

לוגיקה מתמטית

10 במרץ 2012

תקציר

הסיכום מבוסס על הרצאותיו של פרופ' דורון פלד מאוניברסיטת בר אילן, בקורס 89-200 בלוגיקה מתמטית, לסמסטר א' תשע"ב 2011-2012. כולי תקווה שהסיכום יעזור בהבנת החומר הנלמד. לתיקונים, הערות ושאלות, אתם מוזמנים לשלוח לי אימייל mail@studenten.org.

תוכן עניינים

4	I לוגיקה של פסוקים	
4	1 תחביר הפסוקים	
4	1.1 הגדרת תחשיב הפסוקים	
5	1.2 הדרגה של נוסחא	
5	1.3 תתי-נוסחאות	
5	1.4 טבלאות האמת והסמנטיקה של השפה הלוגית	
6	1.5 טיאוטולוגיות וספיקות של נוסחא	
7	1.6 גרירה לוגית	
7	2 מערכת ההוכחה בלוגיקה של פסוקים	
7	2.1 הוכחה ומשמעותה	
8	2.2 משפט הדדוקציה	
9	2.3 הוכחה לפי מקרים	
9	2.4 נאותות	
10	2.5 שלמות	
12	II לוגיקה מסדר ראשון	
12	3 לוגיקה מסדר ראשון - מהי? הגישה הפורמלית, הסמנטיקה	
12	3.1 הגדרת השפה הפורמלית	
13	3.2 הסמנטיקה של לוגיקה מסדר ראשון	
14	3.3 משתנים קשורים וחופשיים	
15	4 מערכת ההוכחה של לוגיקה מסדר ראשון	
16	4.0.1 כללי הוכחה	
16	4.1 הוכחות בלוגיקה מסדר ראשון	
18	5 נאותות ושלמות, ספיקות וקונסיסטנטיות	
18	5.1 הקשר ההדוק בין קונסיסטנטיות וספיקות לשלמות ונאותות	
19	5.2 משפט הקומפקטיות	
20	5.3 משפט השלמות ללוגיקה מסדר ראשון	
21	6 משפט אי-השלמות של גדל	

22	לוגיקה מודלית III
22	לוגיקה מודלית פורמלית במבנה <i>Kripke</i> 7
24	דוגמא למשפחות מודלים 7.1
24	לוגיקה של ידע 7.2
25	לוגיקה טמפורלית 7.3
25	הגדרה פורמלית של לוגיקה טמפורלית 7.3.1
27	אימות תוכנה IV
27	הוכחת נכונות 8
28	הוכחת נכונות חלקית 8.1
29	רלטיוויזציה 8.1.1
30	הוכחת סיום, ולוגיקת <i>Hoare</i> 8.2
30	הערות לסיום V

חלק I

לוגיקה של פסוקים

1 תחביר הפסוקים

אחד העקרונות החשובים בלוגיקה הוא הפרדה בין התחביר, הסימון הכללי והכתיבה הנאותה של נוסחאות, והסמנטיקה, המשמעות של נוסחאות.

כיצד מגדירים סמנטיקה של לוגיקה? אם לוגיקה הינה שפה פורמלית, האם יש צורך להגדיר אותה באמצעות שפה פורמלית אחרת? ניתן להגדיר את הלוגיקה באופן מתמטי, אך רצינו להגדיר את המתמטיקה בלוגיקה.

כיצד נפתור זאת? הסמנטיקה מוגדרת בשפה טבעית, שתיקרא כאן "מטה שפה".

הלוגיקה תשמש להוכחות. הוכחות על לוגיקה יעשו במטה שפה.

1.1 הגדרת תחשיב הפסוקים

הגישה הפשוטה ביותר בלוגיקה, והגישה הראשונה שנעבור עליה כאן תהיה שפת תחשיב הפסוקים.

באופן אינטואיטיבי, נגדיר טענות בסיס A, B, C, \dots כך שלכל טענה שכזו, ניתן ערך 1 או 0. בהתאם לכך, נוכל לבנות טענות משורשות התלויות בנכונות או אי-נכונות של הטענות האחרות.

נתחיל בלהגדיר את שפת התחשיב הפסוקים, או בשם אחר, קבוצת הנוסחאות בשפה (קבוצת הנוסחאות הבנויות היטב).

יהיו הקבוצות

$$Var = \{p_0, p_1, \dots\}$$

$$Symb = \{\wedge, \vee, \neg, \rightarrow, T, F, (,)\}$$

האיברים של Var הינם האטומים של השפה (טענות הבסיס), ו- $Symb$ הינה קבוצת הקשרים הלוגיים שבשפה (למען בניית טענות משורשות).

הגדרה. נגדיר את קבוצת הנוסחאות הבנויות היטב (Well Formed Formulas-מ), בצורה האינדוקטיבית:

$$1. \text{ לכל } p_i \in Var, p_i \in WFF.$$

$$2. T \in WFF.$$

$$3. F \in WFF.$$

$$4. \text{ אם } \phi_1, \phi_2 \in WFF \text{ אזי } (\phi_1 \wedge \phi_2) \in WFF.$$

$$5. \text{ אם } \phi_1, \phi_2 \in WFF \text{ אזי } (\phi_1 \vee \phi_2) \in WFF.$$

$$6. \text{ אם } \phi_1, \phi_2 \in WFF \text{ אזי } (\phi_1 \rightarrow \phi_2) \in WFF.$$

$$7. \text{ אם } \phi \in WFF \text{ אזי } \neg\phi \in WFF.$$

הקבוצה $WFF_{\{\rightarrow, F\}} \subseteq WFF$ מוגדרת באופן דומה, אבל בשימוש רק בתנאים 1,3,6.

1.2 הדוגמה של נוסחא

ההגדרה האינדוקטיבית של WFF בונה את הנוסחאות בשלבים. הגדרות אינדוקטיביות הן בנייה מלמטה למעלה. משפט הקריאה היחידה מאפשר לנו לראות נוסחאות גם מלמעלה למטה בצורה חד משמעית.

הגדרה. תהי $rank : WFF \rightarrow \mathbb{N}$ המוגדרת באופן הבא:

1. נגדיר $WFF_0 = \{T, F\} \cup Var$. אם $\phi \in WFF_0$, אזי $rank(\phi) = 0$. אנחנו קוראים ל- WFF_0 גם נוסחאות אטומיות.

2. אם $\phi_1, \phi_2 \in WFF_n$, אזי $\neg\phi_1 \in WFF_{n+1}$, $\phi_1, \phi_2 \in WFF_n$ אזי $(\phi_1 \wedge \phi_2), (\phi_1 \vee \phi_2), (\phi_1 \rightarrow \phi_2)$ מגדירים $rank(\phi) \in \mathbb{N}$ המינימלי כך ש- $\phi \in WFF_n$.

1.3 תתי-נוסחאות

כל הנוסחאות המשמשות בבניה הרקורסיבית של נוסחא הן תתי הנוסחאות שלה.

למשל, לנוסחא $((p_1 \rightarrow F) \rightarrow (p_2 \rightarrow F))$ יש את תתי הנוסחאות:

$$p_1, (p_1 \rightarrow F), p_2, (p_2 \rightarrow F), ((p_1 \rightarrow F) \rightarrow (p_2 \rightarrow F))$$

נרשום לפעמים נוסחא בצורה פרמטרית $\phi(\phi_1, \phi_2, \dots, \phi_n)$. צורת כתיבה זו תשתמש בסימונים ϕ_i כממלאי מקום עבור נוסחאות.

למשל, אם $\phi(\phi_1, \phi_2) = ((\phi_1 \rightarrow F) \rightarrow (\phi_2 \rightarrow F))$, ונציב $\phi_1 = (p_1 \rightarrow p_3)$, $\phi_2 = (p_2 \rightarrow F)$ נקבל $((p_1 \rightarrow p_3) \rightarrow F) \rightarrow ((p_2 \rightarrow F) \rightarrow F)$.

1.4 טבלאות האמת והסמנטיקה של השפה הלוגית

משמעות נוסחא בנוייה היטב היא אלמנט מתוך הקבוצה $\{0, 1\}$, כאשר 0 הוא שקר ו-1 הוא אמת.

נבחין בין הערכים 0 ו-1 הסמנטיים ו- T ו- F הסינטקטיים. טבלאות האמת מתארות את התנהגות הקשרים הלוגיים \vee, \wedge, \neg .

המטרה של החלק הבא היא להגדיר את פונקציית המשמעות הנתונה בידי קבוצה של השמות. הטבלאות יכלו n ערכים של $\{0, 1\}$ ויחזירו $\{0, 1\}$, זאת אומרת שנוצרת פונקציה

$$\mathbb{T}\mathbb{T} : \{0, 1\}^k \rightarrow \{0, 1\}$$

נרצה לתת פירוט לכל אחד מהמשתנים האטומיים של הנוסחא, זאת אומרת, נשים $\{0, 1\}$ בכל אחד מהם. נגדיר $As = \{Z \mid Z : Var \rightarrow \{0, 1\}\}$ קבוצת ההשמות.

פונקציית המשמעות M הינה פונקציה $M : WFF \times As \rightarrow \{0, 1\}$

הגדרה. טבלת אמת מסדר n , הינה פונקצייה $\mathbb{T}\mathbb{T} : \{0, 1\}^n \rightarrow \{0, 1\}$. לכל אחד מהקשרים הלוגיים $\wedge, \vee, \rightarrow$ נשייך טבלת אמת בינארית:

$$\mathbb{T}\mathbb{T}_{\wedge}(0, 0) = 0, \mathbb{T}\mathbb{T}_{\wedge}(0, 1) = 0, \mathbb{T}\mathbb{T}_{\wedge}(1, 0) = 0, \mathbb{T}\mathbb{T}_{\wedge}(1, 1) = 1$$

$$\mathbb{T}\mathbb{T}_{\vee}(0, 0) = 0, \mathbb{T}\mathbb{T}_{\vee}(0, 1) = 1, \mathbb{T}\mathbb{T}_{\vee}(1, 0) = 1, \mathbb{T}\mathbb{T}_{\vee}(1, 1) = 1$$

$$\mathbb{T}\mathbb{T}_{\rightarrow}(0, 0) = 1, \mathbb{T}\mathbb{T}_{\rightarrow}(0, 1) = 1, \mathbb{T}\mathbb{T}_{\rightarrow}(1, 0) = 0, \mathbb{T}\mathbb{T}_{\rightarrow}(1, 1) = 1$$

$$\mathbb{T}\mathbb{T}_{\neg}(0) = 1, \mathbb{T}\mathbb{T}_{\neg}(1) = 0$$

כמו כן, מוגדר $\mathbb{T}\mathbb{T}_T = 1$ ו- $\mathbb{T}\mathbb{T}_F = 0$.

כעת, נגדיר את פונקציית המשמעות $M_{PL} : \mathbb{WFF} \times \mathcal{A}s \rightarrow \{0, 1\}$ על השמת אמת z באופן האינדוקטיבי הבא:

$$1. M_{PL}(p_i, z) = z(p_i)$$

$$2. M_{PL}(T, z) = \mathbb{T}\mathbb{T}_T = 1$$

$$3. M_{PL}(F, z) = \mathbb{T}\mathbb{T}_F = 0$$

$$4. M_{PL}((\phi_1 \wedge \phi_2), z) = \mathbb{T}\mathbb{T}_{\wedge}(M_{PL}(\phi_1, z), M_{PL}(\phi_2, z))$$

$$5. M_{PL}((\phi_1 \vee \phi_2), z) = \mathbb{T}\mathbb{T}_{\vee}(M_{PL}(\phi_1, z), M_{PL}(\phi_2, z))$$

$$6. M_{PL}((\phi_1 \rightarrow \phi_2), z) = \mathbb{T}\mathbb{T}_{\rightarrow}(M_{PL}(\phi_1, z), M_{PL}(\phi_2, z))$$

$$7. M_{PL}(\neg\phi, z) = \mathbb{T}\mathbb{T}_{\neg}(M_{PL}(\phi, z))$$

באותו אופן פונקציית המשמעות $M_{\{\rightarrow, F\}}$ מוגדרת עבור נוסחאות ב- $\mathbb{WFF}_{\{\rightarrow, F\}}$, כצמצום של הפונקציה M_{PL} .

