi(x)$ יש c במילון Σ כך ש-$\neg\psi\,[c/x] \in \Gamma$.[15]

משפט 5.15 משפט הנקין: אם Γ עקבית מעל מילון σ אז יש Δ עקבית, בעלת תכונת הנקין ל-σ, מעל מילון $\Sigma \subset \sigma$ כך ש-$\Gamma \subset \Delta$.   הרצאה 13 - 12.6.15

רעיון ההוכחה: לכל נוסחה φ כנ"ל נוסיף למילון קבוע חדש ול-Γ את הפסוק $\neg\psi\,[c/x]$.

למה 5.16 אם Γ עקבית, $\neg\forall x\,\psi \in \Gamma$ פסוק ו-c קבוע חדש אז $\Gamma \cup \{\neg\psi\,[c/x]\}$ עקבית.

הוכחה: של הלמה: אם הקבוצה אינה עקבית אז $\Gamma \cup \{\neg\psi\,[c/x]\} \vdash \alpha, \neg\alpha$ לכל פסוק α. כיוון ש-$\neg\psi\,[c/x]$ פסוק (אין לו משתנים חופשיים), נוכל להשתמש במשפט הדדוקציה ונקבל:

$$\begin{aligned} \Gamma &\vdash \neg\psi\,[c/x] \to \alpha \\ \Gamma &\vdash \neg\psi\,[c/x] \to \neg\alpha \end{aligned}$$

לכל γ, δ,

$$\underset{HC}{\vdash} (\gamma \to \delta) \to ((\gamma \to \neg\delta) \to \neg\gamma)$$

זו טאוטולוגיה בתחשיב הפסוקים, ולכן קל לראות שזה יכיח ב-HC. אז נקבל:

$$\vdash (\neg\psi\,[c/x] \to \alpha) \to ((\neg\psi\,[c/x] \to \neg\alpha) \to \neg\neg\psi\,[c/x])$$

נפעיל MP פעמיים ונקבל $\Gamma \underset{HC}{\vdash} \neg\neg\psi\,[c/x]$, ולפי ההוכחה בתחשיב הפסוקים: $\Gamma \vdash \psi\,[c/x]$.

לבסוף לפי משפט שהוכחנו, כיוון ש-c קבוע חדש: $\Gamma \vdash \forall x\,\psi(x)$.

הבנו שיש פסוק φ כך ש-$\Gamma \vdash \varphi, \neg\varphi$ ($\varphi = \forall x\,\psi(x)$)

$$\vdash \varphi \to (\neg\varphi \to \alpha)$$

לכל α ומכאן $\Gamma \vdash \alpha$ לכל α, כלומר Γ אינה עקבית. ■

הוכחה: של משפט הנקין: תהי Γ עקבית, לכל פסוק $\varphi \in \Gamma$ מהצורה $\varphi = \neg\forall x\,\psi$ נוסיף למילון קבוע חדש c ול-Γ את הפסוק $\neg\psi\,[c/x]$.

לפי הלמה, הקבוצה החדשה עדיין עקבית. ברור שבסוף התהליך נקבל קבוצה בעלת תכונת הנקין ביחס ל-σ.■

הערה 5.17 אם נחזור על התהליך מספר בן מניה של פעמים נקבל $\Delta \supset \Gamma$ מעל Σ בעלת תכונת הנקין ביחס ל-Σ.

מסקנה 5.18 (הרחבה של המשפט) אם Γ עקבית מעל σ אז יש $\Delta \supset \Gamma$ מעל $\Sigma \supset \sigma$ ועקבית, בעלת תכונת הנקין ביחס ל-Σ.

משפט 5.19 כל קבוצה עקבית Γ מעל σ מוכלת בקבוצה עקבית Δ מעל $\Sigma \supset \sigma$ שהיא שלמה ובעלת תכונת הנקין ביחס ל-Σ.

---

[15] מותר ש-Γ מעל $\Sigma \supseteq \sigma$

הוכחה: נסמן $\Gamma = \Gamma_0 = \Delta_0$ ו־$\sigma_0 = \sigma$. כעת Γ_i תהיה קבוצה עקבית ושלמה מעל σ_{i-1} המכילה את Δ_{i-1}. תהי Δ_i קבוצה עקבית בעלת תכונת הנקין המכילה את Γ_i. נקרא למילון שלה σ_i. ניקח

$$\Delta = \bigcup_{n=0}^{\infty} \Gamma_n$$
$$\Sigma = \bigcup_{n=0}^{\infty} \sigma_n$$

אז Δ עקבית, שלמה ובעלת תכונת הנקין ביחס ל־σ. מ־"סופיות" התכונות (כל פסוק סופי, ובכל שלב מספר כמתי $\forall$ קטן) קל לוודא ש־Δ אכן כזאת. ■

הוכחה: הוכחת משפט השלמות:

תהי Γ קבוצת פסוקים עקבית מעל σ. לפי המשפט, יש $\Gamma \subset \Delta$ עקבית, שלמה, ובעלת תכונת הנקין ביחס ל־$\sigma \subset \Sigma$.

ניקח מבנה הרברנד ל־Δ, נקרא לו M. נראה כיצד לפרש יחסים. יהי $R \in \Sigma$; תהא $(s_1^M, ..., s_n^M) \in \left(D^M\right)^n$ (s_1^M הוא האיבר ב־D^M המתאים לשם עצם סגור s_1)

אז נאמר ש־$(s_1^M, ..., s_n^M) \in \left(D^M\right)^n$ אם ורק אם $R(s_1, .., s_n) \in \Delta$.

כעת באינדוקצית מבנה מראים כי־$\varphi \in \Delta$ אם ורק אם $M \vDash \varphi$. משתמשים בתכונות מבנה הרברנד (במבנה הרברנד $M \vDash \forall x\, \varphi$ אם ורק אם לכל שם עצם סגור s מתקיים $M \vDash \varphi\left[{}^{s}/_{x}\right]$).

הראינו שאם Γ עקבית אז Γ ספיקה. נשים לב שאם Γ עקבית אז $\Gamma^\forall$ עקבית.

די להוכיח שלמות עבור Γ קבוצת פסוק ו־α פסוק. $\Gamma \overset{v}{\vDash} \alpha \Leftarrow \Gamma^\forall \vDash \alpha^\forall$. נביט ב־$\Gamma^\forall \cup \left\{\neg\alpha^\forall\right\}$, שהיא לא ספיקה ולכן לא עקבית. אז

$$\Gamma^\forall \cup \left\{\neg\alpha^\forall\right\} \vdash \neg\alpha^\forall, \alpha^\forall$$

אז כמו בתחשיב הפסוקים נקבל $\Gamma^\forall \underset{HC}{\vdash} \alpha^\forall$, אז $\Gamma \underset{HC}{\vdash} \alpha^\forall$ ואז $\Gamma \underset{HC}{\vdash} \alpha$ (בעזרת אקסיומה שנפטרת מכמתים). ■

6 המבחן

במבחן יש 4 שאלות, ללא בחירה. שאלה אחת של הוכח / הפרך.

אפשר ללמוד ממבחנים של אלכס וארנון ־ להתעלם משאלות עם $NDFOL$, לוגיקה טמפורלית או מושגים אחרים שאיננו מכירים.

אצל אלכס $[|\varphi|]_\rho^M$ ־ ערך אמת של φב־M תחת השמה ρ.