

# מבוא ללוגיקה מתמטית

## לבעלי אוריינטציה

### תכנותית 67501

---

תשע"ח 2017-2018

סוכם ע"י תמר מילכטייך לביא לפי שיעורי מפי פרופ' נועם ניסן ומר ינאי גונצ'רובסקי

לתיקונים והצעות לשיפור: [tamar.milchtaich@mail.huji.ac.il](mailto:tamar.milchtaich@mail.huji.ac.il)

## תוכן עניינים

1.....	שיעור 1 – 22.10.17	1
1.....	הקדמה	1.1
1.....	מנהלות	1.1.1
1.....	לוגיקה: הקדמה	1.1.2
2.....	הקורס בלוגיקה	1.1.3
3.....	תוכן הקורס	1.1.4
5.....	נוסחאות בנויות היטב	1.2
5.....	הגדרה ומשמעות	1.2.1
5.....	הנוסחא כעץ	1.2.2
8.....	שיעור 2 – 29.10.17	2
8.....	חזרה	2.1
8.....	מבנה (מודל) וטבלאות אמת	2.2
10.....	טאטולוגיה, סתירה ונוסחא ספיקה	2.3
11.....	פתרון בעיות באמצעות תחשיב הפסוקים – צביעת המפות ומכירת התדרים	2.4
11.....	בעיית צביעת המפות	2.4.1
12.....	המכירה הפומבית של התדרים בארה"ב Spectrum Auction	2.4.2
15.....	שיעור 3 – 5.11.17	3
15.....	נוסחאות DNF ונוסחאות CNF	3.1
15.....	הגדרה	3.1.1
15.....	המרה של טבלת אמת לנוסחא	3.1.2
16.....	ספיקות בנוסחאות DNF ו-CNF	3.1.3
17.....	אופרטורים נוספים	3.2
18.....	גרירה →	3.2.1
18.....	שקילות ↔	3.2.2
18.....	& Nand	3.2.3
18.....	Nor	3.2.4
18.....	אופרטור ה-Multiplexer	3.2.5
19.....	ניפוח אקספוננציאלי בהפיכת נוסחה ל-DNF	3.3
22.....	שיעור 4 – 12.11.17	4
22.....	קבוצות קשרים שלמות ובלתי-שלמות	4.1
25.....	מושג ההוכחה	4.2
25.....	כלל היסק	4.2.1
27.....	הוכחה	4.2.2

28 .....	משפט הנאותות	4.3	
30 .....	שיעור 5 – 19.11.17		5
30 .....	משפט הנאותות ומשפט הטאוטולוגיה	5.1	
31 .....	<i>Modus Ponens (MP)</i>	5.2	
32 .....	$I_1, I_2$ וקידוד כלל היסק באמצעות <i>MP</i>	5.3	
33 .....	הערה – שני סוגים של הוכחות	5.4	
34 .....	המשימות בתרגיל 5	5.5	
34 .....	משימה 3	5.5.1	
34 .....	משימה 4	5.5.2	
34 .....	משימה 1	5.5.3	
34 .....	משימה 2	5.5.4	
35 .....	הערות נוספות	5.6	
35 .....	מסקנה ממשפט הדוקציה, וצידוק להגדרה של אופרטור הגרירה	5.6.1	
36 .....	על הוכחות בשלילה	5.6.2	
37 .....	שיעור 6 – 26.11.17		6
37 .....	תרגיל 6	6.1	
37 .....	סקירה כללית של התרגיל	6.1.1	
38 .....	משימות 1-3	6.1.2	
39 .....	משימה 1	6.1.3	
40 .....	משימה 2	6.1.4	
41 .....	משימה 3	6.1.5	
42 .....	משימות 4-5	6.1.6	
42 .....	משימה 7 ומשפט השלמות (הסופי)	6.1.7	
44 .....	שיעור 7 – 3.12.17		7
44 .....	תחשיב היחסים (פרדיקטים) – לוגיקה מסדר ראשון	7.1	
44 .....	רקע	7.1.1	
45 .....	הגדרה פורמלית – סינטקס	7.1.2	
47 .....	הגדרה פורמלית – סמנטיקה	7.1.3	
50 .....	הוכחה של משפט השלמות בתחשיב הפסוקים לקבוצות אינסופיות	7.2	
53 .....	משפט הקומפקטיות	7.3	
55 .....	שיעור 8 – 10.12.17		8
55 .....	משפט הקומפקטיות בתחשיב הפסוקים – המשך	8.1	
55 .....	דוגמא שימושית למשפט הקומפקטיות	8.1.1	
58 .....	בעיית צביעת המישור וסוגים שונים של אינסוף	8.1.2	

62	תרגיל 8	8.2
63	פונקציות	8.2.1
65	יחס השיוויון	8.2.2
67	שיעור 9 – 24.12.17	9
67	הוכחות בתחשיב הפרדיקטים	9.1
69	דוגמא להוכחה	9.1.1
71	תרגיל 9	9.2
74	שיעור 10 – 31.12.17	10
74	תרגיל 10 (הוכחות בתחשיב הפרדיקטים)	10.1
74	הקדמה	10.1.1
75	הוכחת סילוגיזם נוסף	10.1.2
78	הוכחות של מבנים אלגבריים	10.2
78	הוכחת נייטרליות מימין בחבורה לאו דווקא קומוטטיבית	10.2.1
80	הוכחה שיש רק איבר נייטרלי אחד לחיבור	10.2.2
80	הוכחה בשדה	10.2.3
81	אקסיומות פיאו	10.2.4
81	אקסיומות צרמלו-פרנקל	10.2.5
83	שיעור 11 – 7.1.18	11
83	משפט הדדוקציה	11.1
86	נאותות ההוכחה בשלילה מתוך משפט הדדוקציה	11.1.1
86	משפט צורת הקידומת הנורמלית ( <i>Prenex Normal Form</i> )	11.2
86	תהליך המעבר לצורת קידומת נורמלית	11.2.1
87	הוכחת השקילות לצורה המקורית	11.2.2
91	שיעור 12 – 14.1.18	12
91	משפט השלמות בתחשיב היחסים	12.1
91	ניסוח המשפט והוכחת הכיוון הפשוט	12.1.1
91	הוכחת משפט נוסף	12.1.2
93	הוכחת משפט השלמות	12.1.3
97	תרגיל 12	12.1.4
98	שיעור 13 – 21.1.18	13
98	משפט השלמות והוכחתו	13.1
101	הערות של משפט השלמות – גודל המודל ומשפט הקומפקטיות	13.1.1
101	סיכום הקורס	13.2
101	סיכום: תחשיב הפסוקים	13.2.1

102 .....	סיכום: תחשיב היחסים	13.2.2
103 .....	מה לא עשינו בקורס – לקראת לוגיקה 2	13.3

**1 שיעור 1 – 22.10.17****1.1 הקדמה****1.1.1 מנהלות**

סגל הקורס –

נעם ניסן, ינאי גונצ'רובסקי

מתרגל: אלון זיו

הציון בקורס יתבסס על תרגילים (50%) ומבחן (50%). יש להגיש את כל התרגילים, אך התרגיל עם הציון הכי נמוך לא ייכנס בממוצע. על מנת לעבור את הקורס, יש לקבל ציון עובר גם בתרגילים וגם במבחן.

שעות הקבלה באתר נכונות כרגע לשבוע הזה, יתכן שישתנו בהמשך.

תרגילים – התרגילים בקורס יהיו תרגילי תכנות. המבנה של כל תרגיל יהיה דומה לזה של לתרגיל הראשון שכבר התפרסם: קובץ עם שלד לפונקציות וטסטים, וצריך להשלים את השלד. רוב הבדיקה תהיה אוטומטית על בסיס טסטים שיינתנו במודל (ואולי גם טסטים נוספים), ובנוסף מדי פעם בדיקה ידנית מדגמית. התרגילים צריכים להיות כתובים בצורה ברורה ובהירה. ההגשה היא בבודדים, יתכן שיהיו תרגיל אחד או שניים בזוגות.

המבחן בסוף הקורס יהיה מבחן מתמטי (תהיה הכנה במהלך הקורס למבחן כזה), אך חשוב לציין שלמרות שהקורס משתמש בכלים אחרים מאשר בקורס של לוגיקה למתמטיקאים, הרמה שמכוונים אליה היא אותה הרמה, וסקאלת הציונים גם היא אמורה להיות דומה. הקורס אמנם יותר מונגש למדעי המחשב, אבל לא אמור להיות יותר קל.

**1.1.2 לוגיקה: הקדמה**

נסביר קצת מה עומד מאחורי הרעיון של הקורס. כבר היוונים הקדמונים גילו את הסילוגיזם (טיעון המורכב משלוש טענות – שתי הנחות ומסקנה) הבא:

1. כל היוונים הם בני אדם
2. כל בני האדם בני תמותה
3. כל היוונים הם בני תמותה

כיוון שכל היוונים הם בני אדם וכל בני האדם בני תמותה, כל היוונים בני מותה.

חשוב לשאול בלוגיקה מה מעניין בהסקה הזאת. לב הפואנטה של העניין נעוץ בצורת ההסקה, שהיא תלויית סינטקס (תחביר) ולא סמנטיקה (משמעות) – בגלל שכל  $X$  הוא  $Y$  וכל  $Y$  הוא  $Z$ , נובע שכל  $X$  הוא  $Z$ , ולא צריך לחשוב בכלל על השאלה מה הם יוונים ומה הם בני אדם. בנוסף, אפשר להחיל את זה על דברים אחרים, לדוגמה דולפינים (כל הדולפינים הם יונקים וכל היונקים הם בעלי-חיים, אז כל הדולפינים הם בעלי-חיים). כל עוד יודעים ששתי הטענות הראשונות נכונות, אפשר להסיק את המסקנה, אפילו מבלי להבין את המשמעות. כל הפואנטה של הלוגיקה היא להחליף הסקה שמבינה על מה מדברים להסקה מתמטית, לוגית, לא תלויית משמעות, והיוונים מצאו שיטות שונות לעשות כן.

נסתכל על סט נוסף של שלוש טענות:

1. קיימים יוונים שהם בני אדם
2. קיימים בני אדם שהם בני תמותה
3. קיימים יוונים שהם בני תמותה

ברור שהמסקנה הזאת לא נכונה – שלוש העובדות הן נכונות כל אחת בפני עצמה, אבל ברור שהעובדה השלישית אינה מסקנה לוגית מהשתיים הראשונות. נשאלת השאלה המעניינת למה המסקנה הלוגית מהדוגמא הראשונה היא נכונה ומהשנייה לא.

באופן כללי, תורת הלוגיקה (ובפרט קורסים בלוגיקה) מנסים לראות מתי אפשר להסיק מסקנות מבלי להבין את הכוונה, רק על סמך הצורה שבה ניתנות הטענות. לכן, נקודה קריטית בקורסים בלוגיקה היא להסתכל כל הזמן על המשחק העדין שבין הסינטקס לבין המשמעות, הסמנטיקה. כלומר, בין הצורה לבין המשמעות. אנחנו רוצים לקבל דברים בעלי משמעות, סמנטיקה, להוכיח משפט מתמטי, על ידי מניפולציות סינטקסיות.

בכל קורסי המתמטיקה עד כה בתואר זה מה שעשינו – הנחנו הנחות והוכחנו דברים. ההוכחה שלנו לא הייתה על ידי ניסוי לדוגמא, אלא ע"י למות וגרירות. ההוכחה שלנו סינטקסית לחלוטין – כתבנו אותה על נייר, אוסף סימנים. אם מסתכלים על הוכחה כללית שנוגעת לבסיסים באלגברה לינארית, כביכול אין קשר בינה לבין מרחבים וקטוריים ומה אפשר לעשות איתם, ועם זאת, מובן שיש קשר – הוכחנו שלכל הבסיסים יש משהו משותף אנחנו מאמינים שזה נכון, כי כתבנו כל מיני צעדים בהוכחה שהובילו האחד לשני. בלוגיקה יש מחשבה יותר מעמיקה מה הקשר בין זה לבין מה שנכון.

באותה מידה, גם נימוקים במרחב הפוליטי הם סינטקסים. יש הנחות לוגיות שהם נכונות בתחום הזה ויש כאלה שלא, ובשביל להבין מה נכון ומה לא צריך להבין מה עובד ומה לא, ומה הקשר בין מה שנכון סינטקטית ומה שבאמת נכון. בקורס בלוגיקה ננסה להעביר את הנקודות האלה.

### 1.1.3 הקורס בלוגיקה

אפשר לחלק את הקורסים בלוגיקה לכמה סוגים –

- לוגיקה בפילוסופיה: מטרת הקורסים האלה היא להבין מבין הנימוקים וההסקות במילות היום יום מה באמת נכון ומתאר אמת, ומה לא נכון. כלומר, המטרה העיקרית היא לחנך את המח להבחין בצורות הסקה לוגיות נכונות, מה שלא תמיד אינטואיטיבי לבני אדם ביום יום.

- לוגיקה במתמטיקה: מנסים להבין מהן כל ההוכחות שעושים במתמטיקה – מה זה הוכחה, למה זה נכון, מה נכון – להבין את כל השיטה המתמטית שאנחנו משתמשים בה, ולא ממש ברור מה הבסיס שלה. כשאנחנו מתחילים ללמוד מתמטיקה בשנה א' לא מתחילים בדרך כלל מאקסיומה בסיסית של המתמטיקה ולאט לאט בונים מספר טבעיים ממשיים וכו', אלא מתחילים עם מספרים טבעיים, כלומר לא לומדים בצורה מסודרת את המתמטיקה החל מהצורות הבסיסיות שלה. המטרה של לוגיקה מתמטית היא להבין בדיוק מה הקשר בין מה אפשר ואי אפשר להוכיח.

בלוגיקה מתמטית יש שתי תוצאות שפחות או יותר מסכמות את כל שני הקורסים הראשונים (ואנחנו הולכים להיות כמו לוגיקה 1 מהבחינה הזאת):

- **לוגיקה 1 – משפט השלמות של גדל: משהו נכון אם ורק אם אפשר להוכיח אותו.** נשים לב ש"אפשר להוכיח אותו" זה מושג סינטקסי, ואילו "משהו נכון" זה מושג סמנטי. המשפט אומר שאם דבר מה מתקיים בכל מודל בעולם, בכל גוף בעולם (כלומר אם הוא נכון), אזי מתחייב שאפשר להוכיחו. הלוגיקה שלנו תופסת את כל מה שיש בעולם. לדוגמא, אם יש תכונה שכל המרחבים הוקטורים מסוג מסויים יקיימו אזי אפשר יהיה להוכיח אותה. גם ההפך מתקיים, ונשים לב שלמשפט יש שני צדדים: כל מה שמוכיחים הוא נכון, וזה החלק הקל. הכיוון היותר מפתיע אומר שכל דבר שתמיד נכון, כלומר שנובע במובן הסמנטי, אפשר להוכיח אותו מהאקסיומות. זה נותן בסיס יציב למתמטיקה. זה הצד האופטימי של הלוגיקה, הכל מסודר יפה ועובד, אולם בשביל התמונה היותר מלאה נדרש גם לקורס לוגיקה 2.

- **לוגיקה 2 – משפט אי-השלמות של גדל: אין לנו את האקסיומות הנכונות מהן אפשר להוכיח או להפריך כל משפט.** משמעות המשפט היא שבהנתן סט של אקסיומות, כל מה שנובע מהן הוא ניתן

להוכחה (זה נובע מהמשפט הראשון), אבל לא כל טענה ניתן להוכיח או להפריך. כשמסתכלים על סט האקסיומות של המתמטיקה היינו רוצים כל משפט נוכח או להוכיח או להפריך, אך משפט אי-השלמות אומר לנו שהמתמטיקה מוגבלת, והיא אף לא יכולה להיות כזאת שכל משפט אפשר או להוכיח או להפריך. אי אפשר להוסיף עוד אקסיומה ולסדר, ממש אי אפשר לסדר את זה. לא נגע במשפט הזה בקורס.

באופן כללי, הקורס הזה היה צריך להיות אחד היפים ביותר בלימודים – מבינים לראשונה את הקשר בין האמת לבין היופי ואת הבסיס שמצדיק את המתמטיקה. אולם, בדרך כלל זה לא הקורס האהוב ביותר על התלמידים, זאת בגלל ריבוי פרטים טכניים בהוכחות, שבדרך כלל חוזרים על עצמם בסגנון, ומקשים על הלומדים לראות את הרעיון היפה שמאחורי ההוכחה. זה קצת דומה לתכנות באסמבלי, קשה לראות את היופי של הקוד כשמתכנתים בשפה כל כך נמוכה.

מצד שני, ההבדל בין איך שמתמטיקאים לומדים לוגיקה ופילוסופים לומדים לוגיקה זה בדיוק שאת המתמטיקאי מעניין להבין משהו עד הסוף, אז אי אפשר לוותר על הפרטים. זה יוצר בעיה פדגוגית – איך נכנסים לפרטים האלה מבלי לדכא את העניין. הפתרון שניתן בקורס הזה הוא שימוש בתרגילי תכנות, ושימוש בכלים המובנים ובפידבק של שפות התכנות (כלומר דיבאגרים, טסטים). למרות שעדיין נותרת עבודה שחורה, כל העטיפה התכנותית עושה את זה ליותר ברור. נעיר שמרבית החומר בקורס אמנם ניתן לתרגום לתרגילי תכנותי אך לא כולו, ויש דברים שצריך לעשות באופן אבסטרקטי (לדוגמא משפטים עם אינסופים), ואותם נעשה באופן ידני. אולם, המסה העיקרית של הקורס יהיה התרגילים.

#### 1.1.4 תוכן הקורס

הקורס יחולק לשני פורמליזמים לוגיים, שכל אחד מהם ייקח נתח של כחצי קורס.

#### חלק ראשון – תחשיב הפסוקים (propositional logic)

ביטויים מהצורה:

$$(p \vee q) \wedge (\neg p)$$

ומשם אפשר להסיק  $q$ .

בביטוי הזה אנחנו רואים סימנים  $(\vee, \wedge, \neg)$ , ו- $p, q$  שהם משתנים בוליאניים (כלומר, מקבלים ערך אמת או ערך שקר).

בחלק הזה של הקורס נראה מה אפשר לעשות עם הדברים האלה ואיך עובדים איתם.

הנושאים שיופיעו בחלק זה (ובהתאם התרגילים) –

1. סינטקס – הביטוי שראינו הוא מחרוזת, וכדי לעשות עליו משהו צריך לעשות לו פארסינג (ניתוח מחרוזות, parsing): להבין את הסינטקס שלו, שאפשר להציג אותו בצורה של עץ. השאלה היא איזו צורת אותיות היא ביטוי לוגי שאפשר לעבור איתו, ואיך אפשר להבין את הסדרה הזאת במובן של הבנת המבנה שלה. בשלב הזה, הדגש הוא על הצורה ולא על המשמעות.
2. סמנטיקה – בשלב זה מנסים להבין מה הביטוי אמור להגיד, בנפרד מהסינטקס. להבדיל מאקסיומות של מרחב וקטורי לדוגמא, שהם התחביר, המשמעות היא איזה מרחבים מקיימים אותה. נתחיל להבין מה הקשר בין זה לבין הערכים הבוליאניים של אמת ושקר. כאן יש לנו משפט ראשון שאומר שהסינטקס הוא מספיק טוב כדי לייצג כל דבר סמנטי שאנחנו רוצים, בפרט שכל פונקציה בוליאנית אנחנו יכולים לייצג בצורה כזאת (כלומר כמחרוזת כזאת).
3. עוד קשרים – כלומר, יש לא רק או וגם אלא גם עוד קשרים שיכולים להעשיר את השפה שלנו, ונראה איך מתרגמים בין שפות יותר ופחות עשירות.
4. הוכחות – מהי הוכחה בתחשיב הפסוקים? הוכחה זה סדרת דברים שמסיקים משהו משהו אחר, וצריך לכל הפחות שמה שגסיק יהיה נכון. נסביר כאן מהן הוכחות ומהי הוכחה נכונה, ולאחר מכן נתחיל לעבוד עם הוכחות. נכתוב תוכנית שמקבלת הוכחה ומחזירה האם היא הוכחה או לא הוכחה.
5. תכונות של הוכחות – ההוכחה תהיה משהו סינטקטי, מחרוזות שנובעות זו מזו, ומאוד מוגבל. אנחנו רגילים במתטיקה להוכחות יותר עשירות מאשר מה שנעשה כאן, כי אנחנו שם בשפת על, וכאן בשפת אסמבלר. כדי שנוכל להתחיל לעבוד כמו שצריך צריך לדעת שאנחנו יכולים לעשות דברים. לדוגמא, נראה שהוכחה בשלילה



היא נכונה, שיש לה את התכונה שאם יש הוכחה שמוכיחה משהו בשלילה אפשר להוציא הוכחה אחרת שלא משתמשת בשלילה, מעין קומפיילר קטן מהוכחות בשלילה ללא בשלילה.

6. משפט השלמות (משפט הטאוטולוגיה) – משפט הטאוטולוגיה הוא משפט השלמות בתחשיב פסוקים, שאומר שכל דבר שהוא נכון אפשר להוכיח אותו (לפי איך שהגדרנו הוכחה). זו גולת הכותרת של החלק הזה.

## חלק שני – תחשיב הפרדיקטים (predicate logic), הקרוי גם לוגיקה מסדר ראשון (first order logic)<sup>1</sup>

תחשיב הפסוקים הוא מוגבל בכוחו, ולא יכול להביע כל דבר. תחשיב הפרדיקטים מאפשר לנו להגיד משפטים כמו במתמטיקה:

$$\forall x \exists y s.t. x + y = 0$$

עכשיו  $x, y$  הם לא אמת ושקר, אלא מספרים בעולם שאנחנו מדברים עליו, ומה שיפה בתחשיב היחסים זה שהוא קולט את כל הלוגיקה שאנחנו משתמשים באופן רגיל: כל המתמטיקה שלמדנו עד כה ניתנת לפרמול בתחשיב הזה עם מערכת אקסיומות ספציפית.

החשיבות של הלוגיקה התגלתה בתחילת המאה ה-20, כשאנשים החלו להיות מודאגים מהשאלה מה בסיס המתמטיקה. משבר שחיק את הרצון להבין מה יסודות המתמטיקה הגיע עם הצגת הפרדוקס של ראסל –

יש קבוצות שלא מכילות את עצמן, לדוגמה קבוצת כל השלמים לא מכילה את עצמה כי היא קבוצה ולא שלם. יש קבוצות שכן מכילות את עצמן, לדוגמה קבוצת הקבוצות שיש בהן לפחות ארבעה איברים. נסתכל על קבוצת כל הקבוצות  $S$  כך ש- $S$  לא מכילה את עצמה:

$$R = \{S \mid S \notin S\}$$

נשאלת השאלה – האם הקבוצה  $R$  מכילה את עצמה (האם  $R \in R$ )? כאן מתגלה הפרדוקס – אם היא מכילה את עצמה, הרי שהיא לא שייכת לקבוצת הקבוצות שלא מכילות את עצמן, ולכן לא מכילה את עצמה. אם היא אינה מכילה את עצמה, הרי שהיא שייכת לקבוצת הקבוצות שלא מכילות את עצמן, ולכן מכילה את עצמה.

יש כאן בעיה – כתבנו משהו מתמטי בהיר לחלוטין, והגענו לסתירה. זאת הייתה הבעיה בתחילת המאה ה-20, כי זה שם בספק את כל המתמטיקה – אם יש כאלה סתירות, הבסיס של המתמטיקה לא כל כך מוצק. לכן, ניסו להבין מה לוגיקה נכונה ומה לא. תורת הקבוצות המודרנית באמת מספקת כללים שאומרים מה כן ומה לא קבוצה, ושם הקבוצה של ראסל לא עונה לכללים האלה. הצורך הזה בלהבין בדיוק מה כן ומה לא סיכן את כל יסודות המתמטיקה, ולוגיקה מסדר ראשון זו השפה שתעזור לנו להבין את זה. בחלק זה, בגדול, נעבור פחות או יותר על אותו הסדר שעברנו בחצי הראשון, רק עם הלוגיקה היותר שלמה.

1. סינטקס + סמנטיקה – הפעם ביחד, אך נשים לב שאנחנו יודעים להפריד ביניהם.
2. עוד קשרים – קצת פחות מאשר בחלק הראשון. דוגמא לדבר שנעשה הוא לנסות לא להשתמש בפונקציות ובשווה, שקצת קשים לשימוש, ונראה במה אפשר להחליף אותם.
3. הוכחות – נצטרך הוכחות אחרות לסימבוליזם הזה, אז נגדיר מחדש הוכחות, ונרוויח שנקבל בחינם את כל מה שהוכחנו בחצי הראשון (נראה איך עושים את זה). כמו כן, תהיינה הוכחות חדשות שנצטרך לעשות.
4. תכונות של הוכחות – גם כאן נבנה "מיני קומפיילרים" שיעזרו לנו להוכיח הוכחות. אתגר מקדים: נחשוב על מערכת האקסיומות המינילית של האובייקט המתמטי חבורה:

$$x + 0 = x \quad a.$$

$$x + (-x) = 0 \quad b.$$

$$(x + y) + z = x + (y + z) \quad c.$$

$$0 + x = x \quad \text{נטען שמכאן נובע}$$

הקושי המתמטי של להוכיח דברים כאלה מתקשר עם הקושי של השפה, לכן נצטרך לעשות עוד שלבים בדרך, אבל אפשר בינתיים לחשוב על זה.

<sup>1</sup> בספרות ניתן למצוא גם שימוש במונח "תחשיב היחסים"

5. משפט השלמות – שוב, גולת הכותרת של החלק הזה. כאן זה יהיה השלב שיצדיק סופית את לימודי המתמטיקה עד היום.

## 1.2 נוסחאות בנויות היטב

### 1.2.1 הגדרה ומשמעות

הגדרה – המחרוזות הבאות הן **נוסחאות בנויות היטב** (EXP):

א. כל דבר מהצורה –

מספר א א א

שבהם האות בין  $p - z$ , והמספר לא חייב להופע.

לדוגמא, טוב:  $q13, x$

לדוגמא, לא טוב:  $qq, a7$

אלה הם **משתנים אטומיים** או **פסוקיות אטומיות**.

ב. כל דבר מהצורה –

$\sim EXP$

לדוגמא, טוב:  $\sim \sim p$ ,  $\sim p12$  (למה השני טוב:  $\sim p$  בנויה היטב בגלל א', ומכאן  $\sim \sim p$  וכו')  
לדוגמא, לא טוב:  $(p)$  (למה לא: בגלל הסוגריים, לפי הכללים אסור לשים סוגריים אחרי טילדה)

ג. כל דבר מהצורה (כולל הסוגריים) –

$(EXP|EXP)$

לדוגמא, טוב:  $(p|q3)$

לדוגמא, לא טוב:  $p|q3, p|q3$  (לא טוב כי אין סוגריים)

ד. כל דבר מהצורה (כולל הסוגריים) –

$(EXP\&EXP)$

ברגע שיש את הכללים האלה, אפשר לעשות דברים יותר מורכבים, לדוגמא:

$\sim \sim ((p|q)\&q)$

איך יודעים שזאת נוסחא? שוב, מסתכלים לאט לאט –  $(p|q)$  נוסחא בגלל ג', לכן  $(p|q)$  בגלל ב', לכן  $(p|q)$  בגלל א' נוסחא בגלל ב' וכו'.

נקודה חשובה – שום דבר אחר הוא לא נוסחא. רק מה שנבנה אותו ככה הוא נוסחא.