1.5 טיאוטולוגיות וספיקות של נוסחא

נוסחאות אשר לכל השמת אמת מחזירות ערך 1, נקראות **טיאוטולוגיות**.

כיצד ניתן להוכיח שנוסחא היא טיאוטולוגיה? ניתן לבדוק ע"י בדיקת כל השמת אמת, ולבדוק כי אכן הנוסחא מחזירה 1 לכל השמה שכזאת. אלגוריתם זה אינו יעיל שכן קיימות 2^n השמות אמת, כאשר n הינו מספר המשתנים בנוסחא. בהמשך נדבר על מערכת הוכחה, המאפשרת להוכיח זאת באופן יותר פשוט.

נאמר שנוסחא היא ספיקה (ברת סיפוק) אם קיימת השמת אמת למשתנה הנותנת ערך לוגי 1.

קל לראות כי אכן כל טיאוטולוגיה היא ברת סיפוק. האם קיים קשר נוסף?

• לכל ϕ טיאוטולוגיה, $\neg\phi$ אינה ברת סיפוק, ולהיפך.

• לכל נוסחא ϕ שאינה ברת סיפוק, $\neg\phi$ היא טיאוטולוגיה.

1.6 גרירה לוגית

נאמר שקבוצת פסוקים Σ גוררת לוגית את φ אם לכל השמות אמת שמספקת את כל הנוסחאות ב- Σ , מספקת את φ . נסמן זאת ב- $\Sigma \models \varphi$.

נאמר ש- $\Sigma \vdash \varphi$, אם אנחנו יכולים להוכיח את φ מ- Σ . כלומר, קיימת שרשת הוכחה שמשתמשת בהנחות מ- Σ , אקסיומות, וכללי הוכחות (למשל MP), ומסתיימת ב- φ .

למה. $\Sigma \cup \{\varphi \rightarrow F\} \models \varphi \iff \Sigma \models \varphi$. אינה ברית סיפוק.

נניח ש- $\Sigma \models \varphi$, אזי, כל השמות אמת שמספקת את Σ מספקת את φ , ולכן לא יכולה לספק את $\{\varphi \rightarrow F\}$. לצד השני, נניח ש- $\Sigma \cup \{\varphi \rightarrow F\} \models \varphi$, אינה ברית סיפוק. אזי, כל השמות אמת שמספקת את Σ לא מספקת את $\{\varphi \rightarrow F\}$, ולכן מספקת את φ .

2 מערכת ההוכחה בלוגיקה של פסוקים

מהי מערכת הוכחה? ביומיום, אנחנו מוכיחים טענות מתמטיות בשימוש באקסיומות, משפטים שהוכחנו, וכלל הוכחה המאפשר לנו הסקת מסקנות מנכונות של מספר טענות בריחדי.

נכליל את הרעיון, ונאמר שמערכת הוכחה בתחשיב הפסוקים היא קבוצת אקסיומות Γ וכללי הוכחות, כך שכל הוכחה תהיה סדרה סופית של טענות.

נגדיר כעת את מערכת ההוכחה שלנו ע"י האקסיומות הבאות

1. אקסיומה A1: $(\varphi \rightarrow (\psi \rightarrow \varphi))$.

2. אקסיומה A2: $((\varphi \rightarrow (\psi \rightarrow \eta)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \eta)))$.

3. אקסיומה A3: $((\varphi \rightarrow F) \rightarrow F) \rightarrow \varphi$.

עם שימוש בכלל ההיסק MP-Modus Ponens, האומר: אם מניחים $\{\varphi \rightarrow \psi, \varphi\}$ מסיקים ψ .

2.1 הוכחה ומשמעותה

בכל שלב בהוכחה $\Sigma \vdash \varphi$, יכול להופיע או פסוק מ- Σ , או אקסיומה, ואם הופיעו ההנחות של MP אז המסקנה של MP יכולה להופיע.

בכל שלב נרשום גם את ההצדקה לשלב הבא. נשים לב כי המשמעות של הוכחה $\Sigma \vdash \varphi$ הינה כי ההוכחה היא $\Sigma \models \varphi$.

דוגמא. $\emptyset \vdash (\varphi \rightarrow \varphi)$

1. $(\varphi \rightarrow ((\varphi \rightarrow \varphi) \rightarrow \varphi)), \dots, \dots, \dots, A1$

2. $((\varphi \rightarrow ((\varphi \rightarrow \varphi) \rightarrow \varphi)) \rightarrow ((\varphi \rightarrow (\varphi \rightarrow \varphi)) \rightarrow (\varphi \rightarrow \varphi))), \dots, \dots, \dots, A2$

3. $((\varphi \rightarrow (\varphi \rightarrow \varphi)) \rightarrow (\varphi \rightarrow \varphi)) \dots \dots \dots MP(1,2)$
4. $(\varphi \rightarrow (\varphi \rightarrow \varphi)) \dots \dots \dots A1$
5. $(\varphi \rightarrow \varphi) \dots \dots \dots MP(4,3)$

דוגמא. $\{F\} \vdash \varphi$.

1. $F \dots \dots \dots Assumption$
2. $(F \rightarrow ((\varphi \rightarrow F) \rightarrow F)) \dots \dots \dots A1$
3. $((\varphi \rightarrow F) \rightarrow F) \dots \dots \dots MP(1,2)$
4. $((\varphi \rightarrow F) \rightarrow F) \rightarrow \varphi \dots \dots \dots A3$
5. $\varphi \dots \dots \dots MP(3,4)$.

נדגיש כי אם ניתן להוכיח פסוק מסוים φ מקבוצת פסוקים Σ , אזי ניתן להוכיח את φ גם מכל קבוצה המכילה את Σ . ההוכחה לכך פשוטה, אפשר פשוט לחזור על כל סדרת ההוכחה, מבלי להשתמש בפסוקים הנוספים.

2.2 משפט החדוקציה

משפט. $\Sigma \vdash \varphi \rightarrow \psi$ אם ורק אם $\Sigma \cup \{\varphi\} \vdash \psi$.

הוכחה. בכיוון \Leftarrow , נניח ש- $\Sigma \vdash (\varphi \rightarrow \psi)$, אזי, $\Sigma \subseteq \Sigma \cup \{\varphi\}$, לכן $\Sigma \cup \{\varphi\} \vdash (\varphi \rightarrow \psi)$. נשתמש בסוף ההוכחה בכלל MP לקבל את ψ . כלומר, $\Sigma \cup \{\varphi\} \vdash \psi$.

בכיוון \Rightarrow , נביט בסדרת ההוכחה של $\Sigma \cup \{\varphi\} \vdash \psi$, ונראה באינדוקציה על אורך סדרת ההוכחה שכל שורה שבה הוכחנו χ , ניתן להוכיח את $(\varphi \rightarrow \chi)$ מבלי להשתמש ב- φ כהנחה. כלומר, $\Sigma \vdash (\varphi \rightarrow \chi)$.

בסיס. נניח שאנו בשורה הראשונה של ההוכחה, נסמנה χ . אזי, לשורה הראשונה χ יש אפשרות להיות אקסיומה, או איבר של $\Sigma \cup \{\varphi\}$. אם השורה היא φ , אזי, נידרש להוכיח את $\varphi \rightarrow \varphi$, וזה ניתן להוכחה מכל Σ (הוכחנו קודם). עבור המקרה השני, השורה הראשונה היא או אקסיומה או איבר של Σ . אם χ מתקיים, אזי לפי אקסיומה $A1$, מתקיים $(\varphi \rightarrow \chi)$, ועם MP נסיק כי $(\varphi \rightarrow \chi)$, רק בעזרת Σ , כנדרש.

הוכחה. נניח כי אנו בשורה כלשהי χ , ואנחנו מניחים נכונות לכל השורות הקודמות. אזי, אם χ אקסיומה או איבר מ- $\Sigma \cup \{\varphi\}$, ניתן להוכיח כי $\Sigma \vdash (\varphi \rightarrow \chi)$ באותו אופן.

האפשרות השניה היא ש- χ מתקבלת באמצעות MP משתי שורות קודמות, שורה μ ושורה $\mu \rightarrow \chi$. לפי הנחת האינדוקציה, $\Sigma \vdash (\varphi \rightarrow \mu)$, $\Sigma \vdash (\varphi \rightarrow (\mu \rightarrow \chi))$.

נשתמש באקסיומה $A2$ לקבל $((\varphi \rightarrow (\mu \rightarrow \chi)) \rightarrow ((\varphi \rightarrow \mu) \rightarrow (\varphi \rightarrow \chi)))$, ונשתמש פעמיים ב- MP , ונקבל $(\varphi \rightarrow \chi)$.

זה נכון גם עבור השורה האחרונה ψ , ולכן נקבל $\Sigma \vdash (\varphi \rightarrow \psi)$. מ.ש.ל.

באמצעות משפט הדדוקציה ניתן להוכיח טענות חשובות, כגון טרנזיטיביות הגרירה, ואת Contrapositive. (אם מניחים $\varphi \rightarrow \psi$, אזי ניתן להסיק $(\varphi \rightarrow F) \rightarrow (\psi \rightarrow F)$.)

2.3 הוכחה לפי מקרים

נוכיח כי אם $\Sigma \cup \{\varphi\} \vdash \psi$ וגם $\Sigma \cup \{\varphi \rightarrow F\} \vdash \psi$, אזי $\Sigma \vdash \psi$.

הוכחה.

1. $\Sigma \vdash (\varphi \rightarrow \psi)$Deduction From $\Sigma \cup \{\varphi\} \vdash \psi$
2. $\Sigma \vdash (\varphi \rightarrow F) \rightarrow \psi$Deduction From $\Sigma \cup \{\varphi \rightarrow F\} \vdash \psi$
3. $\Sigma \vdash (((\varphi \rightarrow F) \rightarrow F) \rightarrow \varphi)$A3
4. $\Sigma \vdash (((\varphi \rightarrow F) \rightarrow F) \rightarrow \psi)$Transitivity of 3,1
5. $\Sigma \vdash ((\psi \rightarrow F) \rightarrow ((\varphi \rightarrow F) \rightarrow F))$Contrapositive of 2.
6. $\Sigma \vdash ((\psi \rightarrow F) \rightarrow \psi)$Transitivity of 5,4
7. $\Sigma \vdash ((\psi \rightarrow F) \rightarrow (\psi \rightarrow F))$Idempotence ($\chi \rightarrow \chi$)
8. $\Sigma \vdash ((\psi \rightarrow F) \rightarrow (\psi \rightarrow F)) \rightarrow (((\psi \rightarrow F) \rightarrow \psi) \rightarrow ((\psi \rightarrow F) \rightarrow F))$A2
9. $\Sigma \vdash (((\psi \rightarrow F) \rightarrow \psi) \rightarrow ((\psi \rightarrow F) \rightarrow F))$MP(7,8)
10. $\Sigma \vdash ((\psi \rightarrow F) \rightarrow F)$MP(6,9)
11. $\Sigma \vdash (((\psi \rightarrow F) \rightarrow F) \rightarrow \psi)$A3
12. $\Sigma \vdash \psi$MP(10,11).

2.4 נאותות

נאמר שמערכת היסק היא נאותה, כלומר, אם לכל קבוצת פסוקים Σ ופסוק φ , אם $\Sigma \vdash \varphi$, אזי $\Sigma \models \varphi$. המשמעות של דבר כזה היא שהמערכת שהגדרנו היא "נכונה". כלומר, שהאקסיומות שהגדרנו עבור המערכת **נכונות** לוגית, ושכלל ההוכחה שלנו משמר נכונות.

כמו כן, נאמר שמערכת היא שלמה אם עבור כל קבוצת פסוקים Σ ופסוק φ , אם $\Sigma \models \varphi$, אזי $\Sigma \vdash \varphi$. המשמעות של דבר כזה היא שכל דבר שנכון **לוגית**, ניתן להוכיח אותו במסגרת כללי ההוכחה שהגדרנו.

המערכת שהצגנו, מערכת אקסיומות Lyndon וכלל ההוכחה MP , הינה נאותה. ניתן להוכיח זאת באינדוקציה על סדרת ההוכחה, כאשר האקסיומות תמיד מתקיימות, וכלל MP משמר נכונות.

2.5 שלמות

נרצה להוכיח כי לכל Σ ולכל φ , אם $\Sigma \models \varphi$, אזי $\Sigma \vdash \varphi$.

הוכחה.

נוכיח באופן שקול, כי אם $\Sigma \not\vdash \varphi$, אזי $\Sigma \not\models \varphi$. רעיון ההוכחה הוא להראות קיום של השמת אמת שמספקת את Σ אך לא מספקת את φ , מבלי למצוא מפורשות את ההשמה.

נניח כי $\Sigma \not\vdash \varphi$. ידוע כי קבוצת הפסוקים בלוגיקה הינה בת מניה, ולכן ניתן לסדר את כל הפסוקים בסדרה $\varphi_0, \varphi_1, \varphi_2, \dots$ וכך הלאה.

נגדיר קעת סדרה של קבוצות $\Sigma = \Sigma_0 \subseteq \Sigma_1 \subseteq \Sigma_2 \subseteq \dots$ באופן הבא:

1. אם $\Sigma_i \cup \{\varphi_i\} \not\vdash \varphi$, אזי $\Sigma_{i+1} = \Sigma_i \cup \{\varphi_i\}$. אחרת, $\Sigma_{i+1} = \Sigma_i$.

2. נגדיר $\Sigma^* = \Sigma_0 \cup \Sigma_1 \cup \Sigma_2 \cup \dots$.

נוכיח קעת טענות עזר על Σ^* .

טענה. עבור פסוק כלשהו ψ , לא ייתכן ש- $\psi \in \Sigma^*$ וגם $(\psi \rightarrow F) \in \Sigma^*$.

הוכחה. נניח בשלילה שכן. אזי, לפי הבנייה, קיים $i \in \mathbb{N}$ כך ש- $\psi = \varphi_i$. ואז, $\psi \in \Sigma_{i+1}$, $\psi \notin \Sigma_i$. באותו אופן קיים $j \in \mathbb{N}$ כך ש- $(\psi \rightarrow F) \in \Sigma_{j+1}$, $(\psi \rightarrow F) \notin \Sigma_j$. ניקח $n = \max\{i, j\}$. נקבל $(\psi \rightarrow F) \in \Sigma_{n+1}$ ונפעיל כלל MP ונקבל כי $\Sigma_{n+1} \vdash F$. ומכאן $\Sigma \vdash \varphi$ (כי ניתן להוכיח הכל עם F), בסתירה לבנייה!

□ הסתירה מוכיחה את הטענה.

טענה. עבור פסוק כלשהו ψ , לא ייתכן שגם ψ וגם $(\psi \rightarrow F)$ אינם נמצאים ב- Σ^* .

הוכחה. נניח בשלילה שכן. מכאן, לפי הבנייה, קיים $i \in \mathbb{N}$ כך ש- $\psi \in \Sigma_i \cup \{\psi\}$. כמו כן, קיים $j \in \mathbb{N}$ כך ש- $(\psi \rightarrow F) \in \Sigma_j \cup \{\psi \rightarrow F\}$. נסמן $n = \max\{i, j\}$. נקבל כי $\Sigma_n \cup \{\psi\} \vdash \varphi$ וכי $\Sigma_n \cup \{\psi \rightarrow F\} \vdash \varphi$. לפי הטענה "הוכחה לפי מקרים" שהוכחנו לעיל, נקבל $\Sigma_n \vdash \varphi$, בסתירה לבנייה!

□ הסתירה מוכיחה את הטענה.

כלומר, נוכל להסיק כי כל פסוק או השלילה שלו נמצאים ב- Σ^* , אך לא שניהם.

טענה. $(\chi \rightarrow \eta) \in \Sigma^* \iff \eta \in \Sigma^*$ או $(\chi \rightarrow F) \in \Sigma^*$.

הוכחה. עבור \Leftarrow , נניח ש- $(\chi \rightarrow \eta) \in \Sigma^*$. נניח בשלילה שגם $(\eta \rightarrow F) \in \Sigma^*$ וגם $\chi \notin \Sigma^*$. אזי, באותו אופן בהוכחות לעיל, קיים $n \in \mathbb{N}$ כך ש- $\{\chi, (\eta \rightarrow F)\} \subseteq \Sigma_n$. מכאן, נקבל בשימוש פעמיים ב- MP ש- $\Sigma_n \vdash F$, ומכאן נוכל לומר $\Sigma_n \vdash \varphi$, בסתירה לבנייה. ולכן נקבל את הדרוש.

עבור \Rightarrow , נניח ש- $\eta \in \Sigma^*$. אזי, קיים $i \in \mathbb{N}$ כך ש- $\eta \in \Sigma_i$. בעזרת אקסיומה $A1$, נקבל $\Sigma_i \vdash (\eta \rightarrow (\chi \rightarrow \eta))$, ועם MP נסיק $\Sigma_i \vdash (\chi \rightarrow \eta)$. בגלל שכל פסוק או שלילתו נמצאים ב- Σ^* , אם $(\chi \rightarrow \eta) \rightarrow F \in \Sigma^*$, אזי קיים $j \in \mathbb{N}$ כך ש- $(\chi \rightarrow \eta) \rightarrow F \in \Sigma_j$. ניקח $n = \max\{i, j\}$, ונקבל כי $\Sigma_n \vdash (\chi \rightarrow \eta)$. כמו כן,

, $((\chi \rightarrow \eta) \rightarrow F) \in \Sigma_n$, מכך נסיק כי $\Sigma_n \vdash F$, כלומר, $\Sigma_n \vdash \varphi$, בסתירה לבנייה. ולכן $((\chi \rightarrow \eta) \rightarrow F) \notin \Sigma^*$, ולכן, ולכן אם $\eta \in \Sigma^*$ אזי $(\chi \rightarrow \eta) \in \Sigma^*$.

כעת, נניח ש- $(\chi \rightarrow F) \in \Sigma^*$. אזי קיים $i \in \mathbb{N}$ כך ש- $(\chi \rightarrow F) \in \Sigma_i$. נרצה להראות ש- $\Sigma_i \vdash (\chi \rightarrow \eta)$, ואז נקבל, בדומה לעיל, שאם השלילה $((\chi \rightarrow \eta) \rightarrow F)$ היא ב- Σ^* , אזי קיים $n \in \mathbb{N}$ עבורו $\Sigma_n \vdash \varphi$. לפי משפט הדדוקציה, $\Sigma_i \cup \{\chi\} \vdash \eta \iff \Sigma_i \vdash (\chi \rightarrow \eta)$. אבל $(\chi \rightarrow F) \in \Sigma_i$, ולכן $\Sigma_i \cup \{\chi\} \vdash F$, ולכן $\Sigma_i \cup \{\chi\} \vdash \eta$, כנדרש. \square

כעת, מכל התוצאות לעיל נגיע לתוצאה הסופית, שהיא כי $\varphi \notin \Sigma$.

נגדיר סמנטיקה (פירוש של כל נוסחא לערך 0 או 1) באופן הבא, אם פסוק $\psi \in \Sigma^*$, אזי נאמר שמשמעותו 1. אחרת, 0. ראינו באמצעות טענות העזר, שאין שייך פסוק ושלילתו ל- Σ^* , ולכן אין זה מתנגש עם השלילה בסמנטיקה של טבלאות אמת.

הטענה השלישית מוכיחה לנו כי סמנטיקת הגרירה נשמרת גם היא בסמנטיקה שמשרה Σ^* . כלומר, אם הפסוק $(\chi \rightarrow \eta)$ מחזיר ערך אמת, אזי או ש- η מחזיר ערך אמת או ש- $\chi \rightarrow F$ מחזיר ערך אמת, כלומר, χ מחזיר ערך שקר, וגם להפך. כלומר, אם η מחזיר ערך אמת, או $\chi \rightarrow F$ מחזיר ערך אמת, אזי גם $(\chi \rightarrow \eta)$ מחזיר ערך אמת. זה נכון גם ב- Σ^* .

ולכן נוכל לומר שהסמנטיקה שמגדירה כך Σ^* שקולה לסמנטיקה של טבלאות האמת, כלומר, קיימת השמת אמת לקבוצת כל הפסוקים $\mathbb{WFF}_{\{\rightarrow, F\}}$, המתלכדת עם הסמנטיקה של שייכות ל- Σ^* .

ברור כי $\varphi \notin \Sigma^*$, כי אם כן, היה שלב בבנייה בו φ נכנס ל- Σ_n עבור $n \in \mathbb{N}$ כלשהו, וכמובן $\Sigma_n \vdash \varphi$ מיידית, בסתירה לבנייה. ולכן, המשמעות של φ תהיה 0.

כמו כן, $\Sigma \subseteq \Sigma^*$, ולכן כל ערכי האמת של כל הפסוקים ב- Σ הם 1. כלומר, בגלל שקילות הסמנטיקה, קיימת השמת אמת Z (שבעצם מושרית ע"י Σ^*) שמספקת את כל פסוקי Σ , אך אינה מספקת את φ . מכאן מיד נובע כי $\varphi \notin \Sigma$.

■

ובכאן נסיים את דברינו בלוגיקה של תחשיב הפסוקים, המהווה מבוא ללוגיקה מסדר ראשון, עליה נדבר בחלק הבא.

חלק II

לוגיקה מסדר ראשון

3 לוגיקה מסדר ראשון - מהי? הגישה הפורמלית, הסמנטיקה

בלוגיקה מסדר ראשון, במקום לדבר על השמות אמת לפסוקים, נדבר על עולם. העולם הוא מבנה מתמטי המכיל איברים, יחסים, קבועים, ופונקציות.

דוגמאות למבנים שניתן לתאר באמצעות לוגיקה מסדר ראשון:

1. מבנה של גרף $G = (V, E)$, כאשר המבנה הינו קבוצה V , ובעולם קיים יחס $E \subseteq V \times V$, כאשר $(v_1, v_2) \in E$ אם קיימת קשת מ- v_1 ל- v_2 בגרף.