מבחינה מתמטית, אפשר להתרעם על כך שהגדרנו נוסחא ע"י אוסף של כללים שמשתמשים בעצמם, שהגדרנו נוסחא במונחים של נוסחא. עם זאת, ההגדרה המתמטית הרקורסיבית הזו היא הגדרה מתמטית טובה, והכוונה בה היא שמתחיים מהדברים המובטחים והולכים עוד ועוד צעדים לפי הדברים שמובטחים, ובאינסוף מקבלים קבוצה שהיא כלל הנוסחאות בקבוצה. מה שמחוץ לקבוצה, כלומר שאי אפשר להגיע אליו ע"י מספר סופי של פעולות כאלה, הוא לא נוסחא תקינה.

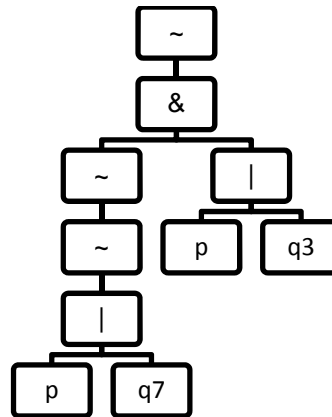
### 1.2.2 הנוסחא כעץ

נסתכל על הביטוי הבא –

$$\sim(\sim\sim(p|q7)\&(p|q3))$$

נשאל את עצמינו האם הביטוי המסובך הזה הוא נוסחא תקנית או לא, ואם כן, מה המשמעות שלה (איך אנחנו צריכים לחשוב בראש שלנו על נוסחא שבנויה מסט של כללים כאלה).

היינו רוצים לכתוב על זה בתור עץ, שעליו מסתכלים בשתי דרכים – הראשונה, עץ לוגי מתמטי, הצורה המתמטית שמתארת את העניין הזה, והשנייה מבנה הנתונים בתוכנה שאנחנו מכירים. העץ של הביטוי הנ"ל יראה כך:



זה המבנה הפנימי שנובע מהצורה הסינטקסית הזאת, זה מה שמעניין אותנו. גם כשנתאר מה משמעות הדברים, נוכיח הוכחות לפעמים באינדוקציה על מבנה הנוסחא – זה יהיה האובייקט המתמטי שנעבוד איתו, לא המחרוזת.

האם כל נוסחא אפשר להפוך לעץ? כן, וזה נובע מההגדרות הרקורסיביות בנוסחא חסרת הקשר – הגדרנו נוסחא ע"י כללים סינטקסיים. כל דבר שאפשר להגדיר בצורה הזאת, בדקדוק חסר הקשר, אפשר יהיה להפוך לעץ. יותר מזה, אם לא הצלחנו להפוך את הנוסחא לעץ, בהנחה שלאטענינו סימן שמראש המחרוזת היא לא ואלידית.

האם יש רק דרך אחת לעשות את זה? אצלינו לא – הסיבה שהתעקשנו על הסוגריים היא שתהיה דרך אחת להבין את זה. המשפט המתמטי שלומדים לרוב בשלב הזה בקורס לוגיקה מתמטית נקרא משפט הקריאה היחידה:

**משפט הקריאה היחידה** – לכל נוסחא בנויה היטב יש דרך יחידה להצגה בעץ.

זה משפט שתלוי ממש בסינטקס שניתן לנו. איך נוכיח את המשפט – בתרגיל צריך לעשות את פארסינג לנוסחא ולהפוך אותה לעץ, ונראה שיש רק דרך אחת לעשות את זה.

איך נעשה את הפארסינג? סוג האתגר של לקחת דקדוק ולקבל טקסט שבנוי לפיו נקרא פארסינג, וזה אתגר נפוץ במדעי המחשב, לדוגמא זה מה שכל קומפיילר צריך לעשות דבר ראשון כשהוא עובד על תוכנית. הקלט שלנו יהיה מחרוזת שבנויה לפי הכללים האלה, ואנחנו נרצה לגלות מה המבנה שלה. נחלק למקרים –

- אות ראשונה אות – בונים עץ שבו האות (או האות והמספרים אחרי) הם השורש.
- אות ראשונה ~ – בודקים ברקורסיה שמה שמופיע אחרי הטילדה הוא ביטוי.
- אות ראשונה ( – צריך למצוא את השורש. לא נגיד בדיוק איך עושים את זה (זה נשאר לתרגיל), רק נדבר באופן כללי על שתי דרכים: דרך ראשונה היא באמצעות ספירה של פתיחה וסגירה של סוגריים. דרך שנייה – הדקדוק שאנחנו משתמשים בו הוא מסוג LLO, כלומר אפשר לעשות לו פארסינג על ידי מעבר תו אחרי תו מבלי להסתכל קדימה על תווים נוספים בכל שלב. לכן, אם ראינו פתח סוגריים אפשר לדעת ישר שאנחנו נמצאים בכלל שלושה. בגלל צורת הפארסינג הזאת, ובכלל שאף ביטוי הוא לא רישא של ביטוי אחר, אם נלך מימנה ברקורסיה תהיה רק נקודה אחת שכל מה שראינו עד אליה יהיה יחד ביטוי תקני. לא בכל שפה זה כך, כמובן, אבל בשפה שלנו כן. כלומר, נוכל לקרוא מההתחלה עד שנגמר ביטוי, וזה יעבוד, כי אין אף ביטוי שהוא רישא של ביטוי אחר.

ניתן כעת אלגוריתם כללי, שאמנם לא משתמשים בו באופן מעשי כי הוא ארוך וגם אנחנו לא נרצה להשתמש בו, אבל הוא כללי לחלוטין, ויעבוד לכל דבר מהצורה הזאת (אפילו שכרגע נסתפק בלתאר אותו רק עבור הדקדוק שלנו). זהו אלגוריתם של תכנון דינמי, הוא הולך כך –

- נניח שאורך המחרוזת הוא  $s$ . נשמור מטריצה בגודל  $s \times s$
- עבור כל תא במטריצה, מספר השורה של התא ייצג את נקודת ההתחלה של תת-המחרוזת, ומספר העמודה את נקודת הסיום
- הרעיון:  $M[i, j] = \text{True}$  אם תת-המחרוזת מ- $i$  עד  $j$  היא נוסחא בנויה היטב

במטריצה יהיה ייצוג עבור כל תת מחרוזת, ע"י אלגוריתם בתכנון דינמי. האלגוריתם ימלא את הטבלה לפי אלכסונים, החל מהאלכסון הראשי, לאחר מכן זה שמעליו וכו' (אין צורך למלא את מה שמתחת לאלכסון הראשי, כי לא יתכן שנקודת ההתחלה לפני נקודת הסיום) –

- מתי תת-מחרוזות באורך 1 הן ביטוי – רק אם זה אות, לכן אפשר למלא את כל האלכסון (כל מה שמתחת האלכסון ריק ולא קיים, אין מחרוזות כאלה).
- מחרוזות באורך 2 – או שהוא מתחיל במספר, או שיש לפני ~ ואז התחלה של ביטוי, או ( ואז ביטוי. אז איך יודעים איפה האמצע? אפשר לנסות את כל האפשרויות – מסתכלים מה כל המקומות שיכול להיות להופיע הקשר באמצע, ואז רואים אם משני הצדדים יש ביטוי. אם היינו עושים ברקורסיה זה היה מגיע למספר אקספוננציאלי, אבל כאן נוכל להעזר במטריצה ובכך כבר מילאנו ביטויים יותר קצרים כאלה, אז רק צריך לבדוק מה רשום שם. הרעיון הוא שאפשר לעבור ולמלא את המטריצה לפי מחרוזות הולכות וגדלות, בהתאם לתאים הקודמים שמילאנו. זו שיטה שעובדת לכל דקדוק חסר הקשר.

נעיר שכל מה שתיארנו עד עכשיו רק אומר בסוף אם המטריצה השלמה היא טובה, ואנחנו גם היינו רוצים לדעת מה נקודת החלוקה עבור ביטויים מהסוג של ג' ו-ד'. לכן, תוך כדי המילוי נשמור את הערכים האלה במטריצה נוספת (במילים אחרות, אנחנו רוצים גם את החלוקה עצמה ולא רק אם קיימת חלוקה).

נשים לב שיש מספר דרכים לסרוק עצים –

- **in order (או infix notation):** זו ההצגה שראינו עד כה – עבור כל דקדוק מדפיסים את דקדוק שמאל, מדפיסים את השורש ואז מדפיסים את דקדוק ימין.  
לדוגמא, עבור העץ שראינו קודם –  $\sim(\sim(p|q7)\&(p|q3))$
- **preorder (או polish notation):** עבור כל דקדוק מדפיסים קודם את השורש, אחר כך את דקדוק שמאל ואז את דקדוק ימין (ואם יש רק צד אחד, רק אותו).  
נשים לב שאין כאן צורך בסוגריים, כלומר יש כאן משפט קריאה יחידה בלי סוגריים. נוכיח את זה בתרגיל ע"י זה שנעשה פראסינג לביטוי הזה ונראה שאנחנו מצליחים לחלץ את העץ.  
לדוגמא, עבור העץ שראינו קודם –  $\sim\&\sim|pq3|pq7|p$
- **postfix notation (או reversed polish notation):** יכול להיות נח כי אפשר לחשב באמצעותו את הביטוי עם מחסנית וללא צורך בסוגריים (פרקטית, זה יכול להיות נח לדוגמא למחשבון).  
לדוגמא, עבור העץ שראינו קודם –  $q3p|q7p|\sim\&\sim$

בשיעור הבא נדבר על המשמעות הלוגית של נוסחאות בנויות היטב, ועל אילו פונקציות בוליאניות אפשר לייצר.

## 2 שיעור 2 – 29.10.17

### 2.1 חזרה

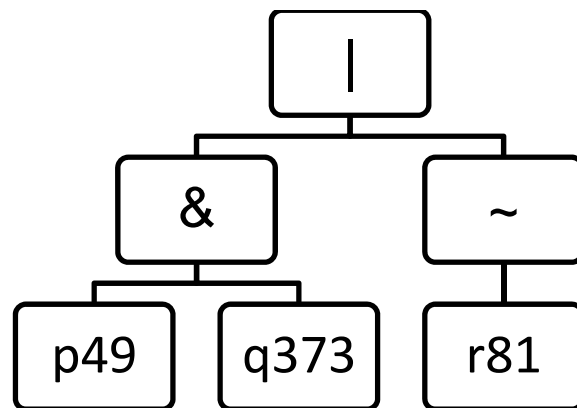
בשיעור שעבר דיברנו על הרעיון הבא: רוצים להוכיח שבכל שדה אלגברי, לכל איבר  $a$  מתקיים  $a \cdot 0 = 0$ . הדרך שהיינו מצפים לעשות את זה היא לעבור שדה שדה ולהראות את קיום הטענה בצורה פרטית לכל השדות שקיימים, עד שנשתכנע. במתמטיקה, במקום לעבור על כל השדות כותבים קטע טקסט שמהווה הוכחה, ולאחר ההוכחה אנחנו יכולים להיות בטוחים שזה מתקיים לכל שדה, ממש באותה מידה כמו אם היינו עוברים שדה אחר שדה.

ראינו גם שכל דבר שהוא נכון לכל שדה קיים עבורו אוסף של משפטים בעברית שישכנע אותנו שהדבר הזה נכון (כלומר הוכחה), כל דבר שאפשר להגיד עליו שהוא נכון לכל השדות אפשר להוכיח אותו. נקודה מעניינת, אותה נראה בהמשך הקורס, היא שאפילו שיש מספר אינסופי של שדות, אם משהו נכון תמיד אפשר לכתוב הוכחה סופית שתוכיח אותו.

בתרגיל הראשון ובשיעור הקודם דיברנו על איך נראית נוסחא. היום נדבר על מה משמעות הנוסחא. כלומר, אם היינו רוצים לעבור על כל השדות ולבדוק נדבר על מה זה שהיינו בודקים בכל שדה, מה המשמעות של נכון או לא נכון בשדה מסויים.

### 2.2 מבנה (מודל) וטבלאות אמת

נסתכל על הנוסחא הבאה:



נגדיר כעת הגדרה שתעזור לנו לנסח היטב את השאלה מה נכון או לא נכון.

**מבנה (model) –** מבנה עבור נוסחא  $f$  הוא השמה של "ערכי אמת" לכל משתנה (נוסחא אטומית) ב- $f$ .

לדוגמא, במקרה שלנו יש שלוש נוסחאות אטומיות, ומבנה עבור הנוסחא שלנו יגיד לנו עבור כל אחת מהנוסחאות האטומיות האלה אם היא שקר או אמת.

כלומר, המבנה יהיה פונקציה מהצורה:  $M: \{p49, q373, r81\} \rightarrow \{T, F\}$ .

המבנה מספר לנו רק את ערך האמת של נוסחא אטומית, ונראה למצוא דרך להעזר במודל כדי לדעת האם הנוסחא כולה נותנת ערך אמת או ערך שקר.

נסתכל על כל אחד מהקשרים שלנו:

• **Not** – שלילה של נוסחא אטומית תיתן אמת אם "מ ערך הנוסחא האטומית הוא שקר.

לדוגמא, אם  $\sim r81 = F$  אז  $M(r81) = T$

- **And** – גימור בין שתי נוסחאות אטומיות ייתן אמת אם"מ ערכי שתי הנוסחאות האטומיות הם אמת. לדוגמא, אם  $(p49 \& q373) = F$  אז  $M('q373') = F$  ו-  $M('p49') = T$

- **Or** – איור בין שתי נוסחאות אטומיות ייתן אמת אם"מ לפחות אחד מהערכים שהוא מקבל הוא אמת. לדוגמא, אם  $(p49 \& q373) = T$  אז  $M('q373') = F$  ו-  $M('p49') = T$

הערה – ה-"או" שאנחנו מדברים עליו נקרא *inclusive*, זאת לעומת *exclusive* "או", שמקבל אמת רק אם ערך אחד בדיוק הוא אמת (*Xor*).

נכתוב את הערך של הנוסחא הזאת עבור כל המודלים האפשריים – **טבלת האמת** של הנוסחא.

$p49$	$q373$	$r81$	$\sim r81$	$(p49 \& q373)$	$f$
$F$	$F$	$F$	$T$	$F$	$T$
$F$	$F$	$T$	$F$	$F$	$F$
$F$	$T$	$F$	$T$	$F$	$T$
$F$	$T$	$T$	$F$	$F$	$F$
$T$	$F$	$F$	$T$	$F$	$T$
$T$	$F$	$T$	$F$	$F$	$F$
$T$	$T$	$F$	$T$	$T$	$T$
$T$	$T$	$T$	$T$	$T$	$T$

\*הערה – בד"כ נהוג לכלול בטבלה רק את המשתנים ואת  $f$ , הוספנו עוד עמודות לצורך נוחות.

\*\*הערה 2 – הכוונה בעמודה הימנית ביותר היא ערך הנוסחא כולה, כלומר:  $f = ((p49 \& q373) | \sim r81)$

טבלת האמת והמודל נותנים לנו התחלה של פורמליזציה שתעזור לנו בהמשך להגדיר מהי הוכחה, מה הדרך להראות שמשהו מתקיים.

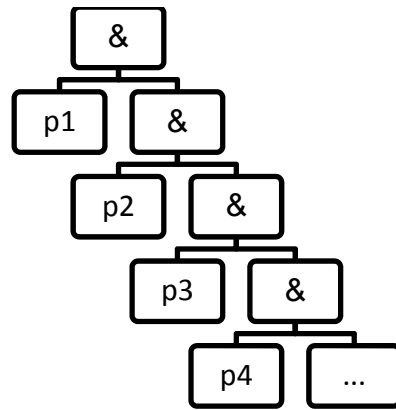
כמה טבלאות אמת יש לנוסחאות שכתובות באמצעות שלושה משתנים?  $2^3$ : עבור שלושה משתנים יהיו  $2^3$  שורות, שורה אחת עבור כל קומבינציה סדורה של ערכי אמת ושקר לכל שורה (כמו שאכן רואים בטבלה שעשינו). לעמודה הימנית שני ערכים אפשריים עבור כל משבצת, כלומר  $2^3$  אפשרויות סה"כ (כי יש שתי אופציות למשבצת הראשונה ראשונה, שתיים לשנייה וכו', כלומר  $2 \cdot 2 \cdot \dots \cdot 2$ , סה"כ מספר השורות  $2^3$ , ואמרנו שמספר השורות הוא  $2^3$ ).

קיבלנו מספר אקספוננציאלי של טבלאות, וזה רק עם שלושה אופרטורים שאנחנו משתמשים בהם.

האם נוכל לכל אחת מ-  $2^3$  הטבלאות האלה להתאים נוסחא שנותנת את טבלת האמת הזאת? התשובה היא חיובית – באופן מפתיע, אפשר באמצעות *and*, *not*, *or* למצוא נוסחא לכל אחת מטבלאות האמת האלה (ושבוע הבא נראה שגם באמצעות פחות אופרטורים).

האם זה נכון גם באינסוף משתנים? אפשר הרי להגדיר טבלת אמת גם לאינסוף משתנים, אז נרצה לשאול האם זה נכון שגם עבורה יש פונקציה רק עם *and*, *not*, *or* שנותנת את הנוסחא. לדוגמא, יש לנו  $p_1, p_2, \dots$  עד אינסוף, וטבלת האמת שלנו היא הטבלה שבה כל הערכים הם  $F$  למעט במקרה שכל המשתנים הם  $T$  ואז הערך הוא  $T$ .

רעיון ראשוני לבניית נוסחא שכזו – נעשה *and* על כל המשתנים, כלומר נבנה את העץ האינסופי הבא:



אולם, זו לא נוסחא, בגלל האופן שבו הגדרנו נוסחא – בשביל להוכיח שהשלב הראשון בעץ הוא נוסחא צריך להוכיח ששלב אחת למטה הוא נוסחא, ובשביל לעשות את זה צריך להוכיח ששלב מתחתיו הוא נוסחא וכך הלאה.

למעשה, אין נוסחא שמכילה בתוכה אינסוף משתנים, כי לפי מה שהגדרנו כל נוסחא היא באורך סופי. נשים לב לאבחנות הבאות בנושא:

- יש אינסוף נוסחאות
- נוסחא יכולה להיות ארוכה ככל שנרצה (כלומר, קיימת נוסחא בכל אורך סופי שהוא)
- כל נוסחא בעצמה צריכה להיות סופית

זה מזכיר מעט טעות רווחת בנוגע לאינדוקציה – הרבה פעמים כשלומדים בתיכון אינדוקציה חושבים שהיא כוללת להוכיח לאינסוף. אין כאן הוכחה לאינסוף, אלא לכל מספר סופי. דוגמא פשוטה להמחשה – נוכיח באינדוקציה שלכל קבוצה בגודל סופי יש גודל סופי, מה שברור למדי כיצד ניתן לעשות. אם חושבים שאינדוקציה זה להוכיח גם לאינסוף מקבלים שגם לקבוצה אינסופית יש גודל סופי, וזה כמובן לא נכון.

בשביל להוכיח פורמלית שאין שום נוסחא שטבלת האמת שלה היא טבלה באינסוף משתנים, נניח בשלילה שקיימת נוסחא כזאת. אזי, יש בה מספר סופי של משתנים (לפי מה שראינו קודם), לכן אחד מאינסוף המשתנים שלנו לא מופיע בה. מכאן לא משנה מה שמנו במשתנים שלא מופיעים, ואין צורך לכלול אותם בטבלה, מה שמחזיר אותנו לטבלה בגודל סופי, בסתירה.

נשים לב שיש אינסוף נוסחאות ורק מספר סופי של טבלאות אמת, לכל טבלת אמת יש אינסוף נוסחאות שמתאימות לה. לקחת שתי נוסחאות ולענות על השאלה האם הן מתאימות לאותה טבלת אמת זו בעיה קשה (בחישוביות אומרים שהיא *coNP* קשה), אנחנו לא מכירים באמת דרך יותר טובה לעשות את זה מאשר לעבור שורה שורה (מבחינת יעילות).

## 2.3 טאוטולוגיה, סתירה ונוסחא ספיקה

מושג שנתקל בו לראשונה בתרגיל השני ונמשיך לעסוק בו כעת הוא מושג ה**טאוטולוגיה**. טאוטולוגיה זה משהו שהוא נכון תמיד, במקרה שלנו –

🔗 **טאוטולוגיה** – נוסחא  $f$  היא טאוטולוגיה אם היא נכונה בכל מודל.

כלומר, בתחשיב הפסוקים שלה אם נסתכל על טבלת האמת נראה רק  $T$  בעמודה הימנית.

דוגמא לטאוטולוגיה –  $(p \sim p)$ .

איך בודקים אם נוסחא היאטאוטולוגיה? דרך אחת היא לעבור מודל-מודל, ולבדוק אם היא מקבלת ערך אמת בכל אחד מהמודלים האלה. אולם, כמות המודלים אקספוננציאלית בכמות המשתנים, כלומר זה לוקח הרבה זמן, ונרצה למצוא

דרך יותר קלה לעשות את זה. עם זאת, מסתבר שאנחנו לא מכירים שום דרך לבדוק אם נוסחא היא טאוטולוגיה שהיא משמעותית יותר טובה מהדרך של לעבוד אחד אחד.

לבדוק האם נוסחא היא טאוטולוגיה זה קשה, אבל נניח שיש לנו נוסחא שאנחנו יודעים אם היא טאוטולוגיה, ונרצה לשכנע בכך משהו אחר. לשכנע שזו לא טאוטולוגיה זה קל, כי מספיק להראות מודל מסויים שבו יש ערך שקר כדי להוכיח שהנוסחא אינה טאוטולוגיה.

מה עם לשכנע שכן? התשובה היא שזו שאלה קשה, פחות או יותר כמו לבדוק מראש האם הנוסחא טאוטולוגיה או לא (אפשר לעשות את זה ע"י מציאת הוכחה, אבל ההוכחה תהיה ארוכה, בערך באותה פרופורציה של לעבור אחד אחד).

לסיכום: האם  $f$  טאוטולוגיה – קשה להוכיח, לשכנע שלא – קל, לשכנע שכן – קשה.

**סתירה** – נוסחא  $f$  תקרא סתירה אם היא לא נכונה באף מודל.

דוגמא לסתירה –  $(p \& \sim p)$

מה יותר קשה, לבדוק האם נוסחא היא סתירה או טאוטולוגיה? נשים לב שאם ניקח סתירה ונשלוף אותה נקבל טאוטולוגיה, ואם נקח טאוטולוגיה ונשלוף אותה נקבל סתירה. בגלל הקלות הזאת במעבר בין שני הסוגים, אפשר להבין ששתי ההוכחות קשות באותה המידה.

נכניס כעת מושג נוסף, שיבטא את ההפך של סתירה – כלומר, משהו שנכון במודל כלשהו. להפך של סתירה קוראים:

**נוסחא ספיקה** –  $f$  היא ספיקה אם איננה סתירה.

מאותן סיבות שראינו קודם, לשאול האם  $f$  היא סתירה זה קשה, לשכנע שהיא סתירה זה קשה, ולשכנע שהיא לא סתירה זה קל (נותנים מודל שמתאים לה). בעיית הספיקות (כלומר הבעיה שבה מקבלים נוסחא וצריך להגיד אם היא ספיקה) היא  $NP$ -שלמה, ולא רק זה אלא שהיא הבעיה ה- $NP$ -שלמה הראשונה שידועה (נסביר קצת מה זה אומר בשיעור הבא, ולמה היא בעיה מרכזית במדעי המחשב).

הערה – עד כה, בכל הקורסים שראינו, דוגמא נגדית וסתירה היו מילים נרדפות. בקורס שלנו, סתירה היא מה שהגדרנו, בעוד דוגמא נגדית היא דוגמא שמראה שמהו לא נכון. בשביל לחדד את ההבדל: כדי להוכיח שמהו הוא לא סתירה מספיק למצוא דוגמא נגדית.

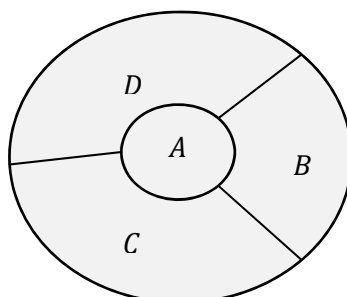
## 2.4 פתרון בעיות באמצעות תחשיב הפסוקים – צביעת המפות ומכירת התדרים

למה טאוטולוגיה וסתירה הם שימושיים, ולמה בכלל תחשיב הפסוקים שימושי? ניתן שתי דוגמאות:

### 2.4.1 בעיית צביעת המפות

**הבעיה:** נתונה לנו מפה (לדוגמא מפת העולם), ורוצים לצבוע כל מדינה בצבע כלשהו, אבל כדי שהמפה תהיה קריאה דורשים שלא תהיינה שתי מדינות גובלות באותו הצבע. נעיר שאנחנו מתייחסים להגדרה סבירה של מפה (לא נדבר נניח על מקרים שבהם כמה שטחים נפרדים שייכים לאותה מדינה וצריך לצבוע אותם באותו הצבע). נשאלת השאלה כמה צבעים אנחנו צריכים.

**תשובה:** אפשר להוכיח שחמישה צבעים מספיקים (לא נעשה זאת כעת, אך זו הוכחה נפוצה שמופיעה בין השאר בקורסי מתמטיקה דיסקרטית), ואפשר לתת דוגמא שמראה ששלושה צבעים לא מספיקים:





בדוגמא ארבע מדינות שגובלות כולן אחת בשנייה, לכן ברור ששלושה צבעים לא יספיקו.

מה בנוגע לארבעה? רק בשנות השבעים הצליחו להוכיח באמצעות מחשב שגם ארבעה צבעים מספיקים. מה שעשו היה להוכיח שיש מספר מסויים של מפות (באיזור האלף) שמספיק להראות שכל אחת מהן אפשר לצבוע בארבעה צבעים כדי שאפשר יהיה לצבוע כל מפה בארבעה צבעים, ואז הוכיחו פרטנית באמצעות מחשב שאפשר לצבוע את המפות האלה.

**מעבר לנוסחא:** נרצה עכשיו לכתוב נוסחא שהיא ספיקה אמ"מ אפשר לצבוע את המפה בארבעה צבעים, כלומר שתקבל אמת רק אם הצביעה היא חוקית.

- נקח מפה מסויימת, שבה 500 מדינות.
- נגדיר את 2,000 המשתנים הבאים –  $p_{\substack{b \\ *}}^{\substack{b \\ **}}$  (\* מספר בין 1 ל-4, \*\* מספר בין 1 ל-500).
- הספרה הראשונה בכל משתנה תייצג את הצבע, השנייה את מספר המדינה.
- כדי שהצביעה תהיה חוקית, נסתכל על סט הדרישות הבא, ולפי כל אחת נגדיר כללים לבניית הנוסחא שלנו –
  - מדינה לא יכולה להיות צבועה בשני צבעים שונים: לכל מדינה  $s$  וצבע  $c \neq d$  נגדיר:  $(\sim pcs | \sim pds)$  (נעשה זאת עבור כל זוג של צבעים).
  - שתי מדינות גובלות לא יכולות להיות צבועות באותו הצבע: לכל שתי מדינות גובלות  $s, t$  ולכל צבע  $c$  נאמר:  $(\sim pcs | \sim tct)$ .
  - כל מדינה צבועה באיזשהו צבע: לכל מדינה  $s$  נאמר:  $(p1s | p2s | p3s | p4s)$

מתוך זה נבנה את הנוסחא:

$$f = (\sim p1001 | \sim p2001) \& \dots \left( \begin{matrix} \text{כל הנוסחאות} \\ \text{מצורה א} \end{matrix} \right) \& \dots (\sim p1001 | \sim p1002) \& \dots \left( \begin{matrix} \text{כל הנוסחאות} \\ \text{מצורה ב} \end{matrix} \right) \& \dots \left( \begin{matrix} \text{כל הנוסחאות} \\ \text{מצורה ג} \end{matrix} \right) \dots$$

בנינו נוסחא  $f$  שמודל עבורה ייתן לה ערך אמת אמ"מ הוא צביעה חוקית של המפה בארבעה צבעים, מה שאומר שלמצוא האם קיימת צביעה חוקית כזו שקול כעת ללהגיד שהנוסחא ספיקה.

היכולת לפרמל את הבעיה לצורה של נוסחא אומרת לנו שאם נלמד לפתור בעיות מהסוג הזה מהר, נוכל לצבוע מהר את כל המפות בארבעה צבעים.

## 2.4.2 המכירה הפומבית של התדרים בארה"ב Spectrum Auction

**הבעיה:** בארה"ב יש הרבה תחנות טלוויזיה, ולמרו שחלקן כבר לא פעילות, הרשיון לתדר השידור נמצא אצל מי שקנה את תדר התחנה במקור. עם השנים הופיעו ספקי סלולרי רבים, ונוצר מצב שבו תדר שווה יותר לספקי סלולר ממה שהוא שווה לתחנות טלוויזיה.

ספקי סלולרי יכולים לקנות תדר מסויים, אבל הוא שווה להם רק אם הם יכולים לשדר בתדר הזה באיזור די גדול, וגם יש להם את התדרים הסמוכים לו. נוצר מצב שבו ספקי סלולרי היו מוכנים לשלם הרבה על תדרים והרבה תחנות טלוויזיה היו מוכנות למכור, אבל התיאום היה מסובך.

ממשלת ארה"ב החליטה להסדיר את העניינים על-ידי כך שהיא קיימה מכירה פומבית גדולה של התדרים, ובו-זמנית גם מכירה פומבית הפוכה – הספק שמוכן לשלם את המחיר הגבוהה ביותר יזכה לקנות, והתחנה שמציעה למכור במחיר הכי נמוך היא זו שתמכור.

בשלב כלשהו מגיעים למצב שכל התחנות שהיו מוכנות למכור בזול מכרו, כל הספקים שמוכנים למכור ביוקר קנו, ובשביל שהתחנה הבאה שמוכנה למכור תמכור אז הספק הבא כבר לא מוכן לשלם (או שיש ספק שמוכן לשלם אבל ההפרש בין הצעת המחיר ובין מחיר הקנייה כבר לא משתלם למדינה, שלוקחת נתח מהעסקה).

הבעיה היא שגם בשלב הזה עדיין יש המון חורים בספקטרום בגלל שלא כל האנשים היו מוכנים למכור את התדרים שלהם, ולכן הממשלה הזיזה את כל מי שלא היה מוכן למכור מתדר אחד לאחר. עם זאת, נקבע שהפגיעה צריכה להיות מידתית – אי אפשר להזיז משהו לתדר אחר אם זה פוגע באיזור שבו קולטים אותו מעבר למידה מינימלית שהוגדרה (כלומר, אם הוא שידר באיזורים גיאוגרפיים מסויימים הוא צריך לקבל תדר שמסדר בערך באיזורים האלה).

**מעבר לנוסחא:** נמדל את הבעיה הזאת באמצעות תחשיב הפסוקים (ונציין גם שאין שזה התבצע בפועל היה די דומה למה שנעשה). כדי לעשות זאת, נעזר בגרף לא מכון:

- נסמן כל תחנה בנקודה.
- נשים קשת בין שתי תחנות אם אסור שהן תשדרנה באותו תדר (זה נועד לאכוף את התקנה שאומרת שאסור לפגוע בטווח הקליטה של תחנות שלא רוצות למכור – הצלע אומרת שאם שתי התחנות תשדרנה באותו התדר, אחת תפריע לשנייה להגיע למי שקלט אותה עד כה. נתעלם מכך שבמקרה האמיתי הרשו ירידה מסויימת במספר הקולטים).
- ננסה לדחוס ל- $N$  תדרים תוך שמירה על החוקים. נגדיר את המשתנים הבאים:

$$p_{**}$$

(\* מספר התדר בין  $1 - N$ , \*\* מספר התחנה)

אנחנו רוצים לכתוב נוסחא כך שיהיה לה מודל אמ"מ אפשר לספק אותה ב- $N$  תחנות.

לכל תחנה נגדיר כללים:

- היא צריכה לשדר באיזשהו תדר: כלומר לכל תחנה  $s$  נאמר  $(p1s|p2s| \dots |pNs)$
- שתי תחנות עם צלע לא יכולות לשדר באותו התדר: לכל שתי תחנות  $s, t$  שיש ביניהן קשת ולכל תדר  $c$ :  
 $(\sim pcs|\sim pct)$

במקרה הזה לא נדאג לציין שאין שום תחנה שאין לה שני תדרים, כי זה חלק ממה שאנחנו מנסים לעשות בבעיה, חלק מהמינימיזציה שאנחנו מנסים לעשות.

על סמך הכללים האלה נוכל לקבל נוסחא שיש לה מודל שמספק אותה אמ"מ אפשר את כל האילוצים האלה לדחוס ל- $N$  תדרים.



Figure 1: Interference graph visualizing the FCC's constraint data [9] (2990 stations; 2 575 466 channel-specific interference constraints).

Figure 1 המחשה של גרף האילוצים מהמכירה בארה"ב<sup>2</sup>

<sup>2</sup> לקוח מהמאמר <https://arxiv.org/pdf/1706.03304.pdf>

לאחר שעושים את זה עבור  $N$ , אפשר לבדוק עבור  $N - 1$  וכך הלאה עד שמגיעים למספר המינימלי האפשרי, וזה יהיה מספר התדרים המינימלי שאותם תאלץ הממשלה להשאיר פנויים לצורך תפעול התחנות שלא מסכימות למכור את התדרים שלהן.

המהירות שבה הצליחו לעשות את זה השפיעה על כמות האיטרציות שאפשר היה להפיק, ובסופו של דבר אפשרה את ההתמשכות של המכירה הפומבית.

## 3 שיעור 3 – 5.11.17

### 3.1 נוסחאות DNF ונוסחאות CNF

#### 3.1.1 הגדרה


בתרגיל 2 חלק 6 נתקלנו במשימה הבאה – רוצים לצור נוסחא שבטבלת האמת שלה יש שורה דולקת אחת (כלומר השמה אחת שנותנת ערך אמת), וכל השמה אחרת תתן שקר. לדוגמא, נניח שיש לנו את המודל:

$$p1 = T, p2 = T, p3 = F$$


הנוסחא המתאימה תהיה:

$$(p1 \& p2) \& \sim p3$$

לאחר מכן, במשימה 7, קיבלנו טבלת אמת, ורצינו לכתוב נוסחא כך שתתאים לטבלת האמת. עשינו את זה ע"י כך שעבור כל שורה שמקבלת אמת בטבלה המרנו אותה לנוסחא באמצעות מה שכתבנו במשימה 6, ואז עשינו איור בין כל הנוסחאות האלה, לקבלת נוסחא שמתאימה לטבלת האמת. הנוסחא הסופית שמקבלים נראית כמו *or* של *and* ים. לנוסחא מהצורה הזאת קוראים *DNF*:

**Disjunctive Normal Form – DNF**  ביטוי שמורכב מאוסף של איברים, כך שכל איבר מורכב מביטויי "וגם", והאיברים מקושרים ביניהם על ידי ביטויי "או".

צורה נוספת לכתוב נוסחא, שהיא דומה ל-*DNF* אבל אולי קצת פחות אינטואיטיבית, נקראת *CNF*:

**Conjunctive Normal Form – CNF**  ביטוי שמורכב מאוסף של איברים, כך שכל איבר מורכב מביטויי "או", והאיברים מקושרים ביניהם על ידי ביטויי "וגם".

זו צורת כתיבה שימושית במדעי המחשב. נתקלנו בה כבר בשבוע שעבר, בדוגמא של המפה – בשביל לפרמל את הבעיה, יצרנו הרבה נוסחאות שבכולן רצינו לעמוד, ואמרנו שאם נעמוד בכל התנאים (שקול ללעשות *and* לכל הנוסחאות) נקבל את הנוסחא שרצינו. דבר דומה עשינו גם בבעיית הספקטרום. גם הנוסחא של המפה וגם של הספקטרום היו נוסחאות מצורת *CNF*. מסתבר שהרבה בעיות במדעי המחשב אפשר לכתוב כסט של משוואות שרוצים לעמוד בהן, והדרך המתמטית להביע שרוצים לעמוד בכולן הוא לגמם ביניהן (ובנוסף, הרבה פעמים כל אחת מהמשוואות בפני עצמה נותנת *or* של דברים).

#### 3.1.2 המרה של טבלת אמת לנוסחא

כעת, נראה איך בהנתן טבלת אמת יוצרים נוסחת *CNF* שזו הטבלה שלה. בתרגיל 2 ראינו איך לקחת טבלה ולקבל ממנה נוסחא, והנוסחא שקיבלנו שם הייתה בצורה של *DNF*. כשעשינו זאת ראינו שהנוסחא שקיבלנו יכולה לקבל ערך *true* אם אחד האיברים שלה מקבל ערך *true*. הפעם, כשנרצה לצור נוסחת *CNF*, נראה שהנוסחא שנקבל יכולה לקבל ערך *true* רק אם כל האיברים שלה מקבלים ערך *true*, או באופן שקול – הנוסחא תיתן *false* אם אחד האיברים שלה הוא *false*.

נתאר אלגוריתם ראשון להפיכת טבלת אמת לנוסחת *CNF*:

צעד 1 – לכל שורה בטבלה שהערך שלה הוא *false*, נצור נוסחא שמקבלת ערך *true* בכל שאר השורות וערך *false* רק בשורה הזו (הערה: בדיוק להפך ממה שעשינו בשיעורי הבית, שם יצרנו נוסחא שמקבלת *false* בכל מקום חוץ מ-*true* במקום אחד).

צעד 2 – נעשה *and* לכל השורות הנ"ל.

נבין איך לעשות את הצעד הראשון של האלגוריתם – נסתכל על שורה בטבלה. אנחנו רוצים נוסחא שמקבלת ערך  $false$  רק על המודל הזה, וערך  $true$  לכל שאר המודלים. איך נעשה את זה? כאמור, בתרגיל 2 עשינו אותו הדבר רק ששם רצינו שמודל מסויים ייתן ערך  $true$  והשאר ייתנו ערך  $false$ . לכן, נוכל לעשות בדיוק מה שעשינו בתרגיל, ולקחת את השלילה של זה (כלומר לעשות לזה  $not$ ).

כעת, נעשה צעד נוסף, ונפעיל את חוק זה מורגן על הנוסחא שקיבלנו. החוק אומר ששלילה של איזוי בין ביטויים שקולה לגימורם בין שלילת הביטויים, כלומר:

$$\sim(a_1 \& a_2 \& \dots) = (\sim a_1 | \sim a_2 | \dots)$$

לדוגמא, עבור המודל:

$$p1 = true, p2 = true, p3 = false$$

לאחר שנעשה מה שעשינו בתרגיל הבית ואז נשלול נקבל:

$$\sim(p1 \& p2 \& \sim p3)$$

לבסוף, נפעיל את חוק זה מורגן, לקבלת:

$$(\sim p1 | \sim p2 | p3)$$

נוכל ישר לראות בדוגמא שלנו שהתוצאה מתאימה למה שרצינו, כי בשביל לקבל שקר צריך שכל הביטויים שיש ביניהם "או" יהיו שקר, והנוסחא שקיבלנו נותנת לנו מיד את ההפך מהערך של כל אחד מהמשתנים.

מה שעשינו עכשיו דואלי במובן מסויים למה שעשינו בבית. כל זה נותן לנו אלגוריתם לכתיבת נוסחא של טבלת אמת דרך מה שעשינו בשיעורי הבית, מבלי להזדקק לדברים נוספים:

**צעד 1 –** נמצא נוסחת  $DNF$  לשלילה של טבלת האמת הנתונה (כלומר, הופכים בעמודה האחרונה של הטבלה כל אמת לשקר וכל שקר לאמת, ומוציאים את נוסחת ה- $DNF$  כמו שעשינו בבית):

$$[(a_1^1 \& a_2^1 \& \dots) | (a_1^2 \& a_2^2 \& \dots) | \dots]$$

**צעד 2 –** שוללים את הנוסחא שקיבלנו:

$$\sim[(a_1^1 \& a_2^1 \& \dots) | (a_1^2 \& a_2^2 \& \dots) | \dots]$$

(נשים לב שברגע שעשינו זאת, הנוסחא מתאימה לטבלת האמת המקורית שלנו)

**צעד 3 –** לוקחים את נוסחת ה- $DNF$  שהתקבלה, ומפעילים עליה את חוק זה מורגן:

$$[(\sim a_1^1 | \sim a_2^1 | \dots) \& (\sim a_1^2 | \sim a_2^2 | \dots) \& \dots]$$

וזו כבר נוסחת  $CNF$ .

התהליך הזה הוא בדיוק כמו התהליך של האלגוריתם הראשון, כי אם לכל שורה שיש לה ערך  $false$  אנחנו מחפשים נוסחא שהיא  $false$  שם ו- $true$  בכל מקום אחר, זה בדיוק כמו לנסות למצוא עבור השלילה של השורה נוסחא שהיא  $true$  שם ו- $false$  בכל מקום אחר, ואז לשלול את התוצאה. שתי הדרכים למעשה שקולות.

### 3.1.3 ספיקות בנוסחאות DNF ו-CNF

נטען שבהנתן נוסחת  $DNF$  קל מאוד לראות אם היא סתירה או אם יש מודל שמקיים אותה.

**טענה –** נוסחת  $DNF$  היא ספיקה אם"מ אחד מאיבריה ספיק.

זו טענה הגיונית, כי בנוסחאות  $DNF$  יש איזוי של ביטויים, כלומר הערך של הנוסחא הסופית היא שקר רק אם כל אחד מהאיברים הוא שקר, לכן מספיק שאחד יהיה אמת בשביל שהכל יהיה אמת.

נותר להבין כיצד בודקים אם איבר בנוסחא הוא ספיק. איבר בודד יהיה לא ספיק רק אם הוא יכיל ערך ושליטתו (או כמובן יכיל קבוע שהערך שלו הוא שקר). כלומר, איך בודקים אם נוסחא היא ספיקה – עוברים על כל האיברים ב- $DNF$ , ובודקים עבור כל אחד מהם האם הוא מכיל משתנה ושליטתו. אם כן – הנוסחא כולה לא ספיקה, אם עברנו על הכל וכל האיברים בסדר – הנוסחא ספיקה.

באופן טבעי, נרצה כעת למצוא שיטה כדי לבדוק אם נוסחת  $CNF$  היא ספיקה. מסתבר שבדיקת ספיקות נוסחאות של  $CNF$  היא בעיה קשה. אולם, גם כאן נוכל לעשות משהו בקלות, והוא להגיד האם הנוסחא היא טאוטולוגיה.

👉 טענה – נוסחת  $CNF$  היא טאוטולוגיה אם"מ כל אחד מאיבריה הוא טאוטולוגיה.

זה הגיוני, כי יש לנו כאן גימום בין איברים, אז מספיק שאחד האיברים לא יהיה טאוטולוגיה כדי שכל הנוסחא כולה תוכל לקבל ערך שקר, ובעצמה לא תהיה טאוטולוגיה.

איך נבדוק זאת עבור כל איבר – באופן דומה למה שראינו קודם, איבר הוא טאוטולוגיה אם"מ הוא מכיל משתנה ושליטתו.

שוב, נשים לב שיש דואליות בין שני סוגי הנוסחאות.

הערה: קל לבדוק האם נוסחת  $DNF$  היא ספיקה, אז אפשר לחשוב שמתוך זה אפשר לקבל אלגוריתם פשוט כדי לבדוק אם נוסחא כלשהיא היא ספיקה – הופכים אותה ל- $DNF$  ואז בודקים. איך זה מסתדר עם כך שלבדוק ספיקות זה  $NP$ -קשה? התשובה היא שהבעיה עצמה של הפיכה ל- $DNF$  היא בעיה קשה.

### 3.2 אופרטורים נוספים

תרגיל 3 מדבר על קבוצות אופרטורים שלמות. בתרגיל 2 ראינו שכל טבלת אמת אפשר לקבל באמצעות האופרטורים  $and$ ,  $or$ ,  $not$ , ונשאל את עצמינו אילו סטים אחרים של אופרטורים אפשר לקחת כך שאפשר לייצר איתם כל טבלת אמת.

נציג ארבעה אופרטורים חדשים (ובהמשך יתווסף עוד אחד):

הסינטקס של האופרטורים –

סינטקס	$\bar{p}$	$\bar{p} \& q$	$p \leftrightarrow q$	$p \rightarrow q$
מוסכמת ציור בפיתון	$\neg$	$\neg \&$	$\leftrightarrow$	$\rightarrow$
שם	NOR	NAND	שקילות	גרירה

הסמנטיקה של האופרטורים –

$p$	$q$	$p \rightarrow q$	$p \leftrightarrow q$	$p \& q$	$p \neg q$
F	F	T	T	T	T
F	T	T	F	T	F
T	F	F	F	T	F
T	T	T	T	F	F

נרחיב כעת מעט על כל אופרטור.

**3.2.1 גרירה →**

$p \rightarrow q$  (כלומר  $p$  גורר  $q$ ) אם בכל מודל שבו  $p$  נכון אז גם  $q$  נכון.

האופרטור הזה הוא לפעמים לא אינטואיטיבי, זאת מכיוון שהמילה גורר היא מעט בעייתית, כי בשפה הדבורה היא מעידה על סיבתיות, ואופרטור הגרירה לא באמת מצביע על קשר של סיבתיות בין גורר ונגרר.

נשים לב שברור שאם  $p$  הוא אמת ו- $q$  שקר אז  $(p \rightarrow q) \sim$ , ואם  $p$  הוא אמת ו- $q$  הוא אמת אז  $p \rightarrow q$ , אבל נשאלת השאלה מה קורה כש- $p$  הוא שקר. הסוגייה הזאת היא עניין של הגדרה, וההגדרה היא שבמקרה כזה מתקיימת הגרירה, כלומר מתייחסים לזה כנכון באופן ריק. כלומר, אם  $p$  הוא שקר אז  $p \rightarrow q$  לא משנה מה ערכו של  $q$ . בהמשך (משפט הדדוקציה) נראה למה ההגדרה הזאת הגיונית.

**3.2.2 שקילות ↔**

קשר של אם ורק אם (אמ"מ), מה שנקרא באנגלית *if and only if* ( $iff$ ).  $p \leftrightarrow q$  מקבל אמת במודלים שבהם שניהם אותו הדבר.

הערה – אופרטור זה הוא השלילה של  $xor$  ("או" אקסלוסיבי).

**3.2.3 Nand &**

כשמו כן הוא –  $not$  של  $and$ . נאנד של  $p$  ו- $q$  אומר לעשות  $and$  לשניהם, ואז  $not$  לתוצאה.

**3.2.4 Nor |**

כשמו כן הוא –  $not$  של  $or$ . נור של  $p$  ו- $q$  אומר לעשות  $or$  לשניהם, ואז  $not$  לתוצאה.

**3.2.5 אופרטור ה-Multiplexer**

האופרטור הבא שלנו הוא אופרטור טרינארי (שלושה משתנים). נשים לב שהוא מכיל שני סימנים, אבל שני הסימנים מהווים לוגית אופרטור אחד.

האופרטור נקרא *Multiplexer*, או בקיצור *Mux*.

הוא אומר כך – אם  $p$  הוא אמת מחזירים את  $q$ , אם הוא שקר מחזירים את  $r$ .

מבחינת הסמנטיקה של האופרטור –

$p$	$q$	$r$	$(p? q: r)$
$F$	$F$	$F$	$F$
$F$	$F$	$T$	$T$
$F$	$T$	$F$	$F$
$F$	$T$	$T$	$T$
$T$	$F$	$F$	$F$
$T$	$F$	$T$	$T$
$T$	$T$	$F$	$F$
$T$	$T$	$T$	$T$

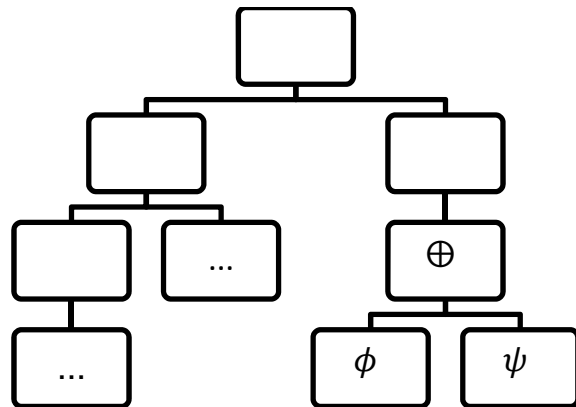
(הערה – הצבעים בטבלה נועדו רק לשם הדגשה. ההדגשה כאן היא על התפקיד של  $p$  בבורר בין  $q$  ל- $r$ )

עוד לא נתקלנו באופרטור שמקבל שלושה משתנים, אבל אין שום דבר מיוחד באופרטורים בינאריים ואונאריים, אפשר גם להגדיר אופרטור עבור כל מספר אחד של משתנים. למעשה, נתקלנו כבר בסוג נוסף של אופרטורים שהם לא בינאריים או אונאריים, אופרטורים שלא מקבלים משתנים – *True* ו-*False*.

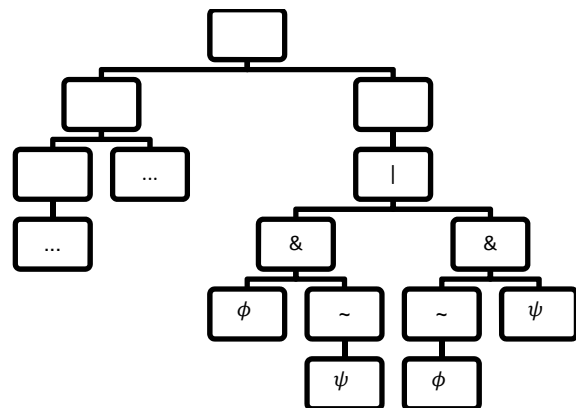
### 3.3 ניפוח אקספוננציאלי בהפיכת נוסחה ל-DNF

נניח שיש נוסחא עם הרבה אופרטורים מסוגים שונים. הנה דרך "בזבזנית" בחישוב להפוך אותה לנוסחא שקולה שמכילה רק  $and, not, or, T, F$  – מחשבים את טבלת האמת שלה, ואז קוראים לפונקציית סינטיסיז שכתבנו בתרגיל הקודם (זו שלוקחת טבלת אמת וממירה אותה לנוסחא, כבר דיברנו על זה כאן מבלי להזכיר את שם הפונקציה). הדרך הזאת תהיה אקספוננציאלית במספר המשתנים, מאוד לא יעילה, ויש דרכים הרבה יותר קלות להפוך נוסחא שיש בה הרבה אופרטורים לנוסחא שיש בה מעט אופרטורים.

כשנמיר נוסחאות לנוסחאות עם אופרטורים שקולים, נעבוד סביב אותה תובנה בסיסית, והיא שאפשר לעשות הכל באמצעות שינויים מקומיים. בשביל להדגים את העניין, נסתכל על עץ גדול שמסמל נוסחא, ובו במקום מסויים יש  $xor$  (שנסמן אותו ב- $\oplus$ ):



אנחנו רוצים לעשות שינוי שיוריד את ה- $xor$ , ולהחליף אותו באופרטורים מהסט  $and, or, not$ . אפשר היה לעשות את זה ע"י מחיקה של ה- $xor$ , והחלפתו באופן הבא:



ההחלפה נותנת את התוצאה הרצויה כי מבחינת טבלת האמת,  $p \oplus q$  שקול ל- $((p \& \sim q) | (\sim q \& p))$ .

הדוגמא הזאת ממחישה שאפשר לעשות את השינוי בצורה נקודתית בקדקוד ובסביבתו כדי להמיר את האופרטור.

הערה: למה שנרצה בכלל להחליף אופרטורים באחרים? סיבה אחת היא מתמטית: מעניין לדעת אם אפשר לצמצם את כמות האופרטורים שמשתמשים בהם, כלומר למצוא מה מינימום קבוצת האופרטורים שצריך לדעת לממש כדי להיות מסוגלים לממש כל פונקציה. סיבה נוספת היא ברמת הארכיטקטוריה: יתכן שנעדיף להגדיל את כמות השערים אם זה מצמצם את המגוון שלהם.

יש בעייתיות מסויימת במה שעשינו – כל  $\phi, \psi$  היה צריך לכתוב פעמיים. בתרגיל נראה שאפשר כמעט את כל השערים האלה להביע באמצעות השערים האחרים בלי שכפול כזה (חוץ מגרירה, שם אין ברירה לחזור).



הבעיה בהתנפחויות כאלה היא כזו – נניח שיש לנו את הנוסחה הבאה (כאמור,  $\oplus$  מסמל  $xor$ ):<sup>3</sup>

$$p_1 \oplus p_2 \oplus \dots \oplus p_n \quad (*)$$

אם נעשה מה שעשינו קודם נקבל עץ בגודל אקספוננציאלי ב- $n$ , כי אנחנו מכפילים עבור כל קדקוד את על העץ פי שניים.

נשאלת השאלה האם אפשר תמיד לעשות משהו אחר, כלומר האם יש שיטה יותר טובה שבה אפשר לעשות את זה, והיא תבטיח תמיד שנקבל משהו לא אקספוננציאלי. התשובה היא שלא – אי אפשר תמיד לכתוב את הנוסחה עם  $and, or, not$  כך שמובטח שלא תהיה אקספוננציאלית במספר המשתנים. לא נראה את ההוכחה הכללית, אבל כן ניתן לה אינטואיציה:

נתחיל מלציין שאפשר לבנות את הנוסחה בצורה אחרת גם ממה שעשינו בפונקציית סינטיסייז – נסתכל לדוגמא על  $((p_1 \& p_2) | (p_3 \& p_4))$ . אם היינו בונים אותה עם סינטיסייז היינו מקבלים משהו הרבה יותר גדול (בפרט, למשל, הביטוי  $(p_1 \& p_2)$  היה מוחלף בארבעה ביטויים, אחד עבור כל אחד מהערכים האפשריים של  $p_3$  ו- $p_4$ ). כלומר, זה שעשינו את זה ארוך בתרגיל הבית לא אומר שאין דרך לכתוב את זה בצורה יותר קצרה.

עם זאת, נראה כעת שזה לא המצב תמיד, זאת ע"י כך שנראה שנוסחת DNF שמייצגת את נוסחה (\*) צריכה מספר אקספוננציאלי של איברים.

טענה – בכל נוסחת DNF  $\phi$  ששקולה ל- $p_1 \oplus p_2 \oplus \dots \oplus p_n$  יש  $2^{n-1}$  איברים.

כלומר, במקרה של הנוסחה הספציפית הזאת שראינו שם, נוסחת ה-DNF היחידה שמייצגת אותה היא מה שהסינטיסייז שלנו היה מוציא אם הוא היה תומך בקסור – חייבים איבר לכל שורה, אין דרך להתחכם. הערה – בשקילות כאן אנחנו מתכוונים שיש להן אותה טבלת אמת.

הוכחה –

1. ראשית, נראה שבכל איבר ספיק (אנחנו לא מתעניינים באיברים לא ספיקים) יש  $n$  נוסחאות אטומיות:

יש לנו DNF ששקול ל-(\*), ואנחנו רוצים להראות שבכל אחד שבכל אחד מהאיברים שביניהם ביטוי "או" מופיעים כל המשתנים  $p_1, p_2, \dots, p_n$ :

a. נניח בשלילה שזה לא כך. אזי, קיים איבר שלא מופיע בו המשתנה  $p_i$  (עבור  $i$  אינדקס כלשהו של משתנה בין  $1 \leq i \leq n$ ).

b. יהי  $M$  מודל עבור הנוסחה, כך שהאיבר הזה מקבל אמת במודל  $M$ . נשים לב שבגלל ש-DNF בנויה כאיווי של איברים, משמעות הדבר היא ש- $M$  מספקת לא רק את האיבר הזה, אלא את נוסחת ה-DNF כולה. מכאן גם ש- $M$  מספקת את הנוסחה (\*), ששקולה ל-DNF שלנו.

c. ניצור  $M'$  ע"י כך שנקח את  $M$ , ונשאיר אותו בדיוק אותו הדבר, חוץ מהערך של  $p_i$  שאותו נהפוך (כלומר, אם היה בו אמת נציב בו שקר, ואם היה בו שקר נציב בו אמת).

d. נשים לב ש- $M'$  הוא עדיין מודל עבור האיבר שלנו, כי המשתנה  $p_i$  לא מופיע באיבר, ורק בו עשינו שינוי. מכאן גם ש- $M'$  הוא מודל עבור נוסחת ה-DNF שלנו כולה, ולכן גם עבור (\*).

e. כלומר, קיבלנו שגם  $M$  וגם  $M'$  מספקות את נוסחת ה-DNF שלנו, וזו סתירה – אם שתיהן מספקות את נוסחת ה-DNF שתיהן גם מספקות את (\*), וזה לא הגיוני. הסתירה היא בכך שהנוסחה (\*) היא  $xor$  של משתנים. לא יכול להיות שעשינו  $xor$  בין משתנים במודל מסויים וקיבלנו אמת, ואז שינינו ערך רק של משתנה אחד ועדיין קיבלנו אמת (זו פשוט תכונה של  $xor$  שנובעת מההגדרה).

f. הגענו לסתירה להנחת השלילה, לכן נסיק שבכל איבר בנוסחת ה-DNF יש  $n$  משתנים.

<sup>3</sup> פונקציה בוליאנית כזאת נראית "פונקציית זוגיות" (parity function)

2. נסיק מכך שיש  $2^{n-1}$  איברים:

אנחנו רוצים כעת להבין כמה איברים יש בנוסחת ה- $DNF$  השקולה ל- $(*)$  שלנו:

- a. באופן כללי, כל איבר בנוסחת  $DNF$  שמופיעים בו כל המשתנים מקבל ערך אמת עבור מודל אחד בלבד. במקרה שלנו, ראינו שבכל האיברים ב- $DNF$  שלנו מופיעים כל המשתנים, לכן עבור כל איבר ב- $DNF$  שלנו קיים מודל שמספק אותו (מודל שונה עבור כל איבר). מכאן, כדי לדעת כמה איברים יש צריך להבין כמה שורות ישנן בטבלת האמת של  $(*)$  שערכן אמת (כי כל שורה כזו תתאים לאיבר אחר ב- $DNF$ , ולכן מספר השורות הללו הוא מספר האיברים).
- b. בשביל לעשות את זה, נצטרך לקחת שוב בחשבון תכונה של  $xor$  – נשים לב ש- $xor$  בין הרבה משתנים מקבל ערך אמת רק במודלים שמספר המשתנים בהם שמקבלים אמת הוא אי-זוגי<sup>4</sup>. זאת אומרת שבדיוק חצי מהשורות בטבלת האמת של  $(*)$  נותנות אמת.
- c. יש לנו  $n$  משתנים, כלומר סה"כ  $2^n$  שורות בטבלת האמת של  $(*)$ . מספר האיברים ב- $DNF$  הוא כאמור חצי מזה, לכן יש לנו  $2^{n-1}$  איברים, וזה מה שרצינו להוכיח.

הוכחנו כאן שקיימת פונקציה בוליאנית באורך  $n$  שנוסחת ה- $DNF$  שלה כוללת  $2^{n-1}$  איברים, לכן בהכרח לא קיימת שיטה להמיר כל נוסחה ל- $DNF$  כך שיובטח שכמות האיברים לא תנופח אקספוננציאלית.

<sup>4</sup> בהמשך להערה הקודמת, זו הסיבה שהפונקציה הבוליאנית  $(*)$  קרויה פונקציית זוגיות – אם נמדל את ערכי האמת כ-1 ואת ערכי השקר כ-0, הפונקציה מעידה על הזוגיות של מספר האחדות בקלט: אם מספר האחדות אי-זוגי היא מחזירה 1 (אמת), אחרת היא מחזירה 0 (שקר). נעיר שזה אומר שהיא מחזירה את החיבור מודולו 2 של ספרות הקלט.

**4 שיעור 4 – 12.11.17****4.1 קבוצות קשרים שלמות ובלתי-שלמות**

בשיעור היום יהיו שני חלקים – חומר תיאורטי על קבוצות קשרים שלמות, ואז נעבור לגולת הכותרת של הקורס שהיא מושג ההוכחה.

קבוצת קשרים זה אוסף של פונקציות על  $k$  פרמטרים, שבאמצעותם אפשר לבטא פונקציות אחרות. קבוצת קשרים נקראית שלמה אם כל פונקציה שהיא ניתנת להבעה עם נוסחא שמורכבת רק מהקשרים האלה.

בתרגיל 2 ראינו ש- $\{and, or, not\}$  היא קבוצת קשרים שלמה. בתרגיל 3 הוכחנו שלמות של קבוצות נוספות באמצעות מה שכבר ידענו (למשל, כדי להביע כל נוסחא שהיא עם  $\{\rightarrow, F\}$  אפשר להביע את  $\{and, or, not\}$  באמצעות שני הקשרים האלה, ואז אנחנו כבר יודעים איך להביע את הכל – באותו האופן שבו הבענו אותם בתרגיל 2). אחד הדברים החשובים שראינו הוא ש- $\{nand\}$  היא שלמה.

יש גם קבוצות שהן לא קבוצות קשרים שלמות, לדוגמא –

1.  $not$  – ברור שהוא לא יכול להיות שלם, כי הוא אונארי, אין שום דרך שבה הוא יכול לפעול על שני דברים.
2.  $\{\rightarrow, T\}$  – אי אפשר לבטא את  $F$  באמצעותם. אפשר לראות אם זה אם מסתכלים על טבלת האמת של הקשר  $\rightarrow$ , ואז רואים שהדרך היחידה לקבל  $F$  זה ש- $T \rightarrow F$ .

טבלה לדוגמא עם כמה קבוצות שלמות ולא שלמות של קשרים:

לא שלם	שלם
$\{and, or\}$ $\{\rightarrow, T\}$ $\{xor, not\}$	$\{and, or, not\}$ $\{and, not\}$ $\{\rightarrow, F\}$ $\{\rightarrow, not\}$ $\{nand\}$

איך מראים שקבוצת קשרים היא לא שלמה? באופן כללי, נניח שאנחנו רוצים להוכיח שקבוצה  $A$  היא קבוצה לא שלמה של קשרים. דרך הפעולה שלנו תהיה לחפש תכונה  $X$  כך ש –

- למה 1: כל פונקציה שניתנת להבעה עם הקבוצה  $A$  מקיימת את התכונה  $X$ .
- למה 2: קיימת פונקציה שאיננה מקיימת את התכונה  $X$ .

ברגע שנוכיח את שתי הלמות האלה ינבע מכך ישירות שהקבוצה אינה שלמה, כי המסקנה תהיה שקיימת פונקציה שאי אפשר להביע באמצעות הקבוצה הזאת, ולכן הקבוצה אינה שלמה.

נסתכל עכשיו על כמה קבוצות, ונוכיח שהן אינן שלמות.

**משפט** – הקבוצה  $\{mux, or, and, T, \rightarrow\}$  אינה שלמה.

הלמות שאנחנו רוצים להוכיח –

- למה 1: כל נוסחא שמשתמשת בקבוצה הזאת נותנת ערך  $T$  כאשר כל הקלטים הם  $T$ .
- למה 2: קיימת פונקציה שנותנת ערך  $F$  כאשר כל הקלטים  $T$ .

הוכחה –

הוכחה של למה 2: לדוגמא, הפונקציות  $not$  (כשהקלט שלא הוא  $T$  היא מחזירה  $F$ ) ו- $F$  (שתמיד מחזירה  $F$ ).

רעיון ההוכחה של למה 1: הרעיון של ההוכחה מאוד פשוט – מכניסים  $T$  לכל אחד מהקשרים בקבוצה, ורואים שעבור כל אחד מהם בנפרד תמיד יוצא  $T$ , מה שאומר שמכל נוסחא שמורכבת רק מהקשרים האלה לא יכולה להתקבל תוצאה שונה מ- $T$ .

הוכחה פורמלית של למה 1: את ההוכחה הפורמלית נעשה באינדוקציה, כמו שאנחנו עושים תמיד בתרגילים כשאנחנו מתכנתים באופן רקורסיבי. האינדוקציה תהיה על מבנה הנוסחא:

- בסיס: בהתאם לאיך שהגדרנו את מבנה הנוסחא ולרשימת הקשרים שעומדים לרשותינו, נקבל שהבסיס יכול להיות אחד משני דברים: משתנה  $p_i$  או הקבוע  $T$ . הערך של  $p_i$  הוא בהכרח  $T$ , כי זה הקבוע היחיד שיש לנו. כלומר, בכל מקרה קיבלנו ערך  $T$  בבסיס, וזה מוכיח את בסיס האינדוקציה.
- צעד האינדוקציה: יש לנו קשר מהמשפחה, ויש לו שתיים (או שלוש) נוסחאות בתור בנים. לפי הנחת האינדוקציה, אנחנו יודעים שכל אחד מהנוסחאות בנפרד קיבלה ערך  $T$ . נעבור כל אחד מהקשרים בקבוצה, ונראה שאם הוא מקבל רק  $T$  כקלט הוא מחזיר רק  $T$ :

$$(T?T:T) = T \quad -$$

$$(T|T) = T \quad -$$

$$(T\&T) = T \quad -$$

$$(T \rightarrow T) = T \quad -$$

$$T = T \quad -$$

לכן, בהכרח קיבלנו שגם הערך של הנוסחא כולה היא  $T$ , וסיימנו.

נוכיח עכשיו משהו קצת יותר מעניין –

**משפט** – הקבוצה  $\{and, or, T, F\}$  אינה שלמה.

בתור עבודה מקדימה להוכחה, ננסה להבין מה אי-אפשר להביע באמצעות הנוסחא הזאת, והדבר הזה הוא  $not$ . לכן, בהתאם למה שראינו באופן כללי, ננסה לחפש תכונה  $X$  כך ש –

- למה 1: לכל פונקציה שניתנת להבעיה עם הקבוצה  $\{and, or, T, F\}$  יש תכונה  $X$
- למה 2: ל- $not$  אין את התכונה  $X$

בשביל למצוא את התכונה, נשים לב לעובדה הבאה – נתחיל מלמדל את הקבועים באמצעות מספרים:  $F = 0, T = 1$ . אם נסתכל על  $not$ , נראה שכשהקלט שלו גדל הפלט שלו קטן (אם הוא מקבל 0 הוא מחזיר 1, ואם הוא מקבל 1 הוא מחזיר 0, כלומר אם הכנסנו לו 0 ואז הגדלנו את הקלט ל-1 אז הפלט קטן). לעומת זאת, אם נגדיל את אחד הפרמטרים של הפונקציה  $or$  או את שניהם התשובה או תגדל או תשאר אותו הדבר, וכנ"ל ל- $and$ .

נרצה להגדיר בצורה מתמטית יותר מהי התכונה הזאת ש- $and$  ו- $or$  חולקים ולא קיימת עבור  $not$  –

**פונקציה מונוטונית** – פונקציה תקרא מונוטונית אם:

$$f(x_1, \dots, x_n) \geq f(y_1, \dots, y_n) \Leftarrow x_1, x_2, \dots, x_n \geq y_1, \dots, y_n$$

ובשביל שההגדרה הזאת תהיה מוגדרת היטב נצטרך להגדיר גם מהו יחס הסדר בין שני וקטורים, כפי שמופיע באגף ימין של הגרירה:

- הגדרה –  $x_1, x_2, \dots, x_n \geq y_1, \dots, y_n$  אם לכל  $i$  מתקיים  $x_i \geq y_i$ . (נזכור  $T = 1 > 0 = F$ )

תכונת המונוטוניות אומרת היא שאם הקלט עולה, הפלט לא יורד.

נחזור להוכחה שלנו –

- למה 1: כל פונ' שניתן להביע עם  $\{and, or, T, F\}$  היא מונוטונית.
- למה 2:  $not$  איננה מונוטונית.

הוכחה של למה 2: אם נותנים ל- $not$  0 היא מחזירה 1, ואם נותנים לה 1 היא מחזירה 0. כלומר, העלנו את הקלט והפלט ירד, לכן  $not$  איננה מונוטונית.

הוכחה של למה 1:

- בסיס: הבסיס הפעםיהיה הקבועים  $T, F$  ומשתנה  $p_i$ , וכל אחד מאלה מונוטונית, כי אם נעלה את הקלט הפלט שלהם לא ישתנה, כלומר בפרט הוא לא ירד.
- צעד האינדוקציה: נסתכל על  $and$  או  $or$  בנוסחא. לפי הנחת האינדוקציה, שני הקלטים שהקשר מקבל לא יכולים לרדת. מכיוון ש- $and, or$  מקיימים, כאמור, את תכונת המונוטוניות, הפלט שלהם יכול רק לגדול או להשאר אותו הדבר, ובכך סיימנו.

מסתבר (לא נוכיח) שאת כל הפונקציות המונוטוניות אפשר להביע באמצעות  $\{and, or, T, F\}$ .

נסתכל עכשיו על קבוצה נוספת:

**משפט** – הקבוצה  $\{F, T, Xor, \leftrightarrow, not\}$  אינה שלמה.

שתי התכונות שנעזרנו בהן עד כה בשביל ההוכחות לא מתקיימות כאן: הרבעייה הזאת לא בהכרח מונוטונית, וכן לא תמיד מחזירה  $T$ , אז נצטרך למצוא תכונה אחרת שמשותפת לכל הקשרים האלה ולא משותפת לקשר אחר.

מסתבר שהתכונה שמשותפת לכל הפונקציות היא תכונת זוגיות. יש כמה דרכים להגדיר את זה, אחת מהן היא לאמר שבאמצעות הפונקציות האלה אפשר להביע פונקציות אפיניות מעל שדה של שני איברים (פונקציה אפינית היא פונקציה ליניארית מוזחת בוקטור, כלומר פונ' מהצורה  $y = \sum_i A_i x_i + b$ ).

הקשרים שלנו הם פונקציות מהצורה  $\{0,1\} \rightarrow \{0,1\}^n$  ( $n$  הוא מספר הקלטים של הפונקציה הבוליאנית), וכל אחד מהם שלנו הוא פונקציה אפינית –

- $Xor$ : אפשר לראות אותו כחיבור מודולו 2 (עבור  $F = 0, T = 1$ , אם נקח הרבה משתנים בוליאניים ונעשה  $Xor$  ביניהם נקבל את תוצאת החיבור מודולו 2 שלהם), וזו פונקציה אפינית.
- $\leftrightarrow$ : אמ"מ נותן בדיקת ההפך של  $Xor$  – פחות החיבור מודולו 2, לכן ברור שגם הוא אפיני.
- $not$ : מקבלים ממנו 0 או 1, גם כן אפיני.
- $F, T$ : מחזירים תמיד ערך קבוע של 1 או 0 בהתאמה, גם אפיני.

נצטרך בשביל ההוכחה שגם לא כל הפונקציות בעולם תהיינה אפיניות, ואכן הפונקציה  $and$  לדוגמא היא לא כזאת.

אם רוצים לקחת בתור תכונה משותפת משהו יותר פשוט מההגדרה המתמטית הזאת, אפשר לקחת את התכונה הבאה של פונקציות אפיניות ולהשתמש בה במקום – בפונקציות אפיניות, כשמסתכלים על משתנה אחד מתוך הקלט הוא שייך בהכרח לאחד משני סוגים: משתנה שערכו אף פעם לא משפיע על התוצאה (כלומר התוצאה תלויה רק במשתני הקלט האחרים), ומשתנה שתמיד הופך את ערך האמת של הנוסחא (כלומר מחשבים את הערך רק תוך התחשבות במשתנים האחרים, וכשמסתכלים גם בו מקבלים תוצאה הפוכה ממה שיצא). נעיר שזו תכונה מיוחדת, כי אם היינו מגדילים נוסחא היינו מצפים שכל משתנה לפעמים ישפיע ולפעמים לא, וכאן יש התנהגות מיוחדת.

עד כה, עסקנו רק במה אפשר ואי אפשר לעשות, וכמעט לא דיברנו על כמה זה קשה לעשות את זה, ואיזה אורך מינימלי של נוסחא צריך כדי לעשות דברים. לא לכל קבוצות הקשרים השלמות יש אותו אורך מינימלי – לדוגמא, את פונקציית הזוגיות<sup>5</sup> אפשר לכתוב באורך לינארי עם  $xor$ , אבל היא תהיה יותר ארוכה עם  $and, not$ . זו שאלה מעניינת בסיבוכיות חישובית ואלגוריתמיקה, ומסבבת מתרחש שדברים שיש להם נוסחא באורך פולינומיאלי זה בדיוק הדברים שאפשר לחשב במקביל בצורה יעילה בזמן לוגריתמי. לא נרחיב על הנושאים האלה כאן, הם רלוונטים לקורס בסיבוכיות.

## 4.2 מושג ההוכחה

נתחיל כעת לדבר על אחד המושגים החשובים בקורס: ההוכחה. אנחנו רוצים להגיע למצב שבו נוכל לקחת אוסף של הנחות לוגיות, ועל בסיסו להסיק מסקנה. נרצה שהמסקנה שנוכל להסיק היא תהיה משהו טכני-סינטקטי: יהיה לנו אוסף של כללים טכניים (כללים שמחשב יוכל לבדוק), ובעזרתם נדע אם אפשר באמצעות ההוכחה להסיק את המסקנות או לא.

נדבר עתה על הפורמליזם של הוכחה, ונתחיל עם פורמליזם של כללי ההיסק –

### 4.2.1 כלל היסק

#### 4.2.1.1 הגדרה ודוגמאות

במתמטיקה, אנחנו רגילים שצעד של הוכחה הוא בצורה של "אם ... אז ..." (לדוגמא, אם פונקציה היא סכום של שתי פונקציות לינאריות, היא בעצמה לינארית). כלל ההיסק שנגדיר יהיה מהצורה הזאת – תהיה רשימה של הנחות (במתמטיקה יכולות להיות אינסוף הנחות, בפייתון זה יהיה אובייקט רשימה בגודל סופי), ואז מסקנה אחת (אפשר היה להגדיר יותר ממסקנה אחת, אצלינו בקורס זה תמיד יחיד):

**כלל היסק** – רשימה של נוסחאות שהן הנחות, ועוד נוסחא נוספת שהיא המסקנה שלהם. נסמן אותו באופן הבא:

רשימת הנחות  
מסקנה

ההנחות והמסקנות שלנו יהיו לוגיות.

נשים לב שאנחנו עולים רמה בתיאור שלנו – עד עכשיו דיברנו על פונקציה שנכנסים לה ערכים בוליאניים ויוצא ערך בוליאני. עכשיו אנחנו קופצים ברמת ההפשטה, והארגומנטים הם נוסחאות בעצמם. מבחינת התיאור התכנותי, לאובייקט החדש שהמצאנו יש שני שדות: שדה של רשימה של נוסחאות ושדה של עוד נוסחא נוספת. המשמעות שאנחנו רוצים לתת לאובייקט הזה היא שמתוך ההנחות ברשימה אפשר להסיק את המסקנה.

דוגמאות לכללי היסק –

דוגמא 1:

$$\frac{(p \& q)}{p}$$

ובמילים, אם גם  $p$  וגם  $q$  מתקיימים, אז אפשר להסיק את  $p$ . כלומר, אם  $(p \& q) = T$  אז  $p = T$ .

<sup>5</sup> להסברים נוספים על פונקציית הזוגיות ר' הערות 3,4 משיעור 3.

נשים לב לאבחנה בין נוסחא לכלל היסק:  $p \rightarrow (p \& q)$  זו נוסחא ולא כלל היסק. אפשר אפשר היה להפוך אותו לכלל היסק באופן הבא לדוגמא:  $\frac{\text{כלום}}{(p \& q) \rightarrow p}$ . זה דוגמא לכלל היסק שאין לו הנחות, וזה הגיוני שזה כך במקרה הזה כי מה שאנחנו מנסים להגיד כאן הוא טאוטולוגיה.

## דוגמא 2:

$$\frac{p}{\sim p}$$

זה אמנם כלל היסק לכל דבר ועניין לפי ההגדרה, אבל ברור לנו שמה שהוא אומר לא נכון. כמובן שאנחנו לא רוצים כללי היסק כאלה בהוכחות שלנו, אנחנו רוצים שבאמת המסקנה תוכל לנבוע מההנחות (נפרמל את זה בהמשך).

## דוגמא 3:

$$\frac{p, (p \rightarrow q)}{q}$$

כלומר, אם ראינו  $p$  בנוסחא וגם  $p \rightarrow q$  אז אפשר להסיק  $q$  (וסמנטית, אם קיום של  $p$  גורר את הקיום של  $q$  ו- $p$  מקיים, הרי ש- $q$  מתקיים). לכלל ההיסק הזה קוראים *modus ponens*, ועוד נדבר עליו בהמשך.

### 4.2.1.2 כלל היסק תקף

נגדיר עכשיו את ההגדרה הבאה:

**כלל היסק תקף** – כלל היסק נקרא "תקף" אם לכל השמה של ערכים למשתנים (שמופיעים איפשהו בהיסק) שמקיימת את כל ההנחות, גם מקיימת את המסקנות.

לכלל היסק תקף נקרא לפעמים גם "היסק טאוטולוגי". נעיר שבמילה "מקיימת" אנחנו מתכוונים לקבלת ערך אמת, כלומר השמה שמקיימת את כל ההנחות היא השמה שעבורה כל אחת מההנחות מחזירה ערך אמת, וכך באופן דומה עבור מסקנה.

### דוגמאות לתקפות של כללי היסק –

נראה ש- $\frac{p}{\sim p}$  אינו תקף: נמצא מודל שבו כל ההנחות מתקיימות, אבל המסקנה לא. במודל שבו  $p = T$  ההנחות מתקיימות אבל המסקנה לא, לכן הכלל אינו תקף.

נראה ש- $\frac{(p \& q)}{p}$  תקף: יש רק מודל אחד שעבורו ההנחה מתקיימת, והוא המודל  $p = T, q = T$ . המודל הזה גם מקיים את המסקנה, לכן הכלל תקף.

בתרגיל 4, הדבר הראשון שנעשה הוא לכתוב קוד שבהנתן היסק בודק אם הוא תקף או לא. אפשר לעשות את זה ע"י כך שעוברים על כל ערכי האמת של כל המשתנים (כלומר כל המודלים), ועבור לכל אחד מהם בודקים אם ההנחות מתקיימות:

- אם אחת מההנחות לא מתקיימת ממשיכים האלה.
- אם כולן מתקיימות, צריך לוודא שגם המסקנה מסתיימת.

חשוב לשים לב שהיסק טאוטולוגי זה מושג סמנטי, תלוי בנכונות של מודלים. אין דרך סינטקטית לדעת אם משהו תקף או לא, צריך לבדוק את כל ההשמות/מודלים האפשריים בשביל לגלות את זה.

**טענה** – אם יש קבוצה סופית של הנחות ורוצים לדעת הוא גורר את המסקנה, מספיק לבדוק האם הנוסחא: מסקנה  $\rightarrow$  (גימזם הטענות) היא טאוטולוגיה.

ברור למה הטענה הזאת נכונה: כשאנחנו עוברים מודל-מודל ובודקים עבור כל אחד האם ההנחות מתקיימות ואם כן אז האם גם המסקנה, אנחנו בעצם דורשים שכל ההנחות יתקיימו (קשר של "וגם"), ושכולן יובילו למסקנה (קשר של "גרירה").

### 4.2.1.3 כלל היסק מהבחינה הצורנית

שאלה: נניח שיש את כלל היסק  $\frac{(p \& q)}{p}$  ויש לנו באיזה מקום בנוסחא  $\frac{(x \& y)}{x}$ . האם שני הכללים אותו הדבר?

התשובה היא שכן – כלל היסק הוא משהו כללי, כל דבר שנשים במקום  $p$  יכול לתת לנו או אמת או שקר, בדיוק כמו ש- $p$  היה נותן, ולכן אם נשמור על הצורה נקבל כלל שהוא מקרה פרטי שלו.

באותו אופן, גם הביטוי  $\frac{(x \& (z|w))}{x}$  או  $\frac{(\sim z \& (z|w))}{\sim z}$  הם מקרים פרטיים למה שראינו. כלומר, אנחנו בעצם מתייחסים לכלל היסק בתור:

$$\frac{(\varphi_1 \& \varphi_2)}{\varphi_1}$$

כש- $\varphi_1, \varphi_2$  מתארים כל נוסחא.

לסיכום העניין, זה מקרה פרטי של  $\frac{(\varphi_1 \& \varphi_2)}{\varphi_1}$  (או אפשר להגיד באופן שקול ש- $\frac{(\varphi_1 \& \varphi_2)}{\varphi_1}$  מגדיר משפחה של פונ').

הלמה המעניינת היא שהמקרה הפרטי גורר את הכללי. מה שנצטרך לעשות בתרגיל 4 הוא לשאול האם בהנתן נוסחא כלשהי הנוסחא מקרה פרטי של נוסחא אחרת. איך נבדוק את זה – לא ניתן בדיוק את האלגוריתם, אבל ניתן התוויה כללית: אנחנו צריכים לעבור על הנוסחא הכללית, ובמקביל גם על הנוסחא שאנחנו חושדים שהיא מקרה פרטי. לנוסחא הכללית יש מבנה של עץ, וכל עוד אנחנו לא מגיעים לעלים של העץ, אנחנו חייבים למצוא את אותו המבנה גם במקרה הפרטי (לדוגמא, אם השורש של הנוסחא הכללית הוא  $and$  אז גם השורש של כל מקרה פרטי צריך להיות  $and$ ). ברגע שנגיע לעלים, אם הגענו לקבוע נדרוש שהוא יהיה אותו דבר גם במקרה הפרטי, אבל אם הגענו למשתנה יש מקום למשחק, בדומה למה שראינו בדוגמאות (לדוגמא, כמו שראינו שאפשר להחליף את המשתנה  $x$  ב- $\sim z$ ).

נשים לב שהשאלה האם משהו הוא מקרה פרטי של משהו אחר זו שאלה סינטקטית, אין כאן בדיקה של ערכי אמת. כשנטפל בכללי היסק, צריך להפריד בין מה שנכון (התקפות של כלל היסק) לבין שאלת הצורה (כלל היסק א' הוא מקרה פרטי של ב'). להמחשה,  $(\sim x \& \sim y)$  שקול ל- $\sim(x|y)$  מבחינת ערכי האמת שלו, מבחינת המשמעות, אבל הם לא מקרה פרטי אחד של השני, כי יש ביניהם שוני צורני.

### 4.2.2 הוכחה

לאחר שהבנו מהו כלל היסק, נעבור לשלב הבא: הוכחת למה או משפט ע"י שימוש בכללי היסק.

**משפט + הוכחה** – כולל את הרכיבים הבאים:

- הנחות
- מסקנה
- הוכחה

זאת בנוסף לרשימה של כללי היסק שמותר לנו להשתמש בהם בהוכחה.



את ההנחות והמסקנה אנחנו כבר מכירים, הן בדיוק כמו בכלל היסק. ההבדל בין משפט לכלל היסק הוא שמשפט אנחנו הולכים להוכיח.

איך נראית ההוכחה – אנחנו נשתמש במנגנון ההוכחות הרגיל ביותר: הוכחה תראה כמו אוסף של שורות, כאשר השורה האחרונה רצוי שתהיה המסקנה. לצורך זה, מבחינה תכנותית הגדרנו אובייקט של *deductive proof*, שהשדות שלו הם הנחות, מסקנות וכללי היסק שמותרים לשימוש בהוכחה, וההוכחה היא רשימה של שורות. נותר לתאר איך נראית שורה בהוכחה (שזו תהיה מבחינה תכנותית מחלקה פנימית של ההוכחה).

**הוכחה** – אוסף של שורות, שכל אחת מהן היא בצורה הבאה:

$\varphi$        $\varphi$   
 שורות קודמות כלל  
 (או הנחות) היסק

המשמעות הסמנטית שאנחנו מייחסים לכל שורה היא משמעות של נוסחא שנובעת מהשורות הקודמות, אז צריך להגיד מאילו שורות הנוסחא נובעת (או מאילו הנחות) ולמה.

דוגמא 1: כלל היסק 2 הוא  $\frac{(p \& q)}{p}$ , ושורה 7 בהוכחה היא  $(x \& y)$ . שורה 13 נגיד יכולה להראות מהצורה:  $x, 2, [7]$ . המשמעות – הנוסחא  $x$  נכונה, זאת על סמך היסק 2 ובהתחשב בשורה 7.

דוגמא 2: נניח שיש לנו את כללי ההיסק  $\frac{(p, q)}{(p \& q)}$ ,  $\frac{(p \& q)}{p}$ , והנחות  $p$  ו- $\sim p$ . משפט שנוכל לדוגמא להוכיח הוא  $(p \& \sim p)$ :

1:  $p$

2:  $\sim p$

3:  $(p \& \sim p), \frac{p, q}{p \& q}, [1, 2]$

נשים לב שזו הוכחה נכונה: מהנחות סותרות אפשר להוכיח כל דבר. זה אולי לא יהיה שימושי, כי אם ההנחות סותרות אי אפשר להשתמש בהוכחה הזאת לשום דבר, אבל כהוכחה היא הוכחה חוקית לחלוטין. בפרט, כלל ההיסק הוא כלל תקף, כי בכל פעם שהמסקנות מתקיימות גם המסקנה מתקיימת.

### 4.3 משפט הנאותות

נגדיר שתי הגדרות שקשורות לכללי היסק –

הגדרה א' – נסמן  $\varphi_1, \dots, \varphi_n \models \varphi$  אם כלל ההיסק  $\frac{\varphi_1, \dots, \varphi_n}{\varphi}$  תקף.

הגדרה ב' – נסמן  $\varphi_1, \dots, \varphi_n \vdash \varphi$  אם יש הוכחה (בהנחת כללי היסק נתונים) של  $\varphi$  מתוך  $\varphi_1, \dots, \varphi_n$ .

נשי לב שההגדרה הראשונה היא הגדרה של תקפות (סמנטיקה), בעוד השנייה היא הגדרה של יכחות, האם יש הוכחה (סינטקס).

**משפט הנאותות** – עבור אוסף של כללי היסק תקפים:

$$\varphi_1, \dots, \varphi_n \vdash \varphi \Rightarrow \varphi_1, \dots, \varphi_n \models \varphi$$

הסבר: נניח שיש לנו סט של כללי היסק, והצלחנו באמצעותם להוכיח את הנוסחא  $\varphi$ . המשפט אומר לנו שאם הוכחנו את הנוסחא, נוכל להסיק מכך שהיא גם נכונה – אם הצלחנו להוכיח משהו מתוך משפטים הוא מתקיים (אם ההנחות שלנו לא היו סותרות, כמובן).

בשביל להראות את זה, נעשה אינדוקציה על מבנה ההוכחה: הבסיס יהיה שורות שמסתמכות רק על הנחות. בצעד האינדוקציה יודעים שמה שאנחנו מסתמכים עליו תקף מהנחת האינדוקציה, ובגלל שהכלל תקף נקבל שגם השורה הזאת תקפה.

משפט הנאותות נותן לנו קשר ראשון, מפתיע, בין שני עולמות נפרדים לכאורה – העולם הסינטקטי (ההוכחה, שהיא מניפולציה של סטרינגים), לבין העולם הסמנטי (התקפות, שהיא שאלה אמיתית של נכונות). לפי המשפט, מהפעולות הסינטקסיות של ההוכחה אנחנו יכולים לקבל משמעות סמנטית, הנכונות של ההוכחה.

ההמשך יהיה בדיוק הצד השני של משפט הנאותות – משפט הנאותות מדבר על זה שכל דבר שאפשר להוכיח הוא נכון, בהמשך נדבר על זה שכל דבר שהוא נכון אפשר להוכיח אותו.

**5 שיעור 5 – 19.11.17****5.1 משפט הנאותות ומשפט הטאוטולוגיה**תזכורת – בהנתן נוסחאות  $\varphi, \varphi_1, \dots, \varphi_n$ :

א. נסמן:

$$\varphi_1, \dots, \varphi_n \models \varphi$$

אם כלל ההיסק  $\frac{\varphi_1, \dots, \varphi_n}{\varphi}$  הוא תקף (טאוטולוגי), כלומר אם מתקיים שבכל מודל שבו  $\varphi_1, \dots, \varphi_n$  הן כולן  $T$  אז גם  $\varphi$  הוא  $T$ . זו הגדרה סמנטית.

ב. נסמן:

$$\varphi_1, \dots, \varphi_n \vdash_{\mathcal{R}} \varphi$$

אם ניתן להוכיח את  $\varphi$  מתוך ההנחות  $\varphi_1, \dots, \varphi_n$  באמצעות כללי היסק מתוך הקבוצה  $\mathcal{R}$ , שהיא קבוצה של כללי היסק. זו הגדרה סינטקטית.

על פניו, שני הדברים מאוד שונים אחד מהשני – הסימון הראשון אומר שבדקנו כל מודל אפשרי וראינו מבחינה סמנטית שהכל מתקיים, הסימון השני אומר שאנחנו יודעים לכתוב משהו על נייר ולפיו אנחנו מכריעים שהכל מתקיים.

עם זאת, בסוף השיעור שעבר ראינו כבר קשר בכיוון אחד בין שני הדברים, והוא משפט הנאותות – אם אפשר להוכיח את  $\varphi$  מתוך  $\varphi_1, \dots, \varphi_n$  אז  $\varphi$  הוא גרירה טאוטולוגית של  $\varphi_1, \dots, \varphi_n$ . נעיר שצריך קצת להזהר כאן, כי לא אמרנו כלום על כללי היסק (הכללים מהקבוצה  $\mathcal{R}$ ) – אם משתמשים בכללי היסק לא תקפים, אפשר להוכיח כל מה שרוצים. לכן, נסייג ונוסיף –

**משפט הנאותות – אם  $\mathcal{R}$  קבוצה כלשהי של כללי היסק תקפים:**

$$\varphi_1, \dots, \varphi_n \vdash_{\mathcal{R}} \varphi \Rightarrow \varphi_1, \dots, \varphi_n \models \varphi$$

זו תוצאה מרשימה – אם לדוגמא רוצים להוכיח שמהו נכון בכל מרחב וקטורי, ברור שבשביל להוכיח את זה אי־אפשר לעבור על כל המרחבים הוקטוריים ולבדוק באופן פרטני עבור כל אחד ואחד שזה אכן מתקיים בו. מה שהמשפט אומר לנו זה שאם נמצא הוכחה לתכונה הזאת של מרחבים וקטוריים (וכמובן אם ההוכחה היא בצורה נכונה ועם גרירות תקפות) אז התכונה הזאת מתקיימת בכל המרחבים הוקטוריים. זה אומר שעל־ידי הוכחה אנחנו יכולים להיות בטוחים במסקנה באותה מידת וודאות כמו אם היינו בודקים אחד אחד את כל המרחבים הווקטוריים שקיימים.

תוצאה אולי אף יותר חזקה אפשר לראות מהכיוון השני של המשפט –

**משפט הטאוטולוגיה**

$$\varphi_1, \dots, \varphi_n \models \varphi \Rightarrow \varphi_1, \dots, \varphi_n \vdash_{\mathcal{R}} \varphi$$

(עבור  $\mathcal{R}$  קבוצה מסויימת של כללי היסק, שאותה נכיר בשבוע הבא)

כלומר, אם משהו הוא היסק טאוטולוגי אז אפשר להוכיח אותו. אם נחזור לדוגמא של מרחבים וקטוריים, זה אומר שלכל תכונה של מרחבים וקטוריים קיימת הוכחה (בפרט הוכחה סופית, כי לאובייקט "ההוכחה" לפי איך שהגדרנו אותו קיימת שורה אחרונה).

על הקבוצה  $\mathcal{R}$  נדבר בהמשך<sup>6</sup>, כעת נסתפק בלציין ש- $|\mathcal{R}| = 14$ . בשיעור הזה נדון על שלושה כללים מתוך הקבוצה הזאת, ונראה שכבר רק מתוך השלושה האלה אפשר להוכיח לא מעט דברים, בפרט משפט מרכזי שנוכיח בשיעורי הבית.

הערה – משפט השלמות הוא וריאנט של משפט הטאוטולוגיה, זה יתבהר כשנדון בזה שבוע הבא.

## 5.2 **Modus Ponens (MP)**

זה כלל ההיסק הראשון שנדבר עליו, והיסטוריונים של הלוגיקה טוענים שהוא הכי קדום, מהמאה השלישית לפני הספירה. אנחנו נסמן בקיצור  $MP$ , ו- $Modus Ponens$  בעצמו הוא קיצור של  $Mudos Ponendo Ponens$ , שמשמעותו "The way that affirms by affirming". השם העברי – כלל ניתוק הרישא.

הכלל אומר כך:

**Modus Ponens** – כלל ההיסק:  $\hookrightarrow$

$$\frac{p, p \rightarrow q}{q}$$

**דוגמא:** אם אנחנו יודעים שהיום יום ראשון, ואם אנחנו יודעים שלמחרת יום ראשון מגיע יום שני, אנחנו יודעים שמחר מגיע יום שני.

בתרגיל 5 נלמד על משפט הדדוקציה, שבמובן מסויים הוא ההפך של  $MP$  – משפט הדדוקציה אומר לנו באילו מקרים שבהם מ- $p$  אנחנו יודעים להסיק את  $q$  נובע ש- $(p \rightarrow q)$  (במילים אחרות, הוא אומר לנו מתוך כל המקרים שבהם אנחנו יכולים להסיק מ- $p$  את  $q$ , באילו מהם מתקיים גם  $(p \rightarrow q)$ ). לפני שנעבור לדבר על משפט הדדוקציה, נבין יותר טוב את  $MP$ , כלומר ננסה לרדת לעומק התכונה שמשפט הדדוקציה נותן את ההפך שלה.

$\hookrightarrow$  **אבחנה** – אם  $MP \in \mathcal{R}$  ואם:

$$\varphi_1, \dots, \varphi_n \vdash_{\mathcal{R}} (\psi \rightarrow \xi)$$

אז:

$$\varphi_1, \dots, \varphi_n, \psi \vdash_{\mathcal{R}} \xi$$

למה זה נכון – לפי ההנחה, קיימת הוכחה שאם  $\varphi_1, \dots, \varphi_n$  מתקיימים אז  $(\psi \rightarrow \xi)$  מתקיים. לכן, יש הוכחה מתוך אותם כללי היסק  $\mathcal{R}$  שאם  $\varphi_1, \dots, \varphi_n, \psi$  מתקיימים אז  $(\psi \rightarrow \xi)$  מתקיים (כי אפשר לקחת את ההוכחה הקודמת ופשוט להוסיף לה את ההנחה של  $\psi$ , ואז רק נותר לשנות בהתאם את האינדקסים של שורות הצידיקים). כעת, נקח את ההוכחה הזאת ונוסיף לה שורה נוספת באמצעות  $MP$ : בשורות הקודמות הייתה לנו הנחה  $\psi$  וגם  $(\psi \rightarrow \xi)$ , ואם נקח את שתיהן כהנחות ל- $MP$  נקבל את המסקנה  $\xi$ . קיבלנו בדיוק מה שרצינו להראות – הוכחה מאותם כללי היסק  $\mathcal{R}$  לכך שאם  $\varphi_1, \dots, \varphi_n, \psi$  מתקיימים אז גם  $\xi$  מתקיים.

(הערה – נשים לב שקודם דיברנו על  $\mathcal{R}$  בתור סט מסויים של ארבעה-עשר כללים, שאותם נפגוש בשבוע הבא. באבחנה שלנו, ה- $\mathcal{R}$  היא לא ה- $\mathcal{R}$  של השבוע הבא, אלא סתם  $\mathcal{R}$  כללי, סתם אוסף כלשהו של כללי היסק.)

<sup>6</sup> הערה – לאוסף של כללי היסק שמוכיחים באמצעותם דברים קוראים Theory (תורה).

משפט הדדוקציה – אם  $MP, I_1, I_2 \in \mathcal{R}$  וגם אף כלל היסק מתוך  $\mathcal{R}$  לא מכיל הנחות (חוץ מ- $MP$ ), ואם:

$$\varphi_1, \dots, \varphi_n, \psi \vdash_{\mathcal{R}} \xi$$

אז:

$$\varphi_1, \dots, \varphi_n \vdash_{\mathcal{R}} (\psi \rightarrow \xi)$$

משפט הדדוקציה אומר לנו משהו חדש, ומשלים לנו את התמונה שאומרת שהקשר אם-אז הלוגי (בהנתן ההנחות על כללי ההיסק שעליהן נפרט בהמשך) שקול לקשר שמגדיר קשר הגרירה.

הדרישה הנוספת שיש כאן היא שכל כלל היסק מהקבוצה  $\mathcal{R}$  למעט  $MP$  יכולול רק מסקנה, בלי הנחו. זה נראה במבט ראשון כמו דרישה די מוגזמת שעשויה להפוך את המשפט ללא שימושי, אבל בקרוב ניווכח שזה לא כך.

### 5.3 $I_1, I_2$ וקידוד כלל היסק באמצעות $MP$

נדבר כעת על שני כללי ההיסק הנוספים מהקבוצה  $\mathcal{R}$  שעליהם נדבר בשיעור הזה:

$I_1$  – כלל ההיסק:

$$(p \rightarrow (q \rightarrow p))$$

$I_2$  – כלל ההיסק:

$$((p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r)))$$

הסיבה שקוראים להם כך היא שהם שני כללי ההיסק היחידים שמכילים רק את  $Implies$  (עבור הקורס הזה, בספרות הם לא ימצאו בשם הזה).

לפני שנפרש את הכללים האלה, נדון קודם במדוע אנחנו לא מגבלים את עצמינו בכך שאנחנו אומרים שאף כלל היסק חוץ מ- $MP$  לא יכיל הנחות.

אבחנה – כל כלל היסק ניתן ל"קידוד" לכלל היסק בלי הנחות באמצעות  $MP$ .

ניסחנו את האבחנה באופן לא פורמלי, אז ניתן דוגמא כדי להסביר –

נקח את כלל ההיסק  $\frac{\varphi_1, \dots, \varphi_n}{\psi}$ . עכשיו נסתכל על כלל היסק נוסף, שלא כולל הנחות, ונטען שכל מה שאפשר היה להוכיח עם הראשון אפשר להוכיח השני בתוספת  $MP$ :

$$\frac{None}{(\varphi_1 \rightarrow (\varphi_2 \rightarrow \dots (\varphi_n \rightarrow \psi) \dots))}$$

למה כל מה שאפשר להוכיח עם הראשון אפשר להוכיח עם השני – נניח שאנחנו יודעים ש- $\varphi_1, \dots, \varphi_n$  נכונים. מכיוון שאנחנו יודעים ש- $\varphi_1$  נכון ואנחנו יודעים ש- $(\varphi_1 \rightarrow (\varphi_2 \rightarrow \dots (\varphi_n \rightarrow \psi) \dots))$  נכון, אפשר להפעיל את  $MP$  ו"להוריד את הרישא", כלומר  $\frac{\varphi_1, (\varphi_1 \rightarrow (\varphi_2 \rightarrow \dots (\varphi_n \rightarrow \psi) \dots))}{(\varphi_2 \rightarrow \dots (\varphi_n \rightarrow \psi) \dots)}$ , כלומר נשארונו עם  $(\varphi_2 \rightarrow \dots (\varphi_n \rightarrow \psi) \dots)$ . כעת, אנחנו יודעים ש- $\varphi_2$  נכון, אז אפשר לחזור על אותו תהליך, ונקבל  $(\varphi_3 \rightarrow \dots (\varphi_n \rightarrow \psi) \dots)$ . נמשיך הלאה, ואחרי  $n$  פעמים כאלה נשאר פשוט עם  $\psi$ . כך הראנו שאפשר להחליף את הכלל השני, ללא ההנחות, בכלל הראשון.

לסיכום, ראינו שכל כלל היסק עם הנחות אפשר לקודד לכלל היסק בלי הנחות. לכן, אנחנו יודעים עכשיו איך אפשר להשתמש בכלל כלל היסק במשפט הדדוקציה, ואנחנו רואים גם שבאמת התנאי על ההנחות של הכללים לא היה כל כך מחמיר.

נשים לב ששני הכללים  $I_1, I_2$  הם בעצם שני כללי היסק עם הנחות שקודדו כך שלא יהיו להם הנחות:

1. כלל ההיסק הראשון  $(p \rightarrow (q \rightarrow p))$  מקודד בתוכו את  $\frac{p}{q \rightarrow p}$
2. כלל ההיסק השני  $((p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r)))$  בעצם מקודד בתוכו:

$$\frac{\overbrace{(p \rightarrow (q \rightarrow r))}^{\varphi_1}, \overbrace{(p \rightarrow q)}^{\varphi_2}}{(p \rightarrow r)} \quad \psi$$

הסבר אינטואיטיבי לקידוד – עבור הכלל הראשון, ברור מבחינת אינטואיציה למה זה נכון. עבור הכלל השני, הכלל קודם כל אומר שאם  $(p \rightarrow (q \rightarrow r))$  מתקיים אז משהו מתקיים. המשהו הזה הוא  $((p \rightarrow q) \rightarrow (p \rightarrow r))$ , שגם אותו אפשר לפרק: אם  $(p \rightarrow q)$  מתקיים אז  $(p \rightarrow r)$  מתקיים. זאת אומרת שהכלל הזה אומר שאם  $(p \rightarrow (q \rightarrow r))$  מתקיים, ואם גם  $(p \rightarrow q)$  מתקיים אפשר להסיק את  $(p \rightarrow r)$ , וזה כבר נותן לנו את כלל ההיסק שכתוב למעלה.

נעיר שיכולנו את כלל ההיסק השני לפרק עוד, לקבלת  $\frac{(p \rightarrow (q \rightarrow r)), (p \rightarrow q), p}{r}$ . זו גם הסתכלות נכונה, הצגנו את זה כמו שהצגנו כי בשיעורי הבית נצטרך את ההצגה הראשונה.

## 5.4 הערה – שני סוגים של הוכחות

כשמתמטיקאי מדבר על הוכחת משפטים, הוא מתכוון שהוא מקבל רשימה של אקסיומות ומוכיח משפט. מה שאנחנו הולכים לעשות עכשיו לדבר על הוכחה כמו שלוגיקאים מתכוונים אליה – מוכיחים שאפשר להוכיח משהו.

הוכחה בלוגיקה נראית מצורה הזאת:

$$A \vdash B \text{ אז } X$$

הוכחה בלוגיקה מדברת על מה אפשר להוכיח. במקום להוכיח את  $B$ , אנחנו מוכיחים שאפשר להוכיח את  $B$ .

זה מעלה את השאלה איך יכולנו עד כה לכתוב הוכחה בלי שראינו שאפשר להוכיח. מה שצריך לעשות זה להפריד בין שני המובנים – כשאומרים שאפשר להוכיח את  $B$  זה במובן הסינטקטי הצר. על  $A \vdash B$  אפשר לחשוב בתור: יש אובייקט  $O$  מסוג  $DeductiveProof$  כך ש- $O.is\_valid()$ .

זה כלל המשחק. בקורסים שלנו, הוכחות מהסוג המתמטי (הוכחות שבהן ממש מוכיחים את  $B$  ולא רק מוכיחים שאפשר להוכיח אותו) יהיו הוכחות דרך קונסטרוקציה – נבנה תוכנית שהפלט שלה הוא האובייקט  $O$ , ועצם זה שהתוכנית רצה כמו שצריך הוא בבחינת הוכחה. צריך להוכיח שהתוכנית תמיד עובדת, כמובן, אבל עצם זה שהיא עובדת זה כבר מראה משהו, ואיפה שזה לא ברור שהיא עובדת נצטרך להוכיח כמו בקורס באלגוריתמים שהיא נכונה. כל הסיבה שאנחנו מדברים על סינטקס היא מכיוון שכל מה שאנחנו אומרים על מתמטיקה אפשר בסוף לכתוב בצורה הזאת של אובייקט.

לסיכום, כשאנחנו מדברים על הוכחות, צריך תמיד לזכור שעובדים בשתי רמות שונות – הוכחה של מתמטיקה רגילה, או משחק של אותיות בתוך האובייקט  $DeductiveProof$  (הוכחה לוגית). זה ההבדל בין הקורס הזה לבין הקורס הרגיל בלוגיקה – את ההוכחה המתמטית אנחנו מחליפים בד"כ בכתיבת תוכנית, ואז הוכחה זה רק הדבר הלוגי ותוכנית זה ההוכחה המתטית.

**5.5 המשימות בתרגיל 5**

נעבור לדבר כעת על המשימות השונות בתרגיל 5.

**5.5.1 משימה 3**

משימה 3 תהיה לכתוב פונ' בשם *inversemp*, שהקלט שלה הוא הוכחה + אחת ההנחות מתוך ההוכחה הזאת, והיא עושה בדיקת מה שמשפט הדדוקציה עושה – היא מקבלת את ההוכחה  $\xi \vdash_{\mathcal{R}} \psi$  ומוציאה  $\varphi_1, \dots, \varphi_n \vdash_{\mathcal{R}} (\psi \rightarrow \xi)$ .

בכך שנממש את הפונקציה הזאת ובכך שהיא עברה את כל הטסטים וראינו שהיא עומדת בכל מקרי הקצה, סימן שהוכחנו את משפט הדדוקציה, זאת במובן שיש לנו את כל הידע להוכיח בצורה מתמטית את משפט הדדוקציה על סמך מה שכתבנו בקוד.

**5.5.2 משימה 4**

במשימה 4 נתבקש להוכיח כלל ידוע ושימושי, שאומר:

סילוגיזם היפותטי (*hypothetical syllogism*) – כלל ההיסק: 

$$\frac{(p \rightarrow q), (q \rightarrow r)}{(p \rightarrow r)}$$

(מכונה גם "הטרנזיטיביות של הגרירה")

זה כלל היסק שהיה מעיק להוכיח אותו ישירות מ- $MP, I_1, I_2$ , וקל להוכיח אותו באמצעות משפט הדדוקציה.

הערת מימוש – בקוד, בשורה אחת לפני *def prove\_hypothetical\_syllogism* (כלומר שורה אחת לפני שורת ההגדרה של הפונקציה) נראה שכתוב @. זה דקורטור

יש *def prove\_hypothetical\_syllogism*, ובשורה לפניה נראה שכתוב @. זה דקורטור שדואג ל-Memoization<sup>7</sup>, כלומר דואג שהפונ' תזכור את התוצאה של חישוב כלשהו בפעם הראשונה שעושים אותו, ובפעם הבאה שמתבקשים לעשות את החישוב הזה היא תחזיר אותה בלי לחשב שוב. בתרגיל 6 אנחנו הולכים לקרוא לפונ' האת הרבה פעמים עם הוכחות שונות, ויהיה לנו חשוב לזמן הריצה של התרגיל שהיא לא תעשה כל פעם את החישוב מחדש.

**5.5.3 משימה 1**

במשימה 1 מתבקשים להוכיח מתוך  $MP, I_1, I_2$  את  $(p \rightarrow p)$ , טאוטולוגיה שאותה נצטרך במימוש של משימה 3. יש הדרכה בתרגיל איך לעשות את זה.

**5.5.4 משימה 2**

במשימה 2 אנחנו מראים ש:

- כיוון שאנחנו יודעים להוכיח את  $\xi \vdash_{\mathcal{R}} \psi$  מתוך  $\mathcal{R} = \{MP, I_1, I_2, (p \rightarrow p)\}$
- וכיוון שאנחנו יודעים להוכיח את  $(p \rightarrow p)$  מתוך  $\mathcal{R} = \{MP, I_1, I_2\}$

אז אפשר להוכיח את  $\xi \vdash_{\mathcal{R}} \psi$  מתוך  $\mathcal{R} = \{MP, I_1, I_2\}$

נסביר זאת עם דוגמא – נניח שאנחנו בשיעור באינפי, ואנחנו רוצים להוכיח ש- $x \cdot 0 = 0$ . נכתוב:

$$x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0 \Rightarrow x \cdot 0 = 0$$

<sup>7</sup> עוד על [דקורטורים בפיתוח](#) ועל [memoization](#) אפשר למצוא בקישורים.

עכשיו רוצים להוכיח ש- $-1 \cdot x = -x$ . נכתוב:

$$-1 \cdot x + x = x \cdot -1 + x \cdot 1 = x \cdot (-1 + 1) = x \cdot 0 = 0$$

הנכונות של הגרירה האחרונה שעשינו נובעת מההוכחה הראשונה.

כעת, נניח שבהתחלה היינו כותבים:

$$y \cdot 0 = y \cdot (0 + 0) = y \cdot 0 + y \cdot 0 \Rightarrow y \cdot 0 = 0$$

בשיעור אינפי עדיין היינו אומרים שאפשר להשתמש בכלל הזה בשביל ההוכחה השנייה, כי זה אותו הדבר. אצלינו בקורס זה לא עובד ככה – אמנם, אם יש לנו כלל היסק מסויים אפשר להסתמך מראש על אינסטנס שלו ולא על כלל ההיסק כמו שהוא כתוב, אבל אי אפשר לקחת את כל ההוכחה ולעשות מה שעשינו בהוכחה המתמטית כאן. אולם, היות שהוכחנו את הכלל הראשון רק על סמך דברים שמותר לנו להשתמש בהם גם בשני, מה שאנחנו יכולים לעשות זה בהוכחה השנייה להוכיח כל פעם מחדש את מה שאנחנו רוצים להגיד.

זה מה שאנחנו עושים במשימה 2 – כותבים מתודה *inline\_proof*, שמקבלת הוכחה וכלל היסק וכותבת את ההוכחה שוב באמצעות כלללי ההיסק חוץ מהכלל האחד.

משפט (למה למות עובדות) – אם:

$$\varphi_1, \dots, \varphi_n \vdash_{\mathcal{R} \cup \{S\}} \psi$$

ואם  $S$  ניתן להוכחה מסט כללי היסק נוסף  $Q$ , אז:

$$\varphi_1, \dots, \varphi_n \vdash_{\mathcal{R} \cup Q} \psi$$

כלומר, אם יש לנו  $\psi$  שאותה אנחנו יודעים להוכיח אותה מ- $\varphi_1, \dots, \varphi_n$  באמצעות מערכת כללי היסק  $\mathcal{R} + S$ , ובנוסף גם מתקיים שאפשר להוכיח את  $S$  באמצעות  $Q$ , אז אפשר להוכיח את  $\psi$  באמצעות  $\mathcal{R} \cup Q$ .

נשים לב שזה בדיוק מה שאנחנו עושים בתרגיל, שם זה עבור  $S = (p \rightarrow p)$  ו- $\mathcal{R} = Q = \{MP, I_1, I_2\}$ .

בשבוע הבא נדבר על משפט הטאוטולוגיה, שזו גולת הכותרת של החצי הראשון של הקורס.

## 5.6 הערות נוספות

### 5.6.1 מסקנה ממשפט הדדוקציה, וצידוק להגדרה של אופרטור הגרירה

אמרנו שמשפט הדדוקציה אומר שתחת תנאים מסויימים, אם אנחנו יודעים ש- $\varphi_1, \dots, \varphi_n, \psi \vdash_{\mathcal{R}} \xi$  אז אפשר להוכיח  $\varphi_1, \dots, \varphi_n \vdash_{\mathcal{R}} (\psi \rightarrow \xi)$ . אם יש לנו את  $MP$  בכללי ההסקה, ראינו שאנחנו יודעים שגם ההפך הוא נכון. שני אלה מובילים אותנו למסקנה הבאה –

מסקנה ממשפט הדדוקציה – אם  $MP, I_1, I_2 \in \mathcal{R}$  וגם אף כלל היסק מתוך  $\mathcal{R}$  חוץ מ- $MP$  לא מכיל הנחות,

$$\varphi_1, \dots, \varphi_n, \psi \vdash_{\mathcal{R}} \xi \text{ אמי"מ } \varphi_1, \dots, \varphi_n \vdash_{\mathcal{R}} (\psi \rightarrow \xi).$$

בהוכחה של המשפט הזה נוכל לראות למה הגדרנו את אופרטור הגרירה כך ש- $F$  גורר כל דבר – עשינו זאת כדי שהוא יהיה שקול לחלוטין לגרירה לוגית שאנחנו חושבים עליה, גרירה של  $X$  אז  $Y$ . זה מסביר את זה כי אם היינו מגדירים את  $\rightarrow$  בכל צורה אחרת לא היינו מצליחים לקבל את המשפט הזה עם קשר של אמי"מ (פשוט כשהיינו מנסים להגדיר את ההוכחה היינו רואים שמהו לא פועל).



## 5.6.2 על הוכחות בשלילה

משפט מעניין שרואים בתרגיל 2 הוא למה למות עובדות. נרצה עכשיו לקבל באותו מחיר למה הוכחה בשלילה עובדת.

כבר כשהתחלנו בלימודים המתמטיקה, ראינו הוכחות בשלילה, כלומר הוכחות מהצורה –

משפט: אם  $A$  אז  $B$ .

הוכחה: נניח בשלילה  $\sim B$  ... סתירה.

ולאחר כל התהליך הזה באו ואמרו לנו –

מסקנה: אם  $A$  אז  $B$ .

מה שבעצם מסתתר כאן זו הטענה שכל מה שעשינו גורר שקיימת הוכחה מהצורה: אם  $A$  אז  $B$ .

במילים אחרות –

אנחנו רוצים הוכחה שנראית כך:

$A$

...

מסקנה בסוף:  $B$

מה שהוכיחו לנו זו הוכחה שנראית כך:

$A$

$\sim B$

...

מסקנה בסוף:  $F$

מה אומר משפט הדדוקציה – שאם מתוך  $A$  ו- $\sim B$  אפשר להוכיח  $F$  (כלומר  $(A, \sim B \vdash_{\mathcal{R}} F)$ ), אז מתוך ההנחה  $A$  אפשר להוכיח  $\sim B \rightarrow F$  (כלומר  $(A \vdash_{\mathcal{R}} (\sim B \rightarrow F))$ ). מה שחסר זה להוכיח שאם  $A$  וגם  $\sim B \rightarrow F$  מתקיימים אז  $B$  מתקיים. ברגע שנעשה זאת, משפט הדדוקציה יאמר לנו שהוכחה בשלילה באמת עובדת, כי אם הצלחנו לעשות הוכחה בדרך של שלילה אז הייתה קיימת גם הוכחה ישירה, בלי שלילה. אנחנו מתחילים לראות שיש כאן משחק מעניין שנוגע לשיטת ההוכחה המתמטית בין סינטקס לבין משמעויות שנובעות ממנו.

**6 שיעור 6 – 26.11.17****6.1 תרגיל 6**

נתחיל מחזרה קצרה – כל מה שעשינו עד עכשיו, מתחילת הקורס, בא לשאול את השאלה מתי, למה ואיך אפשר באמצעות כתיבה של הוכחה על פיסת נייר להשתכנע בזה שמהו נכון מבחינת המשמעות שלו.

היה לנו את משפט הנאותות:

**משפט הנאותות** (גרסא ללא הנחות) – אם  $\mathcal{R}$  קבוצה כלשהי של כללי היסק תקפים, אם  $\varphi \vdash_{\mathcal{R}} \psi$  אז  $\varphi$  טאוטולוגיה.

(הערה – בשיעור שעבר ראינו את המשפט שאומר להוכיח את זה מתוך ההנחות, כאן זו פשוט גרסא של הוכחה בלי הנחות)

מה שמשפט הנאותות בעצם אומר הוא: אם הוכחנו את זה, אז זה נכון.

אמרנו גם שאנחנו כל הזמן מתקדמים לעבר משפט הטאוטולוגיה (שאותו נוכיח בתרגיל 6):

**משפט הטאוטולוגיה** – אם  $\varphi$  טאוטולוגיה אז  $\vdash_{\mathcal{R}} \varphi$ .

מה שחסר עכשיו זה להגיד מה סט כללי ההיסק שלנו, מהו ה- $\mathcal{R}$  שאנחנו מרשים להשתמש בו בהוכחות. לא כל סט של כללי היסק נותן משמעות מעניינת למשפט: לדוגמא, אם בתור  $\mathcal{R}$  היינו לוקחת את קבוצת כל כללי ההיסק הטאוטולוגיים אז לא הייתה בעיה להוכיח כל טאוטולוגיה  $\varphi$  שהיא, כי היינו פשוט לוקחים את כלל ההיסק  $\varphi \Rightarrow []$  (שאנחנו יודעים שהוא חלק מכללי ההיסק שלנו לפי זה שקבוצת כללי ההיסק שלנו כוללת את כל כללי ההיסק הטאוטולוגיים). בשביל שבאמת יהיה עניין במשפט, אנחנו רוצים להראות שאם נוסחא היא טאוטולוגיה אז אפשר להוכיח אותה מתוך סט קטן של כללי היסק. ככה אנחנו גם נשארים נאמנים למהות של הוכחה – אנחנו מכירים הוכחות בתור משהו שקל לבדוק שהוא נכון, אם נקח את סט כללי ההיסק להיות מאוד גדול אז רק להסתכל על שורה כלשהי בהוכחה ולשאול אם זה כן או לא כלל היסק תקין זה ארוך מאוד, ופוגם במהות ההוכחה. לכן, בתרגיל אנחנו מגדירים אוסף כללי היסק שנקרא לו  $\Delta$ , והוא אוסף של 14 כללי היסק מסויימים. אוסף כללי היסק הזה הוא  $\mathcal{R}$  ממשפט הטאוטולוגיה, ומכאן שהמשפט אומר לנו שאם אפשר להוכיח מסקנה כלשהי מתוך הנחות מסויימות בעזרת אוסף של כללי היסק תקפים, אפשר להוכיח את המסקנה הזאת מתוך ההנחות האלה באמצעות כללי ההיסק של  $\Delta$ .

משפט הטאוטולוגיה אומר לנו שאם נוסחא היא תמיד נכונה, כלומר אם נוסחא היא טאוטולוגיה, לא משנה כמה משתנים יש בה ועד כמה מסובכת, תמיד תהיה הוכחה עבורה שמשמשת לכל היותר ב-14 כללי היסק. גם אם כרגע, בהסתכלות שיש לנו דרך המודל של תחשיב הפסוקים, זה לא נראה מאוד מרגש, במודל של תחשיב הפרקדיקטים (אותו נפגוש בסמסטר השני) העומק של זה יהיה יותר ברור, כי המודל הזה יותר מכליל ומדבר על כל המתמטיקה (ואז זה אומר, לדוגמא, שכל תכונה שמאפיינת שדות וקטוריים – אפשר להוכיח אותה).

**6.1.1 סקירה כללית של התרגיל**

**משימות 1-3** – אנחנו פותחים את התרגיל במשימות 1-3 עם הוכחת משפט הטאוטולוגיה עבור נוסחאות שמכילות רק את קשרי הגרירה ( $\rightarrow$ ) והשלילה ( $\sim$ ), בלי אף קשר אחר ובלי קבועים ( $T, F$ ). המשמעות של ההוכחה בתצורה הזאת היא שלכל נוסחא  $\varphi$  שמכילה רק את קשרי הגרירה, קשר השלילה ומשתנים, אם היא טאוטולוגיה אפשר להוכיח אותה באמצעות כללי ההיסק שניתנים במשימות 1-3 (שזה לא כל ה-14, רק חלק מהם). הסיבה לכך שמוכיחים קודם את המשפט רק עבור סט מצומצם יותר של קשרים היא כדאי להבין את הרעיון שלה יותר טוב לפני שעוברים הלאה להוכחה עבור כל הקשרים, כלומר המשימות האלה משמשות כהדרכה לקראת ההוכחה המלאה.

עם זאת, עדיין נשאלת השאלה מדוע זה מעניין להתמקד רק בשני הקשרים האלה. את התשובה כבר ראינו בעבר, והיא שהקשרים האלה מהווים סט שלם – לא משנה איזה קשרים יש בנוסחא כלשהי, אפשר להגיע ממנה לנוסחא שקולה

מבחינת טבלת האמת שלה שכוללת רק את שניהם (או במילים אחרות, שני הקשרים האלה מספיקים בשביל לעשות סינטיסייז לכל טבלת אמת). לכן, קורסים רבים בלוגיקה מצטמצמים כבר מתחילת הקורס לטיפול רק בשני הקשרים האלה, ובכל פעם שהם מדברים על הסימן  $(a|b)$  לדוגמא, המשמעות שלו בעיניהם היא  $(\sim a \rightarrow b)$ .

**משימות 4-5** – במשימות האלה כבר נוכיח ממש משפט הטאוטולוגיה, כלומר נוסיף את הקשרים *and*, *or* ואת הקבועים  $T, F$  (זו תהיה ממש הוספה במובן שכל הקוד שכתבנו בשלוש המשימות הראשונות ישמש אותנו גם כאן). נשאלת השאלה למה בכלל להרחיב את ההוכחה של המשפט לקשרים נוספים אם אפשר באמצעות גרירה ושלילה להביע את כל שאר הקשרים, והתשובה שניתן כאן היא שזה חשוב בגלל איך שהגדרנו הוכחה. מבחינה גיונית אפשר להביע כל נוסחא רק עם גרירה ושלילה, אבל מבחינה טכנית, לפי מה שהגדרנו אין שום דרך לכתוב אובייקט של הוכחה או כלל היסק עם החלפות של אופרטורים. אפשר היה להגדיר את כללי ההיסק בצורה יותר מתוחכמת, אבל זה לא מה שעשינו, ולכן נעדיף להמשיך עם איך שהגדרנו הוכחה.

**משימות 6-7** – נדבר בהמשך.

### 6.1.2 משימות 1-3

נדבר עכשיו על האקסיומות המותרות לשימוש במשימות 1-3. זה סט של שבע אקסיומות, שהן:

שם	האקסיומה
$MP$	$\frac{p, p \rightarrow q}{q}$
$I_1$	$(p \rightarrow (q \rightarrow p))$
$I_2$	$((p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r)))$
$I_3$	$(\sim p \rightarrow (p \rightarrow q))$
$NI$	$(p \rightarrow (\sim q \rightarrow \sim(p \rightarrow q)))$
$NN$	$(p \rightarrow \sim \sim p)$
$R$	$((q \rightarrow p) \rightarrow ((\sim q \rightarrow p) \rightarrow p))$

נזכיר שכל כלל היסק ללא הנחות שכזה בעצם מקודד בתוכו כלל היסק עם הנחות, לדוגמא  $I_3$  מקודד את:

$$\frac{\sim p}{(p \rightarrow q)}$$

ו- $NI$  מקודד את:

$$\frac{p, \sim q}{\sim(p \rightarrow q)}$$

נדבר קצת על האופרטורים בטבלה –

את  $MP, I_1, I_2$  כבר הכרנו בשיעור הקודם (הערה: השימוש היחיד ב- $I_2$  בתרגיל הוא שהוא יאפשר לנו להפעיל את משפט הדדוקציה. בשום הוכחה שנכתוב בתרגיל לא נשתמש ישירות ב- $I_2$ , אבל כן נשתמש ב-*inverse\_mp*, שמשמשת בו).

נשים לב ש- $NI, I_3, I_1$  תופסים ביחד את כל טבלת האמת של אופרטור הגרירה – ב- $I_3$  אפשר לראות ששקר גורר כל דבר (ככה הגדרנו את האופרטור), ב- $NI$  אפשר לראות שאמת לא יכול לגרור שקר וב- $I_1$  אפשר לראות שכל דבר יכול לגרור אמת.

האופרטור  $NN$  מספר על אופרטור השלילה, שאם מפעילים אותו פעמיים ברצף על נוסחא מקבלים את אותו הערך המקורי שלה.

האופרטור  $R$  אומר שאם גם משתנה וגם שלילתו גוררים משהו, המשהו הזה הוא נכון (כלומר אם  $q$  וגם  $\sim q$  גוררים את  $p$  אז  $p$  אמת). זה נכון כי או שמשתנה הוא אמת או שהשלילה שלו היא אמת (או ש- $q$  אמת או ש- $\sim q$  הוא אמת), לכן אחת הגרירות הנתונות היא אמת גוררת משהו, וראינו שאמת לא יכולה לגרור שקר.

### 6.1.3 משימה 1

משימה 3 תהיה, בגדול: בהנתן טאוטולוגיה  $\varphi$  שמשתמשת רק ב- $\sim, \rightarrow$ , הוכח את  $\varphi$  באמצעות רשימת כללי ההיסק המותרים.

במשימה 1 אנחנו מתחילים עם יעד צנוע יותר – בהנתן נוסחא  $\varphi$  שמשתמשת רק ב- $\sim, \rightarrow$  ונכונה במודל  $M$ , להוכיח ש- $\varphi$  "נכון" במודל  $M$ .

צריך להסביר למה אנחנו מתכוונים כשאנחנו אומרים בלהוכיח שנוסחא נכונה במודל. נסביר דרך דוגמא: נקח את הנוסחא  $\varphi = \sim(p \rightarrow q)$  ואת המודל  $M = \{p: \text{True}, q: \text{False}\}$ . להוכיח שהנוסחא נכונה במודל זה אומר להוכיח את כלל ההיסק:

$$\frac{p, \sim q}{\sim(p \rightarrow q)}$$

כלומר, כל משתנה שהוא  $T$  במודל  $M$  לוקחים כהנחה וכל משתנה שהוא  $F$  במודל  $M$  לוקחים את השלילה שלו כהנחה, והמסקנה היא הנוסחא.

ההוכחה של נוסחא עבור מודל מסויים תהיה השלב הראשון לכיוון משפט הטאוטולוגיה.

בשביל לפתור את משימה 1, נעבוד ברקורסיה. נסתכל על המקרים השונים של צורה של נוסחא שמורכבת רק מגרירה ושלילה, ונראה איך אפשר לבנות את ההוכחה עבור כל אחת מהן –

#### מקרה 1 – נוסחאות מהצורה:

$$\varphi = (\varphi_1 \rightarrow \varphi_2)$$

$\varphi_{1,2}$  הן נוסחאות (זה לא דווקא משתנה יחיד, זה יכול להיות נוסחא מסובכת). אנחנו יודעים ש- $\varphi$  נכון במודל  $M$ , כלומר מתקיים בדיוק אחד משני הדברים הבאים:

(\*)  $\varphi_1$  לא נכון ב- $M$  או

(\*\*)  $\varphi_2$  נכון ב- $M$

במקרה (\*\*)  $\varphi_2$  נכון ב- $M$ , לכן אפשר להוכיח (עם קריאה רקורסיבית) את  $\varphi_2$  מתוך ההנחות שמתאימות ל- $M$ . לאחר שנוכיח את זה, נרצה להוכיח מתוך זה ש- $(\varphi_1 \rightarrow \varphi_2)$ , ובשביל זה נוכל להפעיל את  $I_1$  (או ליתר דיוק את כלל ההיסק שמקודד ע"י  $I_1$  ונצטרך לעשות  $MP$  כדי להגיע אליו) ונקבל את מה שרצינו להוכיח.

במקרה של (\*) אנחנו יודעים ש- $\varphi_1$  לא נכון ב- $M$ , אז נוכיח (ברקורסיה) את  $\sim \varphi_1$ . ברגע שיש לנו את ההוכחה הזאת נרצה להוכיח באמצעותה ש- $(\varphi_1 \rightarrow \varphi_2)$ , ואת זה בדיוק נותן לנו  $I_3$ .

בכך סיימנו לטפל במקרה של  $\varphi = (\varphi_1 \rightarrow \varphi_2)$ .

#### מקרה 2 – נוסחאות מהצורה:

$$\varphi = \sim(\varphi_1 \rightarrow \varphi_2)$$

אנחנו יודעים ש- $\varphi$  נכון במודל  $M$ , ולכן בהכרח  $\varphi_1$  נכון ב- $M$  ו- $\varphi_2$  לא נכון ב- $M$  (זה המצב היחיד שבו  $(\varphi_1 \rightarrow \varphi_2)$  יהיה שקר).

לכן, נוכיח רקורסיבית את  $\varphi_1$  ואת  $\sim\varphi_2$ . עכשיו אנחנו יודעים ש- $\varphi_1$  ו- $\sim\varphi_2$ , ואנחנו רוצים להוכיח מזה ש- $\sim(\varphi_1 \rightarrow \varphi_2)$ . את זה בדיוק נותן לנו  $NI$ .

**מקרה 3 –** נוסחאות מהצורה:

$$\varphi = \sim\sim\psi$$

אנחנו יודעים ש- $\varphi$  נכון ב- $M$ , אז בהכרח מתקיים ש- $\psi$  נכון ב- $M$ , ואז נסיק את  $\varphi$  באמצעות  $\psi$  עם  $NN$ .

**מקרה 0 –** יש עוד מקרה שהוא יחסית טריוויאלי, והוא שהנוסחא היא משתנה או שלילתו. במקרה כזה, נחזיר הוכחה שהשורה האחרונה שלה היא ההנחה שנוגעת למשתנה הזאת.

### הערות –

- נשים לב שבתרגיל 1 ייתנו לנו להוכיח נוסחא במודל מסויים רק אם היא נכונה בו.
- המקרים שראינו עכשיו מכסים את כל המקרים האפשריים, כי השורש של הנוסחא  $\varphi$  או שהוא סימן גרירה (בזה טיפלנו במקרה 1), או שהוא משתנה (מקרה 0) או שהוא סימן שלילה. אם הוא שלילה, יש שלוש אפשרויות לשורש של הבן שלו – או משתנה (מקרה 0), או גרירה (מקרה 2) שלילה כפולה (מקרה 3).
- איך נדע שמתישו נגיע למקרה הבסיס ברקורסיה – אפשר להראות את זה בכמה דרכים, לדוגמא לחשוב על הייצוג ה-*infix* של הנוסחא  $\varphi$ , ואז ברור שבכל פעם שאנחנו מפעילים את הרקורסיה יש פחות אותיות בייצוג, כלומר בסוף בטוח נגיע לבסיס.
- מה שקורה כאן זה שלקחנו משהו סמנטי (נכונות של נוסחא במודל) והפלט שלנו הוא משהו סינטקטי (הוכחה). זו הפעם הראשונה של הפיכה של משהו שנכון במודל להוכחה. זה קשה להבנה מבחינה תפיסתית, יש כאן תחבום מחשבתי. אחד הייתרונות של לתכנת את זה ולהסתכל על הכל כאובייקטים הוא שהתכנות גורם לנו לראות את זה בצורה קצת יותר מוחשית.

### 6.1.4 משימה 2

במשימה הזו, בהנתן שתי הוכחות שהראשונה מהן היא מהצורה:

$$\varphi_1, \dots, \varphi_{n-1}, \varphi_n \vdash_{\mathcal{R}} \psi$$

והשנייה היא מהצורה:

$$\varphi_1, \dots, \varphi_{n-1}, \sim\varphi_n \vdash_{\mathcal{R}} \psi$$

לייצר הוכחה ל-

$$\varphi_1, \dots, \varphi_{n-1} \vdash_{\mathcal{R}} \psi$$

או במילים – יש לנו שתי הוכחות של אותה נוסחא, שההנחות שלהן זהות מלבד כך שההנחה האחרונה של אחת מהן כוללת נוסחא, והשנייה כוללת את שלילתה, ואנחנו צריכים לייצר הוכחה לנוסחא ללא ההנחה האחרונה הזו.

למה זה טוב – כי אפשר להעזר בזה במשימה 3.

בשביל לבצע את משימה 2, נשתמש במשפטה הדדוקציה ובכלל ההיסק  $R$ . איך עושים את זה:

א. באמצעות  $inverse\_mp$ , נהפוך את:

$$\varphi_1, \dots, \varphi_{n-1}, \varphi_n \vdash_{\mathcal{R}} \psi$$

ל:

$$\varphi_1, \dots, \varphi_{n-1} \vdash_{\mathcal{R}} (\varphi_n \rightarrow \psi)$$

ב. באמצעות  $inverse\_mp$ , נהפוך את:

$$\varphi_1, \dots, \varphi_{n-1}, \sim \varphi_n \vdash_{\mathcal{R}} \psi$$

ל:

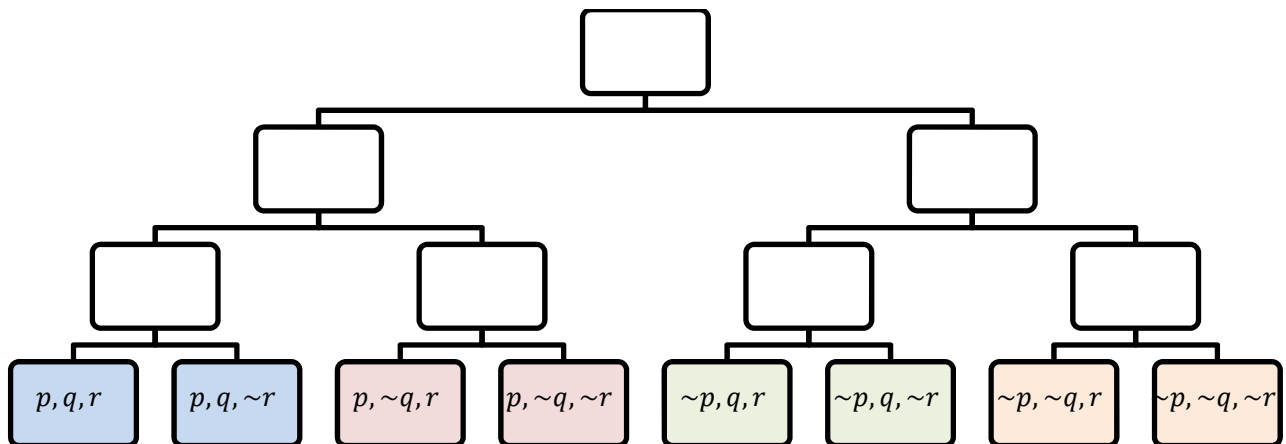
$$\varphi_1, \dots, \varphi_{n-1} \vdash_{\mathcal{R}} (\sim \varphi_n \rightarrow \psi)$$

ג. נפעיל את כלל ההיסק  $R$ , ונקבל את מה שרצינו להוכיח.**6.1.5 משימה 3**

במשימה 3 אנחנו מקבלים נוסחא, וצריך להוכיח אותה אם היא נכונה ולתת דוגמא של מודל שבו היא לא מתקיימת אם היא לא נכונה.

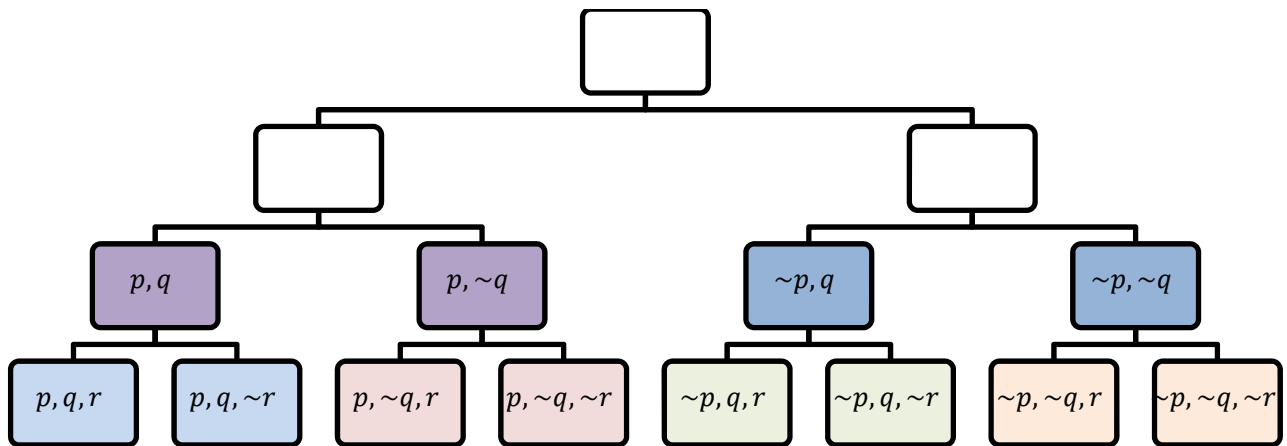
נעשה זאת כך – נתחיל מלבדוק שההוכחה נכונה בכל המודלים. אם מצאנו מודל שבו היא לא נכונה, נחזיר אותו. אחרת, נוכיח אותה בכל המודלים באמצעות מה שבנינו במשימה 1. בשלב הבא, נקח צמדים של הוכחות של הנוסחא במודלים שנבדלים אחד מהשני רק בהנחה האחרונה, ונאחד כל צמד כזה להוכחה באמצעות מה שבנינו במשימה 2. בשביל להבהיר מה הכוונה, ניתן דוגמא ספציפית –

נקח מודל שבו שלושה משתנים:  $p, q, r$ . נכתוב בשורש של העץ את כל המודלים האפשריים על שלושה משתנים:

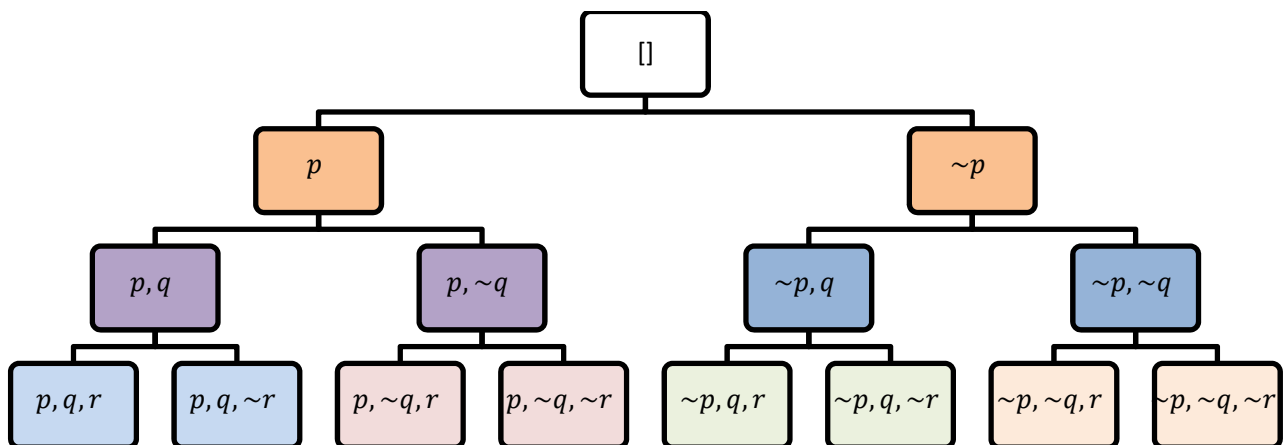


אנחנו רוצים להוכיח על נוסחא  $\varphi$  שמכילה את שלושת המשתנים האלה שהיא טאוטולוגיה.

מה שנעשה – בכל קדקוד נדמיין שיושבת ההוכחה למודל שמייצג הקדקוד (את ההוכחה נייצר באמצעות משימה 1). נסתכל על העץ, ונשים לב שאפשר לחלק אותו לצמדים של הוכחות שנבדלות זו מזו רק בהנחה האחרונה (כל זוג בתרשים צבוע בצבע אחר), אז אפשר (באמצעות משימה 2) למלא את ההוכחות גם של רמה את מעל:



כך ממשיכים האלה – כל פעם לוקחים צמד של הוכחות שנבדלות רק בהנחה האחרונה ומפעילים עליהם את מה שכתבתנו במשימה 2, עד שבסוף מקבלים הוכחה בלי שום הנחות:



#### 6.1.6 משימות 4-5

משימות 4 ו-5 דומות מאוד למשימות 1 ו-3 (בהתאמה), רק עבור סט גדול יותר של אופרטורים.

בשביל לעשות את משימה 4 נפעל בדיוק באותו האופן כמו שפעלנו במשימה 1: נעבור בצורה רקורסיבית, ועבור כל צורה שהנוסחא יכולה להיות בה נשתמש בכללים אחרים כדי להוכיח אותה. ההבדל הוא שהפעם נעשה את זה לסט רחב יותר של אופרטורים, ויהיו לנו יותר כללי היסק, שיעזרו לנו להתמודד עם המקרים שיוצרים האופרטורים החדשים.

משימה 5 תהיה כמו משימה 3, רק עם מה שכתבנו במשימה 4 במקום מה שכתבנו במשימה 1 (נשים לב שמה שכתבנו במשימה 2 תקף לא רק למקרים שבהם האופרטורים הם שלילה וגרירה בלבד, אז אפשר להשתמש בזה גם ב-5).

#### 6.1.7 משימה 7 ומשפט השלמות (הסופי)

במשימה 7 אנחנו מתבקשים להוכיח את משפט השלמות הסופי בלוגיקה של תחשיב הפסוקים. לפני שננסה להבין את המשפט, נתחיל בהגדרה:

☞ **קבוצת נוסחאות לא עקבית** – קבוצת נוסחאות  $S$  תקרא "לא עקבית" אם קיימת נוסחא  $\varphi$  כלשהי כך שניתן להוכיח מתוך  $S$  גם את  $\varphi$  וגם את  $\sim\varphi$ .

הסבר: אם יש לנו קבוצת נוסחאות  $S = \{\varphi_1, \dots, \varphi_n\}$  כך שקיימת נוסחא  $\varphi$  (אולי מאוד מסובכת) שאפשר מתוך קבוצת הנוסחאות שלנו להוכיח גם אותה וגם את השלילה שלה (אפשר להוכיח גם את כלל ההיסק  $\frac{\varphi_1, \dots, \varphi_n}{\varphi}$  וגם את כלל ההיסק

$(\frac{\varphi_1, \dots, \varphi_n}{\sim \varphi})$ , הקבוצה תקרא לא עקבית. כשאנחנו אומרים להוכיח אנחנו תמיד צריכים להגיד באמצעות אילו כללי היסק, וכאן אנחנו מתכוונים ללהוכיח באמצעות כללי היסק תקפים כלשהם, כלומר המשפט הזה לא מוגבל לקבוצה מסוימת של כללי היסק תקפים.

דוגמא:

$$S = \{(p \rightarrow q), (p \rightarrow \sim q), p\}$$

לא משנה אילו כללי היסק נקח, הקבוצה הזאת היא לא עקבית, כי אפשר להוכיח ממנה גם את  $q$  וגם את  $\sim q$  (ביחד עם  $p \rightarrow q$  מוכיח את  $q$ , ו- $p$  ביחד עם  $(p \rightarrow \sim q)$  מוכיח את  $\sim q$ ).

אפשר להבין את ההגדרה הזו כאומרת שאם קבוצה היא לא עקבית אז אפשר להוכיח ממנה את הסתירה  $(\varphi \& \sim \varphi)$ . מכל הסתירות שקיימות, למה אנחנו מסתכלים דווקא על זו? התשובה היא שזה לא משנה, כי שמתוך כל סתירה אפשר להוכיח כל דבר:

☞ טענה – אם  $\psi$  סתירה אז  $(\psi \rightarrow q)$  גרירה טאוטולוגית.

למה זה נכון –  $\psi$  סתירה, לכן היא לא נכונה באף מודל, ולפי איך שהגדרנו את יחס הגרירה, שקר תמיד גורר אמת. איך זה עוזר לנו להראות שמתוך סתירה אפשר להוכיח כל דבר – אם  $\psi$  היא סתירה והוכחנו שהיא נכונה, נקח את  $\psi$  ואת  $(\psi \rightarrow q)$  כהנחות ל- $MP$ , ונקבל כמסקנה את  $q$ , לא משנה מה היא הייתה.

לאחר שראינו את ההגדרה לקבוצה לא עקבית, נוכל להתקדם למשפט השלמות הסופי, אותו נצטרך להוכיח במשימה 7:

☞ משפט השלמות (הסופי) – אם  $S$  קבוצה עקבית סופית, אז יש לה מודל.

מה הכוונה ב"יש לה מודל" – קיים מודל שכל הנוסחאות ב- $S$  מקבלות  $T$  (שכל הנוסחאות ב- $S$  נכונות בו). נשים לב שזה ברור שאם לקבוצה יש מודל אז היא עקבית, כי אם יש לה מודל אז כל מה שמצליחים להוכיח מתוך הנוסחאות הזאת באמצעות כללי היסק תקפים הוא נכון באותו המודל. החלק המפתיע הוא שאם היא עקבית תמיד יש לה מודל.

בתרגיל 7 מקבלים קבוצה של נוסחאות, וצריך להכריע אחד משני דברים – או שיש לה מודל (ואז מחזירים אותו), או שהיא לא עקבית (ואז מחזירים הוכחה של  $p$  והוכחה של  $\sim p$ ).

איך עושים את זה – עוברים על כל המודלים האפשריים של המשתנים של  $S$ . אם יש אחד שהוא נכון – נחזיר אותו. אם לא מצאנו נכון, נוכיח סתירה באופן הבא: נניח ש- $S = \{\varphi_1, \dots, \varphi_n\}$ . נסתכל על הנוסחא (סדר הגימון לא משנה):

$$\varphi = (\varphi_1 \& (\varphi_2 \& (\dots \& \varphi_n)))$$

- בשביל להוכיח את  $\varphi$  נשתמש פשוט בכל ההנחות שלנו (שהן הנוסחאות של  $S$ ).
- בשביל להוכיח את  $\sim \varphi$  נעזר בכך של- $S$  אין מודל: אם ל- $S$  אין מודל זה אומר שבכל מודל שהוא לפחות אחת הנוסחאות של  $S$  תקבל ערך שקר, לכן  $\sim \varphi$  היא טאוטולוגיה, ואנחנו כבר יודעים להוכיח טאוטולוגיות (אפילו לא נזדקק להנחות בשביל זה).

יש לנו שתי הוכחות – אחת ל- $\varphi$  ואחת ל- $\sim \varphi$  – וזה בדיוק מה שרצינו.

נדגיש שההוכחה שראינו כאן תקפה לקבוצה  $S$  סופית. קיימת גם גרסא אינסופית למשפט השלמות, שגם היא נכונה כמובן, אך מכיוון שהיא אינסופית לא נוכל להוכיח אותה באמצעים תכנותיים, ולכן נוכיח אותה בהמשך מתוך הגרסא הסופית באמצעות מתמטיקה "רגילה".



## 7 שיעור 7 – 3.12.17

### 7.1 תחשיב היחסים (פרדיקטים) – לוגיקה מסדר ראשון

#### 7.1.1 רקע

היום נתחיל את החצי השני של הקורס – החלק שעוסק ב**תחשיב היחסים** (שנקרא גם תחשיב הפרדיקטים, או לוגיקה מסדר ראשון).

בחצי הראשון של הקורס הכרנו את תחשיב הפסוקים, ועכשיו נעבור לדבר הכולל יותר שהוא תחשיב היחסים. הקשר בין החצי הראשון לשני הוא כפול – דבר ראשון, החצי הראשון היווה מעין "גלגלי עזר לשני": את אותם קונספטים (סינטקס מולל סמנטיקה, הוכחות ומודלים) יש גם כאן באופן מורחב יותר. דבר שני, החלק הראשון ישמש אותנו ישירות במובן שכל מה שקיבלנו בתחשיב הפסוקים לא נצטרך לקבל שוב בפרדיקטים. בלוגיקה מסדר ראשון יופיעו הקשרים שראינו כבר בתחשיב הפסוקים, כמו גם משפטים שהוכחנו בנוגע לטאוטולוגיות בתחשיב הפסוקים. לסיכום, שתי נקודות החיבור בין חלקי הקורס הן דמיון קונספטואלי בין החלקים, ושימוש בחלק השני במה שהוכחנו בחלק הראשון.

לאחר שסקרנו את נקודות הדמיון, נרצה לדבר על ההבדלים בין תחשיב הפסוקים ותחשיב היחסים, ולהבין מדוע אנחנו זקוקים בכלל לתחשיב היחסים. בתחשיב הפסוקים, הקלט היה בוליאני ועשינו עליו מניפולציות בוליאניות, והתשובה הייתה תמיד ערך אמת כלשהו. אנחנו היינו רוצים לקבל שפה שנוכל להביע באמצעותה גם דברים אחרים, דברים שאנחנו נתקלים בהם בחיי היום-יום ובמתמטיקה. תחשיב היחסים נותן מענה לצורך הזה.

ניתן דוגמאות לשלוש צורות של דברים שהיינו רוצים לדעת להביע –

#### דוגמא 1:

לכל  $x$  קיים  $y$  כך ש:  $x + y = 0$

זו דוגמא למשהו שנרצה להגיד כמתמטיקאים, ותחשיב הפסוקים לא יאפשר לנו. בפרט, לא נוכל להשתמש בתחשיב הפסוקים בשביל זה כי  $x$  ו- $y$  כאן הם לא דווקא בוליאניים, אלא יכולים להיות מכל עולם אחר שהוא (למשל: מספרים, איברים של שדה כלשהו וכו'). השפה שנגדיר של תחשיב היחסים תעזור לנו לתאר פסוקים כאלה

#### דוגמא 2:

אם  $x > y$  וגם  $y > z$  אז  $x > z$

בדומה לדוגמא הקודמת, גם משפט כזה שכולל יחסים בין איברים נרצה לדעת לתאר.

דוגמא 3: עד כה הדוגמאות שראינו היו מעולם המתמטיקה. כמו שצינו, אנחנו רוצים להיות מסוגלים לתאר גם מושגים לוגיים מהשפה היום-יומית, וגם הם מגיעים לא רק מעולם שיש בו רק אמת ושקר. לדוגמא, היינו רוצים לפרמל משהו מהסוג הבא:

כל בעלי החיים מרגישים כאב  
לא מוסרי לאכול מה שמרגיש כאב  
⇐ לא מוסרי לאכול בעלי חיים

אפשר לדון על האם כל אחת משתי ההנחות נכונות (לא בקורס הזה), אבל אפשר גם בצורה נפרדת לדון על האם המסקנה נובעת משתי ההנחות אילו הן היו נכונות (כן בקורס הזה). היינו רוצים לדעת להכריע האם ההיסק הלוגי הזה הוא נכון בהנתן העולם שרלוונטי למשפט הזה.

נציג עכשיו את התחשיב שהוא התחשיב הרגיל שמתמשים בו במתטיקה (ובפרט בלוגיקה), והוא יאפשר לנו לדבר על העולם הזה – תחשיב היחסים.

לפני שנגדיר את המרכיבים שלו בצורה פורמלית, נראה את הפסוקים שרצינו להביע כשהם בצורה של תחשיב היחסים, ונקבל קצת אינטואיציה ונבין לקראת מה אנחנו הולכים –

עבור דוגמא 1:

$$\forall x [\exists y [plus(x, y) = 0]]$$

זה יהיה פסוק בעולם שלנו. מבחינה תכנותית, את ה- $\forall$  נכתוב בפיתוח כ- $A$  ובדומה את  $\exists$  כ- $E$ . כל הדברים מהצורה  $x + y$  נכתבים ישירות כפונקציה אצלינו.

עבור דוגמא 2:

$$((GT(x, y) \& GT(y, z)) \rightarrow GT(x, z))$$

$GT$  הוא יחס כאן.  $GT(x, y)$  אומר ש- $x > y$ .

עבור דוגמא 3:

נצטרך להמציא שמות של יחסים לכל יחס שמופיע במשפטים שלנו, כמו "בעליהחיים" ו-"מרגישים כאב".

$$\begin{aligned} \forall x [(Living(x) \rightarrow FeelsPain(x))] \\ \forall x [(FeelsPain(x) \rightarrow Shouldn'tEat(x))] \end{aligned}$$

ומכאן אנחנו רוצים להסיק:

$$\forall x [(Living(x) \rightarrow Shouldn'tEat(x))]$$

### 7.1.2 הגדרה פורמלית – סינטקס

אחרי שקיבלנו קצת אינטואיציה, נגדיר את האלמנטים של התחשיב בצורה יותר פורמלית. להבדיל מתחשיב הפסוקים, שם היה רק אלמנט אחד של נוסחא, כאן יש שני סוגי אלמנטים: איברים שעליהם מדברים (למשל:  $x, y, plus(x, y), 0$ ) ואיברים שמקבלים ערכי אמת (למשל:  $x \rightarrow y, (Living(x) \rightarrow FeelsPain(x))$ ).

הסוג הראשון של האיברים הם איברים מתוך העולם שאנחנו מדברים עליו, ולאבר מסוג כזה נקרא **Term** (שם עצם). האיברים מהסוג הם איברים שמחזירים תוצאה בוליאנית, כמו שהיה לנו בחלק הראשון של הקורס, וגם כאן נקרא לאבר מהסוג הזה **Formula** (נוסחא).

באופן יותר ספציפי, נגדיר את המונחים והנוסחאות באופן הבא:

#### 1. **Term** –

a. **קבועים** – אלה ערכים מתוך העולם שלנו.

**סינטקס:** מתחילים בספרה או באחת האותיות  $a, \dots, d$ .

**דוגמא:**  $0, aShalom$ .

b. **משתנים** – זה משהו שלתוכו אפשר להציב כל ערך או ערכים מתוך העולם שלנו.

**סינטקס:** מתחילים באותיות  $u, \dots, z$ .

**דוגמא:**  $x, y, u7, xYosi$ .

c. **פונקציות** – משהו שמקבל מספר שמות עצם, ומחזיר שם עצם.

**סינטקס:** מתחילות באותיות  $t, \dots, f$ , והן מהצורה  $f(x_1, \dots, x_n)$  כך ש- $x_i$  הם שמות עצם.  
**הערה על ההגדרה:** פונקציה מוגדרת בצורה רקורסיבית, לעומת שני הקודמים שהיו מוגדרים באופן בסיסי.

**דוגמא:**  $f(g(h(7), 8), abc)$  היא פונקציה – 7 הוא קבוע ומכאן הוא שם עצם, לכן  $h(7)$  הוא שם עצם (כפונקציה שמופעלת על קבועים) וכו', ולבסוף מגיעים לכך ש- $f$  הוא שם עצם.

## 2. Formula –

a. **יחס** – מקבל שמות עצם ואומר האם הם מקיימים תכונה מסוימת או לא.

**סינטקס:** מתחיל באות גדולה בין  $T, \dots, F$ , והוא מהצורה  $R(x_1, \dots, x_n)$  כך ש- $x_i$  הם שמות עצם.  
**הבדל בין יחס לבין פונקציה:** פונקציה מדברת על איבר בעולם. לדוגמא, אם אנחנו בעולם המספרים השלמים,  $h(7)$  שראינו ייתן אמת או שקר אלא מספר. לעומת זאת, היחס נותן תמיד ערכי אמת. לכן, פונקציה של שמות עצם מחזירה שם עצם, אבל יחס של משהו זה כבר נוסחא. עם זאת, נשים לב שיחס כן עובד על איברים מהעולם שלנו, זו הדרך שלנו לעבור מאיברים מהעולם שלנו לעולם הבוליאני.  
**הקשר להגדרה של יחס שמוכרת לנו ממתמטיקה:** במתמטיקה, יחסים  $n$ -ריים (כלומר על  $n$  איברים) הם תתי-קבוצות של  $n$ -יות של איברים. אצלינו, תתי-הקבוצה היא ה- $n$ -יות של איברים שהערך של הפעלת היחס עליהם נותן אמת.

i. **יחס השיוויון** – יחס מיוחד שייכתב בצורה  $t_1 = t_2$  (הם שמות עצם).

b.  $\rightarrow, \sim, |, \&$  – האופרטורים הבינאריים שאנחנו מכירים כבר מהחלק הראשון, ונתנהג איתם באותו האופן. את הפעולות האלה אפשר להפעיל על כל נוסחא.  
**הערה:** בנוסחא, האיברים הפרימיטיביים שיהיו לנו יתקבלו מהפעלת יחס על שמות עצם (בפרט יחס השיוויון, אבל גם כל יחס אחר). עליהם אפשר יהיה להפעיל את האופרטורים הבוליאניים.

c. **כימות** – אם  $\varphi$  היא נוסחא ו- $x$  משתנה, שני הדברים הבאים הם נוסחאות:

$$\forall x [\varphi]$$

$$\exists x [\varphi]$$

**סינטקס:** כאמור, בפייתון נשתמש ב- $A$  בשביל  $\forall$  וב- $E$  בשביל  $\exists$ . כמו כן, נקפיד על סוגריים מרובעים במקרה הזה.

בזאת הגדרנו את הסינטקס של תחשיב הפסוקים. נעיר הערה שתעזור לנו בתרגיל 7 – כשנעשה *parsing* בתרגיל, הן עבור שמות עצם והן עבור נוסחאות, הוגדר לנו לממש קודם כל מתודת עזר בשם *parsePrefix*, ש מקבלת מחרוזת ומתחילה לאכול אותה אות אחרי אות עד לסוף שם עצם הראשון.

לדוגמא:  $\text{parsePrefix}(\text{plus}(x, y)) = 0$  יחזיר שני דברים – את שם העצם  $\text{plus}(x, y)$ , ואת המחרוזת של כל מה שנשאר ממחרוזת הקלט לאחר שהורדנו שם העצם הזה (כלומר את מה שלא גמרנו לעשות לו פארסינג, במקרה של הדוגמא שלנו זה המחרוזת 0).

אנחנו עושים את זה בשביל נוחות העבודה, ספציפית נוחות העבודה עם קריאות רקורסיביות. אם למשל רואים פונקציה, אחרי השם של הפונקציה ופתיחה סוגריים אמורים להופיע מספר שמות עצם. נוכל להפעיל את *parsePrefix* על כל שמות העצם האלה בידוד ולקבל את שם העצם עד הפסיק הראשון (הפרמטר הראשון של הפונקציה) + סטרינג השארית (כל שאר הפרמטרים של הפונקציה), ואז להפעיל את *parsePrefix* על מחרוזת

השארית וכך הלאה בצורה רקורסיבית. זה קצת יותר "מהיר ומלוכלך" מאשר לעשות  $tokenizer^8$ , אבל לצורך רמת הסיבוכיות שלנו בקורס זה מספיק.

### 7.1.3 הגדרה פורמלית – סמנטיקה

כדי שהסינטקס שהגדרנו עכשיו יהיה מעניין, אנחנו צריכים לתת לו משמעות, ובשביל משמעות אנחנו צריכים מודל. בתחשיב החדש, מודל יהיה אובייקט יותר מורכב מאשר מילון בין לדברים לערכים, כי יש לנו די הרבה דברים שצריך לתת להם משמעות.

הדרך שבה נגדיר מודל היא דרך מחלקה שנקראית מודל, והיא צריכה לאפשר לנו לתת משמעות לתת לכל אחד מהאלמנטים. המודל כולל שני רכיבים:

- $\Omega$  – העולם (universe), על אילו עצמים אנחנו מדברים. לדוגמה: שדה הטבעיים. במתמטיקה הרגילה העולם יכול להיות אינסופי, אבל אנחנו כמובן נגביל את עצמינו לעולמות סופיים (מקרה פרטי של העולם במתמטיקה). הייצוג בפייטון של העולם יהיה ע"י סט.

- **משמעות לאלמנטים** – משמעות שניתנת בצורה של מילון בפייטון, שהמפתחות בו הם הדברים שאנחנו צריכים לתת להם משמעות, והערכים הם המשמעות של כל אחד מהם. משמעות ניתנת במודל לכל אחד מהאלמנטים הבאים:

- קבוע: נותן מיפוי בין שמות הקבועים לבין איברים מהעולם.
- פונקציה  $k$ -ערכית: לפונקציה שמקבלת  $k$  ערכים אנחנו צריכים לתת משמעות של מיפוי  $f: \Omega^k \rightarrow \Omega$  (כלומר, בין קבוצות של  $k$  איברים מהעולם שלנו שהם הקלט של הפונקציה לבין איבר כלשהו מהעולם שלנו שהוא הפלט של הפונקציה). נעשה את זה בפייטון באמצעות מילון של טאפלים (כלומר, במילון המקורי כל פונקציה  $k$ -ערכית תמופה למילון שהמפתחות שלו הם טאפלים באורך  $k$  של איברים מהעולם, והערכים שלו הם איבר מהעולם).
- יחס  $k$ -ערכי: בשביל להגדיר מהן קבוצות האיברים שיחס על  $k$  איברים מחזיר עליהן אמת ומה קבוצות שעליהן הוא מחזיר שקר, נמפה כל יחס לתת-קבוצה של אוסף ה- $k$ יות  $\Omega^k$ , שתהיה קבוצת האיברים שלגביהם הוא מחזיר אמת. אצלינו בפייטון נמפה כל יחס ל- $set$  של טאפלים באורך  $k$ , והמשמעות תהיה שעבור כל אחד מהאיברים בסט הזה היחס מחזיר אמת, ורק עבורם (במילים אחרות: אם קבוצה של  $k$  איברים היא טאפל בסט הזה אז היחס מחזיר עבודה אמת, אחרת הוא מחזיר עבודה שקר).

נעיר שלמשתנים לא ניתן משמעות כחלק מהמודל.

**דוגמה 1:** נניח שאנחנו רוצים מודל כלשהו (לאו דווקא מודל שמקיים) עבור:

$$\forall x [\exists y [plus(x, y) = 0]]$$

נוכל להגדיר מודל למשל כך –

- נקח את העולם שלנו להיות:  $\Omega = \{0, 1, 2\}$
- הפונקציה  $plus(t_1, t_2)$  תהיה המיפוי הבא:

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

<sup>8</sup> [https://en.wikipedia.org/wiki/Lexical\\_analysis](https://en.wikipedia.org/wiki/Lexical_analysis). ככה עובדים למשל בקורס Nand To Tetris.

יכולנו למלא את הטבלה איך שאנחנו רוצים והיינו מקבלים מודל כלשהו, אבל נשים לב שלא יכולנו לשים נגיד 4 בטבלה, כי זה לא איבר שקיים בעולם שלנו.

- נצטרך למפות את הקבוצה '0' שמופיע בנוסחא (מצד ימין של השיוויון). נשים לב שזה שהשם של הקבוצה הוא '0' לא אומר בהכרח שגם הערך שלו יהיה אפס. זה יהיה הגיוני להגדיר את זה ככה כשנגדיר את המודל, אבל באופן עקרוני אנחנו לא חייבים לעשות את זה, ומה שקובע את המשמעות של הקבוצה זה הערך שניתן לו במודל ולא השם שלו.
- במודל שאנחנו בונים עכשיו, נחליט ללכת על המיפוי ההגיוני '0': 0 (כלומר, המחרוזת '0' שווה לאיבר 0 בעולם). בפייתון, נשמור את זה בתוך מילון.

דוגמא 2:

$$((GT(x, y) \& GT(y, z)) \rightarrow GT(x, z))$$

- נבחר שוב את העולם שלנו להיות:  $\Omega = \{0, 1, 2\}$
- איך  $GT$  יראה מתמטית:

	0	1	2
0	X	X	X
1	V	X	X
2	V	V	X

ואז בפייתון זה יראה כך:

$$\{(1,0), (2,0), (2,1)\}$$

- נצטרך למפות בין המשתנים  $x, y, z$  לבין ערכים שלהם מהעולם, כמו שעשינו בדוגמא הקודמת עבור המשתנה '0'.

### 7.1.3.1 השמות למשתנים וחישוב ערכים

בשביל להשלים את התמונה הסמנטית, נשאל את עצמנו עכשיו את השאלה הבאה: בהנתן מודל, האם אנחנו יכולים לחשב את הערך של כל נוסחא? התשובה היא שלא, מודל לא כולל את המשמעות של משתנים, ולכן לא נוכל לחשב את הערך של כל נוסחא.

כדי לחשב ערך נצטרך לקבל שני דברים:

1. מודל
2. השמה למשתנים החופשיים (נדבר עוד מעט על מה הכוונה בחופשיים)

מודל לבד לא מספיק כדי לתת ערך לכל נוסחא, כי ברגע שיש משתנים הוא לא יכול לתת להם ערך. ההשמה תאמר לנו עבור כל משתנה איזה ערך הוא מקבל.

בהנתן מודל והשמה, נשים לב שאנחנו יכולים כבר לחשב כל שם עצם שהוא, כי אנחנו יודעים לחשב שמות עצם מכל הסוגים:

- ערך של קבוצה: המודל נותן לנו.
- ערך של משתנה: ההשמה נותנת לנו.
- ערך של פונקציה: המודל אומר לנו מה הפונקציה שצריך להשתמש בה. את ערכי הקלט של הפונקציה מגלים לפי קריאה רקורסיבית על שמות העצם של הפונקציה. לאחר שיש לנו את הערכים של שמות העצם, נוכל להסתכל על המודל כדי לדעת מה הערך שהפונקציה נותנת.

באותו אופן, אנחנו יודעים לחשב ערך של כל נוסחא:

- ערך של יחס: לכל שם עצם ראינו שאנחנו יודעים מה הערך שלו בהנתן השמה ומודל, אז נוכל להרכיב טאפל מכל שמות העצם שהם הקלט של היחס, ולבדוק האם הם נמצאים במילון שבמודל. לפי זה נדע מה להחזיר.
- ערך של היחס  $t_1 = t_2$ : רקורסיבית יודעים איזה איבר יש מימין ואיזה משמאל, ונחליט שהם אמת אם זה בדיוק אותו איבר.
- ערך ארבע הפעולות הלוגיות: הפעולות האלה עובדות על שמות עצם שהם מעין פסוקים אטומים, אז אנחנו כבר יכולים לדעת את הערך של כל אחד מהם, ומכך לדעת את הערך של האופרטור הלוגי כמו שעשינו עד עכשיו.

לכן, אם קיבלנו מודל והשמה ראינו כבר שאפשר לחשב כמעט כל דבר, ורק נותרו לנו הכמתים. הכמתים נותנים לנו מימד סמנטי חדש לשפה שלנו, ואלמלא היולנו הכמתים, אפשר היה לראות בכל מה שדיברנו עליו עד כה כמעט רק שיטה יותר יפה לתת שמות מעניינים לפסוקיות האטומיות. איך נחליט מה הולך להיות ערך האמת של כל כמת:

- הערך של  $\forall x$ : יקבל ערך אמת אם הנוסחא שמופיעה אחריו מקבלת ערך אמת עבור כל השמה אפשרית של  $x$ . במילים אחרות, נעבור אחד-אחד על האלמנטים של  $\Omega$ , ועבור כל אלמנט  $\omega \in \Omega$  נבדוק את ערך האמת של הנוסחא עבור  $x = \omega$ . אם בכל אחת מהבדיקות האלה קיבלנו ערך אמת, נחזיר אמת.
- הערך של  $\exists x$ : יקבל ערך אמת אם הנוסחא שמופיעה אחריו מקבלת ערך אמת השמה כלשהי של  $x$ . במילים אחרות, נעבור אחד-אחד על האלמנטים של  $\Omega$ , ועבור כל אלמנט  $\omega \in \Omega$  נבדוק את ערך האמת של הנוסחא עבור  $x = \omega$ . אם לפחות באחת מהבדיקות האלה קיבלנו ערך אמת, נחזיר אמת.

### 7.1.3.2 משתנים חופשיים, משפטים וסקופים של משתנים

נשים לב שקיבלנו שעבור חלק מהנוסחאות כלל לא נזדקק להשמה בשביל לדעת את ערך האמת של הנוסחא. לדוגמא, בשביל לדעת את הערך של:

$$\forall x [(Living(x) \rightarrow FeelsPain(x))]$$

מספיק מודל שיגיד לנו מה מה העולם ומשמעות הפונקציות, ולא נזדקק גם להשמה, כי במילא אנחנו עוברים על כל האפשרויות עבור  $x$ . לעומת זאת, בשביל לדעת את הערך של:

$$((GT(x, y) \& GT(y, z)) \rightarrow GT(x, z))$$

נהיה חייבים לקבל גם השמה.

זה מוביל אותנו לשתי הגדרות שישלימו לנו משהו שדיברנו עליו קודם:

**משתנה חופשי** – משתנה שלא נמצא בתוך כמת על המשתנה הזאת. במילים אחרות, משתנה מוגדר חופשי אם הוא לא עטוף ע"י כמת.

לדוגמא, ב- $\forall x [plus(x, z) = x]$  הוא משתנה חופשי ו- $x$  אינו משתנה חופשי.

**משפט (sentence)** – פסוק שלא מכיל משתנים חופשיים, כלומר פסוק שאין צורך בהשמה בשביל לדעת את הערך שלו.

ההגדרה הזאת מעניינת אותנו כי אם פסוק הוא משפט נוכל לתת לו ערך מבלי לעשות אבלואציה על השמה.

נשים לב שאותו שם משתנה יכול לחזור בין סקופים (scopes) שונים, ונצטרך לא להתבלבל. לדוגמא:

$$(F(x) \rightarrow \forall x G(x, y))$$

ה- $x$  הראשון (בתכלת) הוא משתנה חופשי, אבל ה- $x$  השלישי (בסגול) הוא לא חופשי. כלומר, ההגדרה של מה שחופשי או לא הוא לגבי אינסנט של משתנה ולא לגבי משתנה באופן כללי.

יכולנו גם לכתוב את הפסוק הבא:

$$\forall x [(F(x) \rightarrow \forall y G(x, y))]$$

עכשיו גם ה- $x$  הפנימי הראשון (תכלת) וגם השלישי (סגול) הם לא חופשיים, אבל צריך לשים לב טוב עבור כל  $x$  מי הכמת שעובד עליו. הראשון (תכלת) יהיה לא חופשי בגלל ה- $\forall x$  הכי חיצוני (בירוק), והשלישי יהיה לא חופשי בגלל ה- $\forall x$  הפנימי (בכתום).

הכלל שלנו יהיה: תמיד הכמת שנותן ערך למשתנה הוא של הסקופ הפנימי ביותר.

נצטרך לשים לזה לב טוב כשנרצה לעשות אבלואציה לנוסחא, אז נצטרך לדעת האם משתנה הוא חופשי או לא, ולהיות מודעים לכך שמשתנה שהופיע בסקופ חיצוני יכול להופיע שוב בתור משתנה מקומי של סקופ פנימי.

בכך סיכמנו את ההכנה לתרגיל 7 – סינטקס וסמנטיקה של פסוקים בתחשיב הפרדיקטים.

## 7.2 הוכחה של משפט השלמות בתחשיב הפסוקים לקבוצות אינסופיות

נחזור עכשיו לתחשיב הפסוקים כדי להוכיח את משפט השלמות בגרסתו הרגילה (זו שלא מצומצמת לקבוצות סופיות).

גולת הכותרת של תרגיל 6 הייתה משפט השלמות לקבוצות סופיות. הייתה לנו אז קבוצת פסוקים עקבית (כלומר כזו שאי-אפשר להוכיח ממנה סתירה), והוכחנו שקיים לה מודל ע"י כך שבנינו אותו (הכוונה ב"קיים לה מודל" היא שיש מודל שבו כל הנוסחאות שלה מקבלות ערך אמת).

גם הכיוון השני הוא נכון – כל קבוצת פסוקים שיש לה מודל שמקיים אותה היא עקבית. זה נכון כי אנחנו יודעים שאם קיים מודל, כל מה שהוכחנו מתוך המודל חייב להיות נכון, כלומר כל מה שאפשר להוכיח מתוך קבוצת פסוקים שנכונה במודל מסויים הוא גם נכון (אם כל ההנחות הן אמת אז גם התוצאה היא אמת). כלומר, כל נוסחא  $\varphi$  שנוכיח מתוך המודל תקבל ערך אמת, ולכן לא יכול להיות ש- $\sim\varphi$  גם הוא אמת. לזה קראנו משפט הנאותות.

מה שהוכחנו היה רק עבור קבוצות סופיות של פסוקים. משפט השלמות מכליל את מה שעשינו גם לקבוצות אינסופיות של פסוקים – יש אינסוף פסוקים, ואם הם עקביים יש מודל שנותן אמת לכולם. נעיר שהאינסופיות היא במספר הפסוקים ולא באורך שלהם: כל פסוק בפני עצמו הוא סופי, אבל יש מספר אינסופי של פסוקים.

נעבור להוכחה של המשפט:

👉 **משפט השלמות** – תהי  $F$  קבוצת פסוקים עקבית, אזי יש ל- $F$  מודל.

בשביל לעשות את זה, נעזור בשתי למות שיתבססו על דברים שהוכחנו בתרגיל 6:

👉 למה 1: יהי  $\varphi$  פסוק ו- $M$  מודל על משתנים  $x_1, \dots, x_n$ . נטען:

$$\xi_i := \begin{cases} x_i, & \text{אם ערך } x_i = T \text{ במודל} \\ \sim x_i, & \text{אם ערך } x_i = F \text{ במודל} \end{cases}$$

אזי  $\{\xi_1, \dots, \xi_n, \varphi\}$  עקבית אמ"מ  $M \models \varphi$ .

הטענה היא כאן שהקבוצה הזאת עקבית אמ"מ הנוסחא  $\varphi$  מקבלת ערך אמת במודל. אנחנו הראנו את זה בתרגיל ע"י כך שהראנו שאם  $\varphi$  היא נכונה אז הפסוק  $\left( \left( \xi_1 \& (\xi_2 \& \dots \& \xi_n) \right) \rightarrow \varphi \right)$  ניתן להוכחה (משימה 1). מזה נובע שקיים מודל שמספק את כל איברי הקבוצה  $\{\xi_1, \dots, \xi_n, \varphi\}$  (המודל  $M$  בעצמו), וכמו שאמרנו קודם, אם לקבוצה מודל אז היא עקבית, וזה מה שרצינו להראות.

למה 2: תהי  $F$  קבוצת פסוקים עקבית ו- $\varphi$  פסוק, אזי מתקיים  $F \cup \{\varphi\}$  עקבית או  $F \cup \{\sim\varphi\}$  עקבית.

למה זה נכון – בתרגיל הראנו שאם אנחנו יכולים להוכיח נוסחא  $\psi$  כלשהי גם מ- $F \cup \{\varphi\}$  וגם מ- $F \cup \{\sim\varphi\}$  אז אפשר להוכיח את  $\psi$  ישירות מ- $F$  (משימה 2). אם גם  $F \cup \{\varphi\}$  וגם  $F \cup \{\sim\varphi\}$  היו לא עקביות, זה אומר שהיה אפשר מכל אחת מהן להוכיח סתירה כלשהי. ראינו בשיעור שעבר שמתוך סתירה אפשר להוכיח כל דבר, לכך אפשר היה בפרט להוכיח מתוך שתיהן פסוק מסויים כלשהו ושליטתו. זה אומר שאפשר היה להוכיח את אותו פסוק ואת שלילתו גם מ- $F$ , בסתירה לעקביות של  $F$ . לכן, מתקיים  $F \cup \{\varphi\}$  עקבית או  $F \cup \{\sim\varphi\}$  עקבית, וזה מה שרצינו להוכיח.

נעבור עכשיו להוכחה עצמה, ונרצה להוכיח שאם  $F$  עקבית אז יש לה מודל. ההוכחה, בקווים כלליים, תעבוד כך: נקח את  $F$  ונוסיף לו פסוקים תוך שמירה על כך שהקבוצה שאנחנו יוצרים עקבית, ובקבוצה היותר גדולה שנגיע אליה יהיה לנו יותר ברור איך לייצר מודל.

### הוכחה:

1. נסדר את כל הפסוקים בעולם בסדרה  $\varphi_1, \varphi_2, \dots$ .  
הסבר: יש אמנם אינסוף פסוקים, אבל כל פסוק הוא סופי וגם הא"ב שלנו הוא סופי, ולכן נוכל להסתכל על סדרה שתהיה מורכבת מכל הפסוקים באורך 1, אחריהם כל הפסוקים באורך 2 וכך הלאה. בגלל שהא"ב שלנו הוא סופי, לכל אורך נתון יהיה מספר סופי של פסוקים שקיימים באורך הזה, ולכן נוכל להגדיר את הסדר הזה.

2. נגדיר עכשיו סדרה של קבוצות באופן הבא:

$$F_0 = F$$

$$\forall i > 0: F_i = \begin{cases} F_{i-1} \cup \{\varphi_i\}, & \text{אם זה עקבי} \\ F_{i-1}, & \text{אחרת} \end{cases}$$

הסבר: אם הוספה של הפסוק ה- $i$  לקבוצה במקום ה- $i-1$  נותנת קבוצה עקבית, נבחר את הקבוצה במקום ה- $i$  להיות הקבוצה במקום ה- $i-1$  בתוספת הפסוק במקום ה- $i$ . אם הוספה של הפסוק במקום ה- $i$  גורמת לקבוצה במקום ה- $i-1$  להיות לא עקבית, נקח את הקבוצה במקום ה- $i$  להיות הקבוצה במקום ה- $i-1$  ללא שינוי.

3. נגדיר את הקבוצה:

$$F^* = \bigcup_i F_i$$

נוכיח שתי טענות עזר על  $F^*$  שבאמצעותן נוכל להמשיך את ההוכחה.

טענת עזר 1:  $F^*$  עקבית.

למה זה נכון:



- כל  $F_i$  הוא עקבי כי התחלנו מקבוצה עקבית, ועשינו שינויים רק אם הם שמרו על העקביות.
- למה האיחוד של כל ה- $F_i$ ים עקבי: נניח בשלילה ש- $F^*$  לא עקבית. זה אומר שקיימת הוכחה של סתירה מתוך  $F^*$ . נשים לב שאמנם  $F^*$  אינסופית, אבל ההוכחה הזאת חייבת להיות סופית – ככה הגדרנו הוכחה, כדבר סופי. זה אומר שהיא משתמשת רק במספר סופי של פסוקים מתוך  $F^*$ . נסתכל על הפסוק בעל האינדקס הגבוה ביותר שבו ההוכחה משתמשת, שנסמן אותו ב- $\varphi_j$ . כל הפסוקים שהשתמשנו בהם בהוכחה נמצאים ב- $F^*$  והאינדקסים של כולם קטנים או שווים  $j$ , לכן זה אומר שכל הפסוקים שהשתמשנו בהם בהוכחה נמצאים ב- $F_j$  (זה נובע ישירות מאיך שבנינו את הקבוצות  $F_i$ ). כלומר, את אותה הסתירה שהוכחנו מתוך  $F^*$  אפשר היה להוכיח גם מתוך  $F_j$ , וזו סתירה למה שאמרנו בנקודה הקודמת. קיבלנו סתירה להנחת השלילה, כלומר הראנו ש- $F^*$  אכן עקבית.

👉 טענת עזר 2:  $F^*$  מקסימלית.

נצטרך קודם כל להסביר למה אנחנו מתכוונים –

👉 **קבוצת פסוקים עקבית מקסימלית** – קבוצת פסוקים עקבית  $F$  נקראית מקסימלית אם לכל  $\varphi$  מתקיים או  $\varphi \in F$  או  $\sim\varphi \in F$ .

כלומר, הקבוצה נקראית מקסימלית אם היא מכילה לכל פסוק בעולם או אותו או את שלילתו.

למה  $F^*$  היא עקבית מקסימלית:

- נניח בשלילה שיש פסוקית  $\varphi \notin F^*$  וגם  $\sim\varphi \notin F^*$ . ראינו כבר ש- $F^*$  עקבית, אז מלמה 2 מתקיים  $F^* \cup \{\varphi\}$  עקבית או  $F^* \cup \{\sim\varphi\}$  עקבית. זה אומר שבבנייה שלנו היינו אמורים להכניס או את הפסוק  $\varphi$  או את הפסוק  $\sim\varphi$  ל- $F_k$  בלשהו, כי כשהגענו אל הפסוק הזה הוא שמר על עקביות (כי אם הוא עקבי עם  $F^*$  הוא מן הסתם עקבי גם עם כל  $F_i$  שהוא, שמכיל פחות פסוקים מאשר  $F^*$ ). מכאן שהפסוק היה אמור להכנס גם ל- $F^*$ , בסתירה להנחת השלילה.

עכשיו כשהראנו את שתי הטענות האלה, נחזור להוכחה של המשפט. בשלב הזה אנחנו כבר מוכנים לתת מודל –

4. לפי טענת עזר 2 אנחנו יודעים שלכל משתנה  $x_i$  מתקיים  $x_i \in F^*$  או  $\sim x_i \in F^*$ . נבנה את המודל  $M$  הבא:

$$\circ \quad x_i \in F^* \text{ אם } x_i = T$$

$$\circ \quad x_i = F \text{ אם } \sim x_i \in F^*$$

👉 טענת עזר סופית: כל נוסחא  $\varphi \in F^*$  מסתפקת במודל (כלומר  $M \models \varphi$ ).

למה זה נכון:

- יהיו  $x_1, \dots, x_n$  המשתנים ב- $\varphi$ .
- אנחנו יודעים שכל אחד מה- $x$ ים האלה או שלילתו נמצאים ב- $F^*$  (טענת עזר 2), כלומר לפי איך שבחרנו את המודל  $M$  נקבל ש- $\{\xi_1, \dots, \xi_n\} \in F^*$  (מוגדר כמו שהוא הוגדר בלמה 1).
- כיוון שכך, הקבוצה  $\{\xi_1, \dots, \xi_n, \varphi\}$  היא עקבית כתת-קבוצה של  $F^*$ .
- לכן, מלמה 1 נקבל ישירות  $M \models \varphi$ , וזה מה שרצינו להראות.

זה מוביל אותנו לצעד האחרון של הוכחת משפט השלמות –

5. כל נוסחא  $\varphi \in F^*$  מסתפקת במודל  $M$  (לפי טענת העזר הסופית). הקבוצה  $F$  היא תת־קבוצה של  $F^*$ , ולכן בפרט כל הפסוקים שלה מסתפקים במודל  $M$ , וזה מה שרצינו להוכיח.

בזאת סיימנו את הוכחת משפט השלמות.

נעיר שלא הוכחנו שתת־קבוצה של קבוצה עקבית היא גם עקבית, אבל זה טריוויאלי – נניח בשלילה שהקבוצה הגדולה היא עקבית אבל תת־הקבוצה היא לא. זה אומר שאפשר להוכיח סתירה מתוך תת־הקבוצה, אבל כל הפסוקים שמהם הוכחנו את זה נמצאים בקבוצה היותר גדולה, אז אפשר להוכיח את הסתירה גם מהקבוצה הגדולה, בסתירה לעקביותה.

### 7.3 משפט הקומפקטיות

מתוך כל מה שעשינו עד כה נוכל לקבל "במתנה" הוכחה של משפט חשוב נוסף, משפט הקומפקטיות:

**משפט הקומפקטיות לתחשיב הפסוקים** – לקבוצת פסוקים בתחשיב הפסוקים יש מודל אם"מ לכל תת־קבוצה סופית שלה יש מודל.

בשביל לראות את זה, נסתכל על הטבלה הבאה:

אינסופי	סופי	
$F$ עקבית	כל תת־קבוצה סופית של $F$ עקבית	<b>סינטקס</b>
$F$ יש מודל	לכל תת־קבוצה סופית של $F$ יש מודל	<b>סמנטיקה</b>

נתחיל מלהסתכל על הגרירות הברורות, ומאיפה הן נובעות:

אינסופי	סופי	
$F$ עקבית	כל תת־קבוצה סופית של $F$ עקבית	<b>סינטקס</b>
$F$ יש מודל	לכל תת־קבוצה סופית של $F$ יש מודל	<b>סמנטיקה</b>

- הגרירות הכחולות: כמו שכבר אמרנו, ברור שאם  $F$  עקבית אז כל תת־קבוצה סופית שלה היא גם עקבית, ושם  $F$  יש מודל אז לכל תת־קבוצה סופית של  $F$  המודל הזה גם מתאים.
- הגרירה האדומה: מה שהוכחנו היום.
- הגרירה הסגולה: מה שהוכחנו בשיעורי הבית.
- הגרירה הירוקה: זה נובע מהגדרת ההוכחה. אם נניח בשלילה שכל תת־קבוצה של  $F$  היא עקבית אבל אפשר להוכיח סתירה מתוך  $F$  זה אומר שיש תת־קבוצה סופית של פסוקים ב- $F$  שמתוכם מוכיחים אותה, כי הוכחה היא תמיד סופית, ולכן מצאנו תת־קבוצה סופית של  $F$  שהיא לא עקבית, בסתירה.

לכן, מתוך כל אלה אנחנו יכולים להסיק גרירה נוספת: ל- $F$  אינסופית יש מודל אמ"מ לכל תת־קבוצה סופית של  $F$  יש מודל.

אפשר לראות את זה בצורה ויזואלית בטבלה:

אינסופי	סופי	
$F$ עקבית	כל תת־קבוצה סופית של $F$ עקבית	<b>סינטקס</b>
ל- $F$ יש מודל	לכל תת־קבוצה סופית של $F$ יש מודל	<b>סמנטיקה</b>

קיבלנו את משפט הקומפקטיות כפי שהגדרנו אותו.

הגענו למשפט לא טריוויאלי מתוך הדברים שכבר הוכחנו. ראינו שמתוך זה שאנחנו יודעים שמבחינה סינטקטית סופי ואינסופי מתנהגים אותו הדבר, קיבלנו שגם מבחינת סמנטיקה הם אותו הדבר.

## 8 שיעור 8 – 10.12.17

### 8.1 משפט הקומפקטיות בתחשיב הפסוקים – המשך

לפני שנחזור לתחשיב הפרדיקטים, נדבר עוד קצת על תחשיב הפסוקים. בשיעור הקודם הגענו לגולת הכותרת של החלק הראשון, והיו לנו שני משפטים:

✎ **משפט השלמות (לתחשיב הפסוקים)** – לכל קבוצה עקבית של פסוקים יש מודל.

✎ **משפט הקומפקטיות (לתחשיב הפסוקים)** – לקבוצת פסוקים יש מודל אם"מ לכל תת-קבוצה סופית שלה יש מודל.

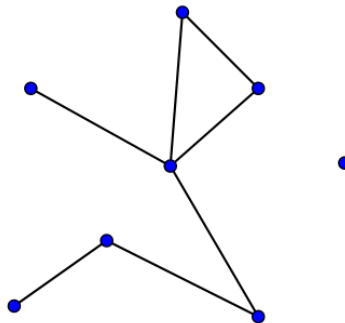
משפט השלמות מחבר בין הסינטקסט לסמנטיקה, ואומר שעקביות גוררת קיום של מודל.

נשים לב לנקודה מעניינת שנוגעת למשפט הקומפקטיות – ברור שאם לקבוצת פסוקים יש מודל אז גם לכל תת-קבוצה שלה יש מודל (אותו המודל), אבל המשפט הזה מבטיח לנו גם את הכיוון הפחות ברור, והוא שאם לתת-קבוצות יש מודל אז גם לקבוצה כולה. זה אומר שאם יש לנו קבוצה אינסופית מספיק לבדוק את תת-הקבוצות הסופיות שלה, ואם לכולן יש מודל זה מבטיח מודל לכל אינסוף הפסוקים בקבוצה הגדולה.

נדון עכשיו בשני נושאים שלא נכנסו אליהם – דוגמא למה מעניין במשפט הקומפקטיות, דוגמא לשימוש, ומשם ננסה להמשיך את הדוגמא ונדון באינסופים של פסוקים, בגדלים שונים של אינסוף כדי לסגור את זה.

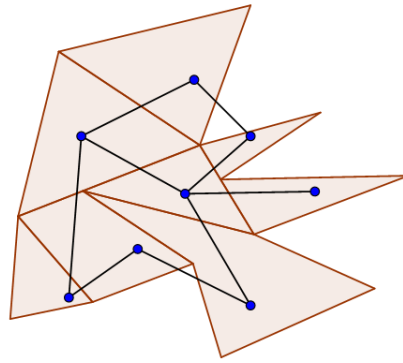
#### 8.1.1 דוגמא שימושית למשפט הקומפקטיות

נרצה לראות עכשיו דוגמא שבה משפט הקומפקטיות יבוא לידי שימוש. לצורך זה, נדבר על **צביעה של גרפים אינסופיים**. כזכור, גרף מורכב מקדקודים ונקודות, לדוגמא:



בבעיות של צביעת קדקודים נרצה לבחור סט של צבעים (כמות הצבעים שנקח תלויה בבעיה) ולתת צבע לכל קדקוד בגרף, כך שאסור ששני קדקודים שיש ביניהם צלע יהיו באותו הצבע.

צביעה של גרפים קשורה להרבה בעיות אחרות שאנחנו נתקלים בהן במדעי המחשב. לדוגמא, **בעיית צביעת המפות**: נחשוב על הקדקודים כאילו הם מייצגים חלקים במישור, ועל הצלעות כאילו הן מייצגות שכנויות בין החלקים האלה. איור להמחשה:



משפט מפורסם שקשור לצביעה של גרפים אומר שכל גרף מישורי (כלומר שיכול להוצר ע"י חלוקה של המישור לחלקים) אפשר לצבוע בארבעה צבעים.

לפי האיורים נראה שהגרפים סופיים, בעצם אפשר לחשוב לא רק על גרף סופי, אלא על אינסופי. גרף מורכב קבוצה של קדקודים וקבוצה של צלעות, אז נוכל לקחת את קבוצת הקדקודים להיות אינסופית, או את קבוצת הקדקודים וגם את קבוצת הצלעות להיות אינסופיות. לדוגמא, אפשר לקחת בתור קדקודים את המספרים הטבעיים, ולחבר אותם לפי כלל (למשל, בין שני מספרים יהיה צלע אם הסכום שלהם זוגי), והגרף שמתקבל הוא אינסופי. באותה מידה, אם מסתכלים על מישור אפשר לחשוב על חלוקה אינסופית של המישור.

נחשוב על בעיית הצביעה בקונטקסט של גרף אינסופי – יש גרף אינסופי, ואנחנו רוצים לצבוע אותו בשלושה צבעים כך שכל שני קדקודים שמחוברים אחד לשני לא יהיו באותו צבע. נסתכל על גרף מישורי שמורכב ממספר אינסופי של חלקים. האם זה עדיין נכון שאפשר לצבוע אותו בארבעה צבעים? את התשובה נקבל ממשפט הקומפקטיות, שבאמצעותו נוכל להוכיח את המשפט הבא –

**משפט** – אפשר לצבוע גרף אינסופי ב- $k$  צבעים אם"מ אפשר לצבוע כל תת-גרף סופי שלו ב- $k$  צבעים.

המשפט מדבר על צביעה של גרפים, והוא נשמע כמו משהו שקשור לקומבינטוריקה אינסופית, לצבעים או למפות, אבל אנחנו נראה שאנחנו מצליחים לקבל את ההוכחה של המשפט הזה "בחינם" באמצעות משפט הקומפקטיות, מבלי להדרש להבין את ההוכחה של משפט ארבעת הצבעים או לדבר על תכונות של מפות.

המשפט טוען שכל מה שצריך לעשות כדי לדעת אם יש צביעה חוקית בגרף אינסופי הוא לבדוק האם היא קיימת לגבי גרפים סופיים, שהם תתי-גרפים של הגרף האינסופי. בפרט, נחזור לגרף האינסופי המישורי שלנו ונסתכל על תתי-גרפים שנוצרים ע"י החלוקה של המישור. הרעיון של הוכחת המשפט יהיה כזה: לפי משפט ארבעת הצבעים, כל גרף סופי אפשר לצבוע בארבעה צבעים, לכן גם את הגרף האינסופי שלנו אפשר לצבוע בארבעה צבעים ממשפט הקומפקטיות.

זה כבר רומז לנו על העבודה שלמשפטים בלוגיקה יש השלכות רחבות על כל דבר שאפשר לעשות במתמטיקה. מה שחסר לנו כאן הוא להראות באיזה אופן אפשר להחיל את משפט הקומפקטיות על גרפים אינסופיים