2. המבנה של המספרים הטבעיים. הקבוצה במבנה היא $\mathbb{N} \cup \{0\}$, פונקציית חיבור $+\mathbb{N} : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, פונקציית כפל $\cdot\mathbb{N} : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$. כמו כן, קיימים הקבועים $0_{\mathbb{N}}, 1_{\mathbb{N}}$, והיחס $\leq_{\mathbb{N}} \subseteq \mathbb{N} \times \mathbb{N}$, שמשמעותו היא $(x, y) \in \leq_{\mathbb{N}}$ אם x קטן או שווה ל- y .

באופן דומה גם ניתן לדבר על המבנה של המספרים הממשיים, הרציונלים, ועוד.

באופן כללי, ניתן לדבר על מבנה כלשהו כ- $\langle X, f_X, g_X, r_X, c_X, d_X \rangle$, כאשר X הוא העולם עליו אנחנו מדברים, f_X, g_X הינן פונקציות, r_X היא יחס, ו- c_X, d_X הינם קבועים.

נרצה להגיד את השפה שלנו כדי שתתאים לתיאור מבנים מתמטיים, ולכן נגדיר כמה מושגים.

הגדרות.

1. נגדיר אוסף של סימני יחסים $R_{n,m}$, כאשר n הינו מספר הפרמטרים שהיחס מקבל, ו- m הינו סודר.
2. נגדיר אוסף של סימני פונקציות $f_{n,m}$, כאשר n הוא מספר הפרמטרים שהפונקציה מקבלת, ו- m הינו סודר.
3. נגדיר אוסף של קבועים C_m , כאשר m הינו סודר. (ניתן להסתכל על קבועים כפונקציות עם 0 פרמטרים)
4. נגדיר אוסף משתנים $v_i \in \mathbb{V}$.

נרצה לבטא בלוגיקה הזו בין היתר טענות על המבנים המתמטיים שדיברנו עליהם לעיל. למשל, הטענה כי "לכל צומת בגרף יש בדיוק k שכנים", או כי "יש אינסוף מספרים ממשיים". נגדיר את השפה של לוגיקה מסדר ראשון באופן כזה שנוכל לבטא את כל הטענות הללו.

3.1 הגדרת השפה הפורמלית

נגדיר כעת את מושג ה-"ביטוי" (term) באופן אינדוקטיבי להלן:

1. **ביסס**. המשתנים וסימני הקבועים הם ביטויים.
2. אם t_1, t_2, \dots, t_n הם ביטויים, ו- $f_{n,m}$ פונקציה המקבלת n פרמטרים, אזי $f_{n,m}(t_1, t_2, \dots, t_n)$ הינו ביטוי.

בנוסף לביטויים, גם הקשרים הלוגיים $\neg, \vee, \wedge, \rightarrow, \exists, \forall$ נכנסים לפעולה בשפה.

הגדרה. נגדיר נוסחא אטומית כהפעלת יחס $R_{n,m}(t_1, \dots, t_n)$ על קבוצה של ביטויים t_1, t_2, \dots, t_n . (או יחס נוסף של $=$)

סימן השיוויון לעיל, גם הוא הינו יחס בינארי, ונסמן אותו ע"י סימן מיוחד ע"מ לייחד את משמעותו בעתיד (להבטיח שסימן זה יקיים את אקסיומות השיוויון).

כעת נוכל להגדיר את מושג ה-"נוסחא", באופן דינדוקטיבי להלן:

1. **בסיס.** נוסחא אטומית היא נוסחא.

2. אם φ_1 ו- φ_2 נוסחאות, ו- v_i הוא משתנה, אזי גם $(\varphi_1 \wedge \varphi_2)$, $(\varphi_1 \vee \varphi_2)$, $\neg \varphi_1$, $(\varphi_1 \rightarrow \varphi_2)$, $\exists v_i \varphi_1$, $\forall v_i \varphi_1$ הן נוסחאות.

3.2 הסמנטיקה של לוגיקה מסדר ראשון

כעת, איך נפרש את השפה שהגדרנו?

נשייך את הסימנים שהגדרנו לאלמנטים מן המבנה המתמטי אותו אנו מתארים. כלומר, לסימני הפונקציות נתאים פונקציות אמיתיות בתוך המבנה, לסימני היחסים נתאים יחסים כלשהם המוגדרים על המבנה, ולסימני הקבועים נשייך קבועים במבנה.

באופן דומה ללוגיקה פסוקית, נגדיר פונקציית הצבה, שתיתן למשתנים בנוסחא ערך מעל המבנה המתמטי, ובאופן קורסיבי נגדיר את המשמעות של נוסחא בלוגיקה מסדר ראשון.

הגדרה. פונקציית הצבה $Z : \mathbb{V} \rightarrow X$, הינה פונקצייה הנותנת ערך במבנה המתמטי מעל הקבוצה X לכל משתנה $v_i \in \mathbb{V}$. כמו כן, נגדיר פונקצייה \mathbb{P} המייחסת לכל סימן פונקציה, סימן קבוע וסימן יחס לפונקציה ויחס במבנה.

כעת, נוכל להגדיר את פונקציית המשמעות, \mathbb{MT} , התייחס משמעות לביטויים:

1. **בסיס.** $\mathbb{MT}(v_i, Z) = Z(v_i)$. $\mathbb{MT}(c_i, Z) = \mathbb{P}(c_i)$.

2. אם t_1, \dots, t_n ביטויים, אזי $\mathbb{MT}(f_{n,m}(t_1, \dots, t_n), Z) = \mathbb{P}(f_{n,m})(\mathbb{MT}(t_1, Z), \dots, \mathbb{MT}(t_n, Z))$.

כעת, נגדיר את פונקציית המשמעות \mathbb{M} , התייחס ערכי אמת לנוסחאות.

1. **בסיס.** עבור נוסחא אטומית $R_{n,m}(t_1, \dots, t_n)$, $\mathbb{M}(R_{n,m}(t_1, \dots, t_n), Z)$ היא האם $(\mathbb{MT}(t_1, Z), \dots, \mathbb{MT}(t_n, Z)) \in \mathbb{P}(R_{n,m})$ (במילים, האם הביטויים מקיימים את היחס).

2. אם t_1, t_2 ביטויים, אזי $\mathbb{M}(t_1 = t_2, Z) = T$ אם $\mathbb{MT}(t_1, Z) = \mathbb{MT}(t_2, Z)$ ואם $\mathbb{MT}(t_1, Z) \neq \mathbb{MT}(t_2, Z)$.

3. אם φ_1, φ_2 נוסחאות, אזי,

$$\mathbb{M}(\varphi_1 \wedge \varphi_2, Z) = \mathbb{TT}_\wedge(\mathbb{M}(\varphi_1, Z), \mathbb{M}(\varphi_2, Z))$$

$$\mathbb{M}(\varphi_1 \vee \varphi_2, Z) = \mathbb{TT}_\vee(\mathbb{M}(\varphi_1, Z), \mathbb{M}(\varphi_2, Z))$$

$$\mathbb{M}(\varphi_1 \rightarrow \varphi_2, Z) = \mathbb{T}\mathbb{T}_{\rightarrow}(\mathbb{M}(\varphi_1, Z), \mathbb{M}(\varphi_2, Z))$$

$$\mathbb{M}(\neg\varphi_1, Z) = \mathbb{T}\mathbb{T}_{\neg}(\mathbb{M}(\varphi_1, Z))$$

4. אם φ נוסחא, מתקיים כי $\mathbb{M}(\exists v_i \varphi, Z) = T$, אם קיימת פונקציית הצבה \bar{Z} , השונה מההצבה Z עד כדי המשתנה v_i , כך ש- $\mathbb{M}(\varphi, \bar{Z}) = T$.

5. אם φ נוסחא, מתקיים כי $\mathbb{M}(\forall v_i \varphi, Z) = T$, אם לכל פונקציית הצבה \bar{Z} , השונה מההצבה Z עד כדי המשתנה v_i , מתקיים $\mathbb{M}(\varphi, \bar{Z}) = T$.

נוסחא יכולה להיות בעלת ערך אמת עבור הצבה כלשהי תחת כל מבנה, ויכולה להיות נכונה תחת מבנה ספציפי, ואינטרפרטציה ספציפית. למשל הנוסחא $\forall v_i (v_i = v_i)$ נכונה תחת כל מבנה בו מוגדר יחס השיוויון.

לעומת זאת, הנוסחא $\forall v (\exists u (R(u, v)))$, כאשר היחס R מבטא יחס $<$, תהיה נכונה עבור המספרים השלמים (כי לכל מספר קיים מספר שקטן ממנו), אך לא תהיה נכונה בהמספרים הטבעיים.

3.3 משתנים קשורים וחופשיים

נאמר שמשנתנה v הוא קשור בנוסחא φ , אם v נמצא תחת השפעה של כמת ב- φ (כאשר כמת משמעו \forall או \exists). אחרת, ייקרא v משנתנה חופשי.

נגדיר כעת פורמלית, בהינתן ביטוי t , את $var(t)$, המשתנים של הביטוי t ,

$$1. \text{ בסיס. אם } v \text{ משנתנה, אזי } var(v) = \{v\}$$

$$2. \text{ אם } t_1, \dots, t_n \text{ ביטויים, אזי } var(f_{n,m}(t_1, \dots, t_n)) = var(t_1) \cup \dots \cup var(t_n)$$

נגדיר כעת פורמלית, בהינתן נוסחא φ , את קבוצת המשתנים החופשיים שלה, $free(\varphi)$,

$$1. \text{ בסיס. אם } \varphi = R_{n,m}(t_1, \dots, t_n) \text{ נוסחא אטומית, אזי } free(\varphi) = var(t_1) \cup \dots \cup var(t_n). \text{ באופן דומה עובר " = "}$$

$$2. \text{ אם } \varphi_1, \varphi_2 \text{ נוסחאות, אזי,}$$

$$free(\varphi_1 \wedge \varphi_2) = free(\varphi_1) \cup free(\varphi_2)$$

$$free(\varphi_1 \vee \varphi_2) = free(\varphi_1) \cup free(\varphi_2)$$

$$free(\varphi_1 \rightarrow \varphi_2) = free(\varphi_1) \cup free(\varphi_2)$$

$$free(\neg\varphi_1) = free(\varphi_1)$$

$$free(\exists v \varphi_1) = free(\varphi_1) \setminus \{v\}$$

$$free(\forall v \varphi_1) = free(\varphi_1) \setminus \{v\}$$

למשל, כל הופעה של משתנה v בנוסחא φ , בנוסחא $\exists v_i \varphi$ ההופעה הינה קשורה.

נגדיר כעת פורמלית את קבוצת המשתנים הקשורים בנוסחא φ , $bound(\varphi)$,

1. **בסיס.** אם $\varphi = R_{n,m}(t_1, \dots, t_n)$ נוסחא אטומית, אזי $bound(\varphi) = \emptyset$. באופן דומה עבור " = " .

2. אם φ_1, φ_2 נוסחאות, אזי,

$$bound(\varphi_1 \wedge \varphi_2) = bound(\varphi_1) \cup bound(\varphi_2)$$

$$bound(\varphi_1 \vee \varphi_2) = bound(\varphi_1) \cup bound(\varphi_2)$$

$$bound(\varphi_1 \rightarrow \varphi_2) = bound(\varphi_1) \cup bound(\varphi_2)$$

$$bound(\neg \varphi_1) = bound(\varphi_1)$$

$$bound(\exists v \varphi_1) = bound(\varphi_1) \cup \{v\}$$

$$bound(\forall v \varphi_1) = bound(\varphi_1) \cup \{v\}$$

נדגיש כי משתנה יכול להופיע קשור וגם חופשי באותה נוסחא, למשל, בנוסחא $R_{2,1}(v_0, v_1) \wedge \exists v_1(R_{2,2}(v_0, v_1))$. כמו כן, נדגיש כי אין קשר בין המופעים הנ"ל של v_1 .

ובכאן סיימנו לדבר על הספנטיקה וההגדרה הפורמלית של לוגיקה מסדר ראשון, ונעבור לערכת ההוכחה בלוגיקה מסדר ראשון.

4 מערכת ההוכחה של לוגיקה מסדר ראשון

מערכת ההוכחה שלנו בלוגיקה מסדר ראשון תהיה דומה לזו שנתקלנו בה בתחשיב הפסוקים. באותו אופן לעיל, נשתמש בקשרים הלוגיים $\{\rightarrow, F\}$ בלבד, ובמקום הכמת $\exists v_i \varphi$ נשתמש בכמת $(\forall v_i(\varphi \rightarrow F)) \rightarrow F$.

להלן האקסיומות של מערכת ההוכחה שלנו:

1. $(\varphi \rightarrow (\psi \rightarrow \varphi))$.
2. $((\varphi \rightarrow (\psi \rightarrow \eta)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \eta)))$
3. $((\varphi \rightarrow F) \rightarrow F) \rightarrow \varphi$
4. $(\forall v(\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \forall v(\psi)))$ כאשר v אינו מופיע חופשי ב- φ .
5. $\forall v(\varphi) \rightarrow \varphi(t)$ כאשר t אינו מופיע קשור ב- φ .

מדוע יש חשיבות להגבלות באקסיומות 4,5? נדגים זאת ע"י דוגמא.

עבור האקסיומה הרביעית, נביט בטענה $\forall v(R(v) \rightarrow R(v))$. טענה זו נכונה לכל מבנה. אם לא הייתה ההגבלה, ניתן היה להסיק מן הטענה כי $R(v) \rightarrow \forall v(R(v))$. אם נביט בעולם בני האדם, בו $R(v)$ משמעו האדם v הינו ג'ינג'י, נקבל שאם v כלשהו הוא ג'ינג'י, כל בני האדם הם בעלי שיער ג'ינג'י (?).

עבור האקסיומה החמישית, נביט בטענה $(\forall v(\neg \forall w(v = w)))$. אם נשתמש באקסיומה החמישית ללא ההגבלה, נוכל להסיק כי $\neg \forall w(w = w)$, כלומר, לא מתקיים לכל w כי $w = w$ (?).

נגדיר כעת אקסיומות נוספות עבור סימן השיוויון, פרדיקט מיוחד שיסמל שיוויון במבנה:

- $\forall v(v = v)$

- כאשר $A(v, w)$ מתקבל מ- $A(v, w)$ ע"י החלפת ההופעות החופשיות של $A(v, w) \rightarrow A(v, w)$ של $(v = w) \rightarrow (A(v, w) \rightarrow A(v, w))$ ב- w

לאקסיומות הנ"ל נקרא אקסיומות 6,7 בהתאמה.

4.0.1 כללי הוכחה

כללי ההוכחה במערכת ההוכחה יהיו Modus-Ponens, או בקיצור MP, וכלל נוסף, (Generalization) Gen, האומר, כי אם מסיקים $\varphi(v)$, ניתן להסיק $\forall x\varphi(x)$, רק כאשר v אינו חופשי באף אחת מן ההנחות Σ . מדוע הגבלה זו? נניח שבהנחות נמצאת הנוסחה $v = 0$. מכאן נוכל להסיק $\forall x(x = 0)$ (?).

4.1 הוכחות בלוגיקה מסדר ראשון

תזכורת. הוכחה של $\Sigma \vdash \varphi$ הינה סדרת הוכחות, כאשר כל שלב בה יכול להיות הנחה מ- Σ , אקסיומה מן הרשומות לעיל, או שימוש בכללי MP, Gen על השלבים הקודמים.

דוגמא. $\{\forall v\forall w\varphi(v, w)\} \vdash \forall v\forall v(\varphi(v, w))$

- $\forall v\forall w\varphi(v, w)$Assumption.
- $\forall v\forall w(\varphi(v, w)) \rightarrow \forall w(\varphi(v, w))$A5.¹
- $\forall w(\varphi(v, w))$MP(1,2).
- $\forall w(\varphi(v, w)) \rightarrow \varphi(v, w)$A5.²
- $\varphi(v, w)$MP(3,4).
- $\forall v\varphi(v, w)$Gen(5).³
- $\forall w\forall v(\varphi(v, w))$Gen(6)⁴

¹שימו לב כי כאן אנו מחליפים את v עם עצמו, ולכן כל מופע קשור של v בתוך φ לא יינזק עקב ההצבה.
²שימו לב כי כאן אנו מחליפים את w עם עצמו, ולכן כל מופע קשור של w בתוך φ לא יינזק עקב ההצבה.
³קל לראות כי אין מופע חופשי של v ב- $\forall v\forall w\varphi(v, w)$.
⁴קל לראות כי אין מופע חופשי של w ב- $\forall v\forall w\varphi(v, w)$.

דוגמא. $\{v = w\} \vdash w = v$.

1. $v = w$Assumption.
2. $(v = w) \rightarrow ((v = v) \rightarrow (w = v))$A7⁵.
3. $(v = v) \rightarrow (w = v)$MP(1,2).
4. $\forall v(v = v)$A6.
5. $\forall v(v = v) \rightarrow (v = v)$A5.⁶
6. $v = v$MP(4,5).
7. $w = v$MP(3,6).

דוגמא. $\{u = v, v = w\} \vdash u = w$

1. $v = u$Previous example
2. $(v = u) \rightarrow ((v = w) \rightarrow (u = w))$A7($A(v, v) = (v, w)$)
3. $(v = w) \rightarrow (u = w)$MP(1+2)
4. $v = w$Assumption.
5. $u = w$Assumption.

משפט הדדוקציה: לכל קבוצת נוסחאות Σ ולכל שתי נוסחאות φ, ψ מתקיים: $\Sigma \cup \{\varphi\} \vdash \psi \iff \Sigma \vdash \varphi \rightarrow \psi$.
 כזכור, משפט זה זהה למשפט הדדוקציה מתחשיב הפסוקים, וגם מתקיים כאן, וכרגע לא נוכיח אותו כאן.
 כמו כן, גם בלוגיקה מסדר ראשון "הוכחה לפי מקרים" מתקיים. כלומר, $\Sigma \cup \{\varphi\} \vdash \psi \wedge \Sigma \cup \{\varphi \rightarrow F\} \vdash \psi \implies \Sigma \vdash \psi$.

⁵כאשר $A(v, v)$ מסמל את $v = v$.
⁶שימו לב, מדוע ניתן להשתמש באקסיומה?

5 נאותות ושלמות, ספיקות וקונסיסטנטיות

בחלק זה נזון בשלמות של לוגיקה מסדר ראשון, בשקילות בין סיפוק וקונסיסטנטיות של קבוצת נוסחאות, ואף נציג דוגמא לכוחה החלש של לוגיקה מסדר ראשון.

הגדרה. נאמר שקבוצת נוסחאות Σ היא **קונסיסטנטית** אם לא קיימת נוסחא φ כך ש- $\Sigma \vdash \varphi$ וגם $\Sigma \vdash (\varphi \rightarrow F)$.⁷
משפט. לכל קבוצת נוסחאות Σ ונוסחא φ , מתקיים $\Sigma \vdash \varphi \iff \Sigma \cup \{\varphi \rightarrow F\}$ לא קונסיסטנטית.
הוכחה. בכיוון \Rightarrow , נניח ש- $\Sigma \cup \{\varphi \rightarrow F\}$ לא קונסיסטנטית. אזי, בהכרח $\Sigma \cup \{\varphi \rightarrow F\} \vdash \varphi$.⁸
 כמו כן, בהכרח מתקיים $\Sigma \cup \{\varphi\} \vdash \varphi$. מכאן, לפי "הוכחה לפי מקרים", בהכרח $\Sigma \vdash \varphi$.

□

בכיוון \Leftarrow , נניח ש- $\Sigma \vdash \varphi$. מכאן, בהכרח $\Sigma \cup \{\varphi \rightarrow F\} \vdash F$,⁹ ולכן לפי ההגדרה, $\Sigma \cup \{\varphi \rightarrow F\}$ לא קונסיסטנטית.

■

תזכורת. נאמר שקבוצת נוסחאות $\Sigma \models \varphi$, אם לכל מודל (לכל מבנה) ולכל הצבה המספקת את כל המשתנים בנוסחאות ב- Σ , בהכרח ההצבה מספקת את φ .

נאמר שקבוצת נוסחאות Σ היא ספיקה (או כי ל- Σ קיים מודל), אם קיים מודל בו כל נוסחא ב- Σ מקבלת ערך T .

5.1 הקשר ההדוק בין קונסיסטנטיות וספיקות לשלמות ונאותות

נניח כרגע כי שלמות ונאותות מערכת ההוכחה שלנו הוכחה. כלומר, $\Sigma \models \varphi \iff \Sigma \vdash \varphi$ לכל קבוצת נוסחאות Σ ונוסחא φ .

טענה. $\Sigma \vdash \varphi \iff$ קיימת תת-קבוצה סופית $\Sigma_0 \subseteq \Sigma$ כך ש- $\Sigma_0 \vdash \varphi$.¹⁰ מדוע?¹⁰

מכאן, נוכל להסיק כי $\Sigma \models \varphi \iff$ קיימת תת-קבוצה סופית $\Sigma_0 \subseteq \Sigma$ כך ש- $\Sigma_0 \models \varphi$.¹¹

□

מכאן, נוכל להסיק בעזרת השלמות, כי $\Sigma \cup \{\varphi \rightarrow F\} \models \varphi \iff \Sigma \cup \{\varphi \rightarrow F\}$ אינה ספיקה.

משפט. אם קבוצת נוסחאות Σ קונסיסטנטית, אזי לכל φ נוסחא, או ש- $\Sigma \cup \{\varphi\}$ קונסיסטנטית או $\Sigma \cup \{\varphi \rightarrow F\}$ קונסיסטנטית.

הוכחה. נניח בשלילה ששתי הקבוצות לא קונסיסטנטיות. תהי נוסחא ψ , אזי, בהכרח מתקיים $\Sigma \cup \{\varphi \rightarrow F\} \vdash \psi$ ו- $\Sigma \cup \{\varphi\} \vdash \psi$.

מכאן, לפי מקרים נסיק כי $\Sigma \vdash \psi$, וזה נכון לכל פסוק ψ . כלומר, Σ לא קונסיסטנטית, בסתירה.

■

תזכורת. $\Sigma \models \varphi \iff \Sigma \cup \{\varphi \rightarrow F\}$ אינה ספיקה. הוכחנו זאת בפרק הקודם.

⁷ניסוחים שקולים: $\Sigma \not\models \varphi$. ניסוח נוסף לאי-קונסיסטנטיות הוא שלכל נוסחא φ מתקיים $\Sigma \vdash \varphi$.

⁸מדוע? היזכרו בהגדרה השקולה לקונסיסטנטיות.

⁹ניתן להסיק את F בעזרת כלל MP.

¹⁰רמז: כל הוכחה היא בהכרח סופית.

¹¹זה נובע משלמות מערכת ההוכחה ומן הטענה לעיל.

נראה כעת את הקשר החזק בין ספיקות וקונסיסטנטיות, לשלמות ונאותות.

משפט. נניח כי קונסיסטנטיות גוררת ספיקות. אזי מערכת ההוכחה שלמה.

הוכחה. נניח כי $\Sigma \not\vdash \varphi$. אזי, $\Sigma \cup \{\varphi \rightarrow F\}$ קונסיסטנטית. ולכן, לפי ההנחה, $\Sigma \cup \{\varphi \rightarrow F\}$ ספיקה. ולכן $\Sigma \not\vdash \varphi$.

■

משפט. נניח כי ספיקות גוררת קונסיסטנטיות. אזי, מערכת ההוכחה נאותה.

הוכחה. נניח כי $\Sigma \vdash \varphi$. אזי, $\Sigma \cup \{\varphi \rightarrow F\}$ לא קונסיסטנטית, ולכן לפי ההנחה, $\Sigma \cup \{\varphi \rightarrow F\}$ אינה ניתנת לסיפוק, ומכאן נוכל להסיק $\Sigma \models \varphi$.

■

מכאן, נוכל לקבל שקילות בין הקשר של תכונה סינטקטית לתכונה סמנטית:

- לכל קבוצת נוסחאות Σ , מתקיים: Σ קונסיסטנטית $\iff \Sigma$ ספיקה.
- לכל קבוצת נוסחאות Σ ונוסחא φ , מתקיים: $\Sigma \vdash \varphi \iff \Sigma \models \varphi$.

ולכן, קיימת שקילות בין היחס הסינטקטי של קונסיסטנטיות וספיקות לנאותות ושלמות.

כעת, בעזרת שלמות ונאותות, נוכיח את משפט הקומפקטיות.

5.2 משפט הקומפקטיות

משפט. (קומפקטיות) לקבוצת נוסחאות Σ קיים מודל \iff לכל תת קבוצה סופית $\Sigma_0 \subseteq \Sigma$ קיים מודל.

הוכחה. כזכור, Σ לא קונסיסטנטית $\iff \Sigma \vdash F \iff$ קיימת תת קבוצה סופית $\Sigma_0 \subseteq \Sigma$ כך ש- $\Sigma_0 \vdash F$ \iff קיימת תת קבוצה סופית לא קונסיסטנטית של Σ .

מכאן, לפי קונטרפוזיציה, יתקיים כי Σ קונסיסטנטית \iff כל תת קבוצה סופית שלה קונסיסטנטית.

לפי שלמות מערכת ההוכחה, קונסיסטנטיות שקולה לספיקות, כלומר, לקבוצת נוסחאות Σ קיים מודל \iff לכל תת קבוצה סופית של Σ קיים מודל.

■

למשפט הקומפקטיות יש משמעות חזקה. עבור קבוצת נוסחאות Σ קיים מודל מתמטי שבו כל הנוסחאות ב- Σ מתקיימות אם ורק אם לכל תת קבוצה סופית של Σ יש מודל מתמטי המקיים אותן.

נוכיח כעת בעזרת זאת את אחת מחולשותיה של לוגיקה מסדר ראשון:

סימון. נסמן ב- Γ_∞ את כל הנוסחאות φ_i , כך שמשמעות φ_i היא כי בעולם קיימים לפחות i אלמנטים.¹²

משפט. לא קיימת קבוצת נוסחאות Σ , המתארת אך ורק את כל המודלים הסופיים.

¹²חשבו כיצד ניתן לרשום פסוק זה.

הוכחה. נניח בשלילה ש- Σ היא קבוצת נוסחאות המתארת אך ורק את כל המודלים הסופיים. תהי תת קבוצה סופית כלשהי של $\Gamma \subseteq \Gamma_\infty$. בגלל שהיא סופית, קיים $i \in \mathbb{N}$ מקסימלי כך ש- $\varphi_i \in \Gamma$.

בהכרח לקבוצה $\Sigma \cup \Gamma$ יש מודל, מכיוון שניתן לקחת מודל עם בדיוק i איברים, והוא יקיים גם את Σ (המתארת את כל המודלים הסופיים) גם כל תת קבוצה סופית שלה ואת Γ (המתארת מודל עם לפחות i אלמנטים).

מכאן, בהכרח נקבל כי לכל תת קבוצה סופית של $\Sigma \cup \Gamma_\infty$ יש מודל¹³, וממשפט הקומפקטיות נוכל להסיק כי יש מודל ל- $\Sigma \cup \Gamma_\infty$, אבל אז קיים מודל המספק את Σ ואת Γ_∞ , ובכך נקבל כי קיים מודל סופי המספק את Γ_∞ , בסתירה לכך שהקבוצה מספקת אך ורק מודלים אינסופיים.

■

משפט. לא קיימת נוסחא φ , שתתאר אך ורק את המודלים האינסופיים.

הוכחה. נניח בשלילה שקיימת נוסחא שכזו φ . אזי, בהכרח $\Gamma_\infty \models \varphi$. לפי שלמות המערכת, קיימת תת קבוצה סופית $\Gamma \subseteq \Gamma_\infty$ כך ש- $\Gamma \models \varphi$. אבל, קיים מודל בו כל נוסחאות Γ מתקיימות (מודל עם מספר סופי של אלמנטים, בהתאם לנוסחא המקסימלית המופיעה ב- Γ), אבל הוא לא מקיים את φ (שמתארת אך ורק מודלים אינסופיים), בסתירה.

■

מסקנה. לא קיימת קבוצה סופית Γ המתארת אך ורק את המודלים האינסופיים.

הוכחה. נניח בשלילה שקיימת קבוצה $\Gamma = \{\chi_1, \chi_2, \dots, \chi_n\}$ כך שמתארת אך ורק את המודלים האינסופיים. אזי, נגדיר $\varphi = \chi_1 \wedge \chi_2 \wedge \dots \wedge \chi_n$.

מכאן בהכרח נקבל כי φ מתאר אך ורק את המודלים האינסופיים, בסתירה למשפט.

למחשבה. נגדיר את הנוסחא $\varphi = \forall x \forall y ((f_{1,1}(x) = f_{1,1}(y)) \rightarrow (x = y) \wedge \exists y \forall x (f_{1,1}(x) \neq y))$. למעשה נוסחא זו מתארת כי יש פונקציה חח"ע שאינה על, תנאי הכרחי לאינסופיות הקבוצה.

האם זה סותר את המשפט לעיל?¹⁴

■

5.3 משפט השלמות ללוגיקה מסדר ראשון

ההוכחה למשפט תשתמש בשקילות שהראנו. למעשה, ניתן להוכיח, עם הוכחה דומה למשפט השלמות לפסוקים, כי אם קבוצה היא קונסיסטנטית, אזי יש לה מודל.

המודל שנבנה יהיה בנוי מ- Σ^* מן הפרק הקודם, למעט מספר תיקונים וחיידודים. עקב קוצר הזמן (והמקום), איני הולך לרשום את ההוכחה כאן.

¹³מדוע?

¹⁴נשים לב בעיון כי הפונקציה החח"ע שאינה על היא סימן פונקציה, כלומר, עבור מודל מתאים ומבנה מתאים, בהחלט יכול להתקיים כי $f_{1,1}$ חח"ע ואינה על. אך במודל אינסופי אחר יכול להתקיים כי $f_{1,1}$ חח"ע ועל, ולכן הנוסחא אינה מספקת כל מודל אינסופי. למעשה בלוגיקה מסדר שני, ניתן לתאר זאת בנוסחא אחת, מכיוון שניתן לנסח בלוגיקה מסדר שני קיום פונקציה (בסופו של דבר, פונקציה היא קבוצה של זוגות סדורים, כשכל זוג סדור הינו קבוצה של אלמנטים).

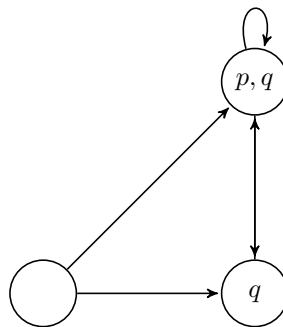
6 משפט אי-השלמות של גדל

את ההוכחה לפשט הנ"ל איני הולך להוכיח כאן. ההוכחה שהוצגה הינה הוכחה בעזרת כלים מתורת החישוביות (רדוקציה פשפה שאינה כריעה). את ההוכחה הפקורית ניתן לפצוא באינטרנט.

חלק III

לוגיקה מודלית

עד כה דיברנו על מודל של לוגיקה בו לכל נוסחא יש שני מצבים, נכונות או אי-נכונות. ברצוננו להרחיב את המודל הנ"ל לעולם דינמי, עולם בו נכונות של נוסחא תלוי בממד נוסף (למשל, זמן, מצב, ידע...). השימוש העיקרי בלוגיקה מודלית בא לידי בידי בהוכחת נכונות של תכניות, בינה מלאכותית, ועוד. לדוגמא, נביט בעולם הבא



העולמות שלנו מייצגים "מצבים", ולכל עולם מותאמים כל הפסוקים המתקיימים בו, ועולמות הנגררים ממנו¹⁵.

7 לוגיקה מודלית פורמלית במבנה Kripke

מבנה Kripke מהווה פורמליזציה לאינטואיטיביות מאחורי ההגדרה לעיל.

הגדרה. מבנה Kripke הינו רביעייה (W, R, L, \mathcal{P}) המוגדרת כך:

1. \mathcal{P} הינה קבוצת נוסחאות¹⁶.
2. W הינה קבוצת העולמות במבנה¹⁷.
3. R הינו יחס בינארי $R \subseteq W \times W$ ¹⁸.
4. $L : \mathcal{P} \rightarrow 2^W$ ¹⁹, המתאימה לכל $w \in W$ תת קבוצה של נוסחאות \mathcal{P} , שמתקיימות בעולם w .

כעת, נוכל להגדיר פורמלית את פושג המשמעות, "נכונות" של נוסחא בעולם כלשהו.

¹⁵ זאת ניתן לזהות ע"י הקשתות בגרף.

¹⁶ למעשה זו קבוצת הנוסחאות להן נייחס משמעות במבנה הלוגי.

¹⁷ לקבוצה זו ניתן להתייחס עפ"י הדוגמא לעיל כקבוצת הקודקודים בגרף.

¹⁸ יחס זה הינו "יחס הנגררות" בין העולמות.

¹⁹ משמעות $2^{\mathcal{P}}$ הינה קבוצת החזקה של \mathcal{P} - קבוצת כל תתי קבוצות של נוסחאות ב- \mathcal{P} .

הגדרה. יהי $x \in \mathcal{W}$ עולם כלשהו. נאמר ש- $x \Vdash p$ ²⁰ פסוק יסודי $p \in \mathcal{P}$, אם $p \in L(x)$. מכאן נגדיר רקורסיבית את הגרירה הלוגית:

1. נאמר ש- $x \Vdash \neg \varphi$ אם ורק אם $x \not\Vdash \varphi$.
2. $x \Vdash \varphi \wedge \psi$ אם $x \Vdash \varphi$ וגם $x \Vdash \psi$.
3. $x \Vdash \varphi \vee \psi$ אם $x \Vdash \varphi$ או $x \Vdash \psi$.
4. $x \Vdash \Box \varphi$ אם $x \Vdash \varphi$ לכל $y \in \mathcal{W}$ כך ש- $(x, y) \in R$, מתקיים $y \Vdash \varphi$.
5. $x \Vdash \Diamond \varphi$ אם $x \Vdash \varphi$ קיים $y \in \mathcal{W}$ כך ש- $(x, y) \in R$, ומתקיים $y \Vdash \varphi$.

דוגמא. נשים לב לשקילויות הבאות:

- $\Box \varphi = \neg \Diamond (\neg \varphi)$
- $\Diamond \varphi = \neg \Box (\neg \varphi)$
- $\Box (p \wedge q) = (\Box p \wedge \Box q)$
- $\Diamond (p \vee q) = (\Diamond p \vee \Diamond q)$

שימו לב, כי $\Box (p \vee q) \neq (\Box p \vee \Box q)$ וכי $\Diamond (p \wedge q) \neq (\Diamond p \wedge \Diamond q)$, מדוע?²¹

הגדרה. נאמר שנוסחא φ היא

- ברט סיפוק אם קיים עולם $w \in \mathcal{W}$ המקיים אותה, במודל²² מסוים.
- אינה ברט סיפוק אם אינה מתקיימת בכל עולם ובכל מודל.
- נכונה במודל, אם מתקיימת בכל $w \in \mathcal{W}$.
- *valid* אם לכל מודל ולכל עולם $w \in \mathcal{W}$, φ מתקיימת ב- w .
- *valid* במשפחה מוגבלת של מודלים²³, אם לכל מודל במשפחה ולכל עולם $w \in \mathcal{W}$, φ מתקיימת ב- w .

כמו כן, יוגדרו כללי היסק ואקסיומות, בדומה ללוגיקה הפסוקית - כלל MP , אקסיומות A_1, A_2, A_3 , האקסיומה החדשה $\Box(\varphi \rightarrow \psi) \rightarrow (\Box \varphi \rightarrow \Box \psi)$, \mathcal{K} : $\Box(\varphi \rightarrow \psi) \rightarrow (\Box \varphi \rightarrow \Box \psi)$ וכלל היסק GEN האומר כי מ- φ ניתן להסיק $\Box \varphi$.

²⁰הסימון בהרצאה היה \models , ובתרגול \Vdash .

²¹עבור הראשון, אין זה מחייב שאם כל העולמות מקיימים את $p \vee q$, אזי כל העולמות השכנים מקיימים את p או כל העולמות השכנים מקיימים את q . עבור השני באותו האופן.

²²המשמעות של מודל הינה זהה למשמעות בלוגיקה מסדר ראשון, ה"ייקום" עליו אנו מדברים.

²³דוגמא לזאת נראה בהמשך.

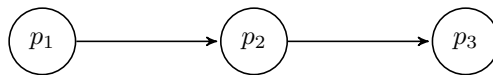
7.1 דוגמא למשפחות מודלים

נגדיר כעת תכונות שמודלים מסויימים יכולים לקיים:

הגדרות. נאמר שמודל הוא

1. מודל T (רפלקסיבי) אם לכל עולם $w \in \mathcal{W}$, $(w, w) \in R$, שקול ל- $\Box\varphi \rightarrow \varphi$.
2. מודל D (סיראלי²⁴) אם לכל $w \in \mathcal{W}$, קיים $w' \in \mathcal{W}$ כך ש- $(w, w') \in R$, שקול ל- $\Box\varphi \rightarrow \Diamond\varphi$.
3. מודל 4 (טרנזיטיבי) אם לכל $u, v, w \in \mathcal{W}$, אם $(u, v) \in R$ ו- $(v, w) \in R$ אזי $(u, w) \in R$, שקול ל- $\Box\varphi \rightarrow \Box\Box\varphi$.
4. מודל 5 (אוקלידי) אם לכל $u, v, w \in \mathcal{W}$, אם $(u, v) \in R$ ו- $(u, w) \in R$ אזי $(v, w) \in R$, שקול ל- $\Diamond\varphi \rightarrow \Box\Diamond\varphi$.

כמו כן, נאמר שמודל הוא **ליניארי**, אם הוא טרנזיטיבי, מסודר היטב, ואין בו מעגלים. למשל



7.2 לוגיקה של ידע

בלוגיקה של ידע, נרצה לבנות מודל המתאר את יחסי הידע בין המצבים.

נגדיר לשם כך קבוצת סוכנים A, B, C . בניגוד ללוגיקה מודלית, כאן יהיו לנו מספר יחסים R_A, R_B, R_C , כך ש- R_A מסמל יחס בין מצבים ש- A אינו יכול להבדיל ביניהם. נדרוש כי אלו יהיו יחסי **שקילות**.

הגדרה. יהי $s \in \mathcal{W}$ עולם במודל ידע (המוגדר באופן דומה למודל *Kripke*). נאמר ש:

1. $s \models K_A(\varphi)$ אם לכל $r \in \mathcal{W}$ כך ש- $(s, r) \in R_A$ מתקיים $r \models \varphi$ ²⁵, עבור סוכן A .
2. $s \models C(\varphi)$ אם φ הוא ידע משותף. כלומר, כל סוכן יודע את φ , כל סוכן יודע שכל סוכן יודע את φ , וכך הלאה.

למעשה, המשמעות של ההגדרה הראשונה, $K_A(\varphi)$ אומר כי בכל העולמות שהסוכן A אינו יכול להבדיל ביניהם, φ בהכרח מתקיים. מכך ניתן להסיק שהוא יכול לדעת **בוודאות** כי φ מתקיים.

דוגמאות. תכונות לוגיקת ידע משמרות תכונות טריוויאליות שנדרוש מידע.

- מתקיים $K_A(\varphi \rightarrow \psi) \rightarrow (K_A\varphi \rightarrow K_A\psi)$, כלומר, ידע היא תכונה בה ניתן להסיק מסקנות.
- $K_A\varphi \rightarrow \varphi$, כלומר, אם אני יודע ש- φ מתקיים, אז הוא בהכרח מתקיים בעולם שלי.
- $K_A\varphi \rightarrow K_AK_A\varphi$, כלומר, אני יודע שאני יודע משהו.
- $\neg K_A\varphi \rightarrow K_A\neg K_A\varphi$, כלומר, אני יודע מה אני לא יודע.

²⁴בלעז Serial.

²⁵שימו לב כי גם מוגדרת הסמנטיקה הקשורה ללוגיקה פסוקית.

7.3 לוגיקה טמפורלית

בלוגיקה טמפורלית, נרצה למדל מצבים של ריצה של תכנית. בין המצבים יתקיים יחס ליניארי, וסדר. נשתמש בלוגיקה זו לנסח טענות על ריצה מסוימת, ולאחר מכן על כל ריצה.

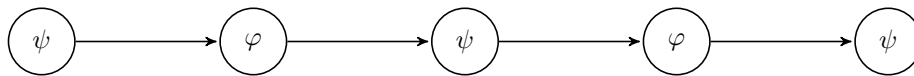
הגדרה. נגדיר את הכמתים

- $\Box\varphi$ - φ יתקיים תמיד, לעולם.
- $\Diamond\varphi$ - φ יתקיים מתישהו, בשלב מסוים.
- $\bigcirc\varphi$ - φ יתקיים בשלב הבא.
- $\varphi\mathcal{U}\psi$ - φ יתקיים עד ψ .

דוגמאות.

- $\Box\Diamond p$ - משמעו כי p יתקיים אינסוף פעמים.
- $\Diamond\Box p$ - משמעו כי בשלב כלשהו, p יתקיים לתמיד.

קיימות שלל דוגמאות בנושא זה. במידה ותרצו להפריך טענה מסוימת, למשל, הדוגמא הבאה מפריכה את הטענה כי $\Box(\varphi \vee \psi) = (\Box\varphi) \vee (\Box\psi)$



7.3.1 הגדרה פורמלית של לוגיקה טמפורלית

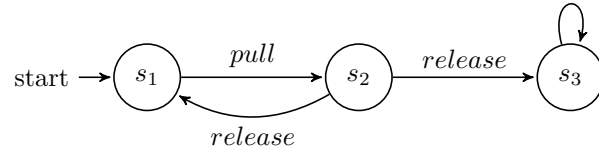
הגדרה. תהי $\sigma = s_0, s_1, \dots$ סדרת ריצה, ו- $s_i \in \mathcal{W}$. נגדיר σ^i להיות הסיפא s_i, s_{i+1}, \dots . נאמר ש:

1. $\sigma^i \models p$ אם ורק אם $s_i \models p$.
2. $\sigma^i \models \Diamond\varphi$ אם קיים $j \geq i$ כך ש- $\sigma^j \models \varphi$.
3. $\sigma^i \models \Box\varphi$ אם לכל $j \geq i$, $\sigma^j \models \varphi$.
4. $\sigma^i \models \bigcirc\varphi$ אם $\sigma^{i+1} \models \varphi$.
5. $\sigma^i \models \varphi\mathcal{U}\psi$ אם קיים $j \geq i$ כך ש- $\sigma^j \models \psi$, ולכל $i \leq k < j$ מתקיים $\sigma^k \models \varphi$.

למעשה, $s \in \mathcal{W}$ מתארים לנו את המצבים, σ הינה ריצה אפשרית כלשהי. נוכל לומר כי $P \models \varphi$ אם כל סדרת ריצה σ של P מקיימת $\sigma \models \varphi$.

²⁶שימו לב כי גם מוגדרת הסמנטיקה הקשורה ללוגיקה פסוקית.

דוגמא. נציג את דוגמת מצב קפיץ



כאשר נגדיר $L(s_2) = \{extended\}$, כאשר משמעות $extended$ היא כי הקפיץ מתוח, ו- $L(s_3) = \{extended, malfunction\}$, כאשר $malfunction$ משמעו כי הקפיץ אינו עובד יותר.

להלן טענות שניתן לנסח על סדרת הריצה $\sigma = s_1 s_2 s_1 s_2 s_3 s_3 s_3 \dots$

- $r_2 \models extended$ - זה לא מתקיים, כי $L(s_1) = \emptyset$.
- $r_2 \models \circ extended$ - זה מתקיים, כי ב- s_2 כן מתקיים $extended$.
- $r_2 \models \circ \circ extended$ - זה לא מתקיים, וזאת כי לאחר שני מצבים, המצב יהיה s_1 חזרה, ושם לא מתקיים $extended$.
- $r_2 \models \diamond extended$ - זה מתקיים, כי הרי ב- s_2 מתקיים $extended$.
- $r_2 \models \square extended$ - זה לא מתקיים, המצב s_1 אינו מקיים $extended$ ומגיעים אל המצב הזה בהרצה r_2 .
- $r_2 \models \diamond \square extended$ - זה מתקיים, כי מתישהו בהרצה מגיעים לשלב s_3 (לאחר 4 צעדים) ושם מתקיים $\square extended$.
- $r_2 \models \neg \diamond \square extended$ - בסעיף הקודם הראנו שהשליה של הטענה נכונה, ולכן זו אינה נכונה.
- $r_2 \models (\neg extended) \mathcal{U} (malfunction)$ - זה לא מתקיים, שכן הפעם הראשונה בה מתקיים $malfunction$ היא בצעד הרביעי, בעוד שבצעד בשני כבר מתקיים $extended$ ולכן לא מתקיים $\neg extended$.
- $r_2 \models \square (\neg extended \rightarrow \circ extended)$ - זה מתקיים, שכן לכל צעד, אם מתקיים בו $\neg extended$, הרי שהמצב היחיד שזה יקרה הוא s_1 , והשלב שאחרי s_1 הוא s_2 , ולכן שם יתקיים $extended$.

חשוב לנסות ולהבין בלוגיקה מודלית והלוגיקות הנגזרות מפנה פהו הפודל, איך הוא פוגדר ואיך לנסח בו טענות אותן היינו רוצים להוכיח או לדרוש בפודל.

חלק IV

אימות תוכנה

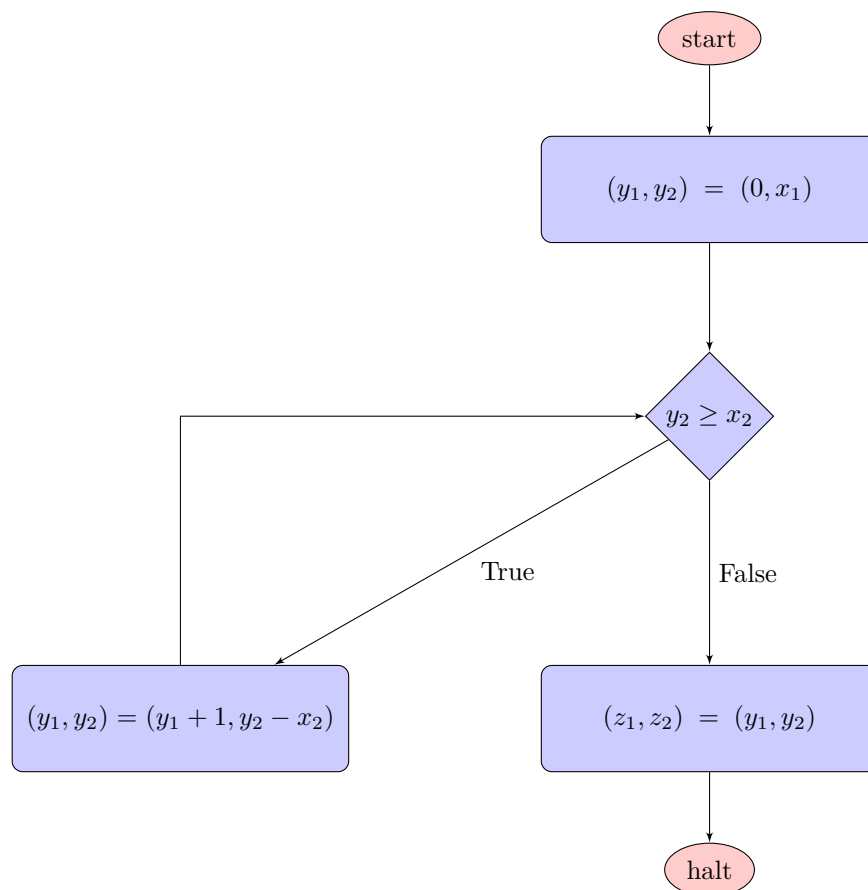
נרצה כעת באמצעות שימוש בלוגיקה מסדר ראשון לאמת את נכונותן של תכניות, ובמקרה שלנו Flowchat programs.

8 הוכחת נכונות

השיטה לאימות תכניות שנציג כאן פיתח Floyd בשנת 1967.

הגדרה. המשתנים בנוסחאות שלנו יהיו מן הקבוצות הבאות: משתני הקלט, $X = \{x_1, \dots, x_n\}$, משתני התכנית $Y = \{y_1, \dots, y_n\}$ ומשתני פלט $Z = \{z_1, \dots, z_k\}$.

נביט בתכנית הבאה:



התכנית מחשבת את החילוק בשארית של x_1 ב- x_2 . כלומר, מחשבת z_1, z_2 כך ש- $x_1 = z_1 \cdot x_2 + z_2$ ו- $0 \leq z_2 < x_2$. נרצה להוכיח כי אכן התכנית מבצעת את הדרוש. כלומר, בהינתן קלט (x_1, x_2) , הפלט (z_1, z_2) מקיים $x_1 = z_1 \cdot x_2 + z_2 \wedge 0 \leq z_2 < x_2$.

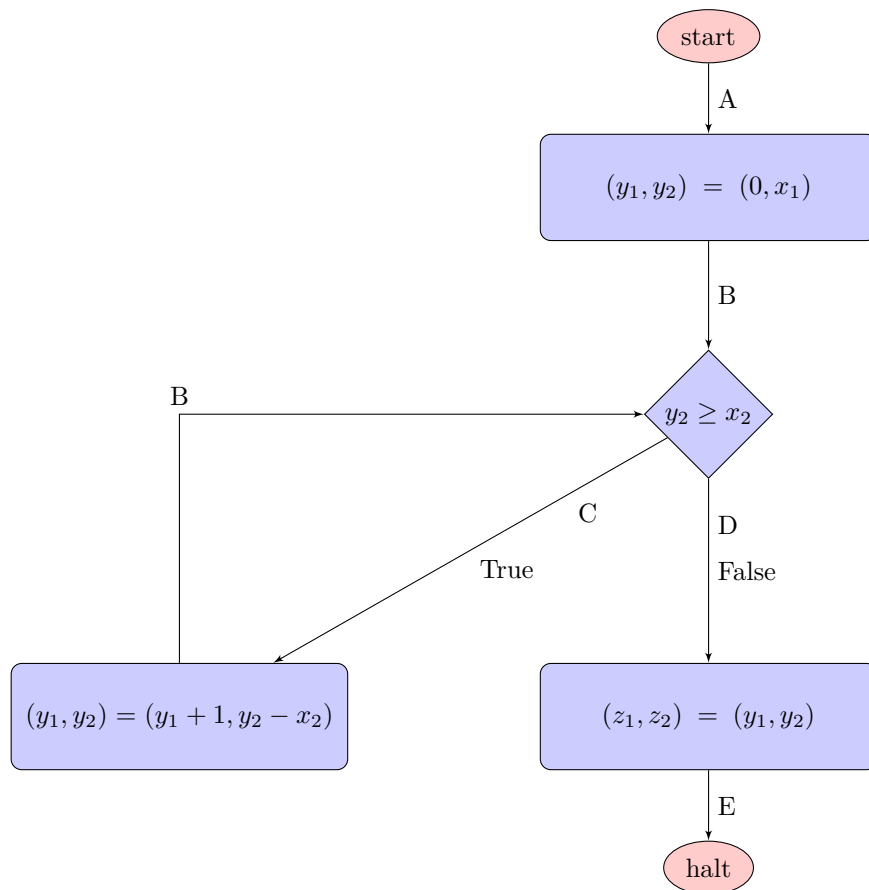
הגדרה.

- נכונות חלקית - אם התנאי ההתחלתי מתקיים והתכנית עוצרת, אז יחס הקלט-פלט מתקיים.
- סיום - אם התנאי ההתחלתי מתקיים, אזי התוכנית עוצרת.
- נכונות מוחלטת - אם התנאי ההתחלתי מתקיים, אזי התכנית עוצרת ויחס הקלט-פלט מתקיים.

למשל, בדוגמא לתוכנית לעיל, התכנית נכונה חלקית עבור תנאי התחלה $x_1 \geq 0, x_2 \geq 0$, אך נכונה באופן מוחלט עבור $x_1 \geq 0, x_2 > 0$.

8.1 הוכחת נכונות חלקית

לכל נקודה בין שני מצבים ניתן שם. למשל:



לכל נקודה נשייך שמורה, טענה לוגית שתתקיים במהלך הריצה של התכנית.
למשל, נציג שמורות לכל נקודה בתכנית לעיל:

$$\begin{aligned} \varphi(A) &: (x_1 \geq 0) \wedge (x_2 \geq 0) \bullet \\ \varphi(B) &: x_1 = (y_1 \cdot x_2 + y_2) \wedge (y_2 \geq 0) \bullet \\ \varphi(C) &: x_1 = (y_1 \cdot x_2 + y_2) \wedge (y_2 \geq x_2) \bullet \\ \varphi(D) &: x_1 = (y_1 \cdot x_2 + y_2) \wedge (y_2 \geq 0) \wedge (y_2 < x_2) \bullet \\ \varphi(E) &: x_1 = (z_1 \cdot x_2 + z_2) \wedge (z_2 \geq 0) \wedge (z_2 < x_2) \bullet \end{aligned}$$

מתקיים $\varphi(A)$ - הוא פרה־תנאי של השורה $(0, x_1) = (y_1, y_2)$, ו־ $\varphi(B)$ הוא פוסט־תנאי של אותה שורה.
ע"מ להוכיח את נכונות התכנית, נרצה להראות קונסיסטנטיות של השמורות. כלומר, בהנחה שכל שמורה גוררת את השמורה הבאה, נרצה כי למשל השמורה ב־ A תגרוור את נכונות השמורה ב־ B . אם זה יתקיים, נקבל כי סה"כ תנאי הקלט ב־ A גורר את תנאי הפלט ב־ E , ובכך הוכחה נכונות התכנית.
אך למרות זאת, אם נרצה להוכיח כי השמורה C גוררת את השמורה B , לא נוכל להוכיח $\varphi(B) \rightarrow \varphi(C)$, שכן הצבנו ערכים שונים לאותם משתנים!
כיצד נפתור זאת?

8.1.1 רלטיזציה

נמיר את השמורה לפסוק שקול בשמורה הקודמת לה. לכל המשתנים בשמורה נוסף סימן $'$, ונציב לכל משתנה x' את $x' = f(x)$ כאשר f הינה ההצבה שהתבצעה.
הטענה שנקבל תהיה הטענה השקולה לשמורה בעולם של השמורה הקודמת, שם נצטרך להוכיח גרירה.

דוגמא. נוכיח את הנכונות של הדוגמא לעיל.

הוכחה.

ראשית, נוכיח קונסיסטנטיות מנקודה A ל־ B . אנו יודעים כי $\varphi(B) : x_1 = (y_1 \cdot x_2 + y_2) \wedge (y_2 \geq 0)$. נבצע רלטיזציה ל־ A ונקבל את הנוסחא

$$\varphi(B)_A : x_1 = (0 \cdot x_2 + x_1) \wedge (x_1 \geq 0)$$

קל לראות כי אכן $\varphi(A) \rightarrow \varphi(B)_A$.

כעת, נוכיח קונסיסטנטיות בין הנקודה B אל C .

כלומר, נצטרך להראות כי בהינתן שתנאי הלולאה מתקיים, השמורה B גוררת את השמורה C . נזכיר כי $\varphi(C) : x_1 = (y_1 \cdot x_2 + y_2) \wedge (y_2 \geq x_2)$.

מכיוון שלא התבצעה הצבה בתנאי, קל לראות כי אכן $\varphi(B) \rightarrow \varphi(C)_B$.

כעת נוכיח כי השמורה C גוררת את השמורה B . נזכיר כי $\varphi(B) : x_1 = (y_1 \cdot x_2 + y_2) \wedge (y_2 \geq 0)$. נבצע רלטיזציה ל־ C ונקבל את הנוסחא

$$\varphi(B)_C : x_1 = ((y_1 + 1) \cdot x_2 + (y_2 - x_2)) \wedge (y_2 - x_2 \geq 0)$$

קל לראות כי אכן $\varphi(C) \rightarrow \varphi(B)_C$.

כעת, הצעד האחרון הוא כי השמורה D גוררת את השמורה E . זהו צעד פשוט שכן לאחר הרלטיויזציה, מתקיים $\varphi(D) = \varphi(E)_D$.

וכאן השלמנו את הוכחת הנכונות החלקית.

■

דוגמאות נוספות ניתן למצוא במצגותיו של המרצה.

8.2 הוכחת סיום, ולוגיקת Hoare

לצערנו, הזמן אינו מאפשר לי לעבור על נושאים אלו, ואולי תמצאו נחמה בכך שאלו אינם לבחינה. (;

חלק V

הערות לסיום

אין להסתמך על סיכום זה בלבד, ואני ממליץ ללמוד גם מן המצגות של פרופ' פלד, לפתור מבחנים, ועוד. ברצוני לאחל בהצלחה לכל הסטודנטים בקורס ולהודות למי שקרא את הסיכום ונהנה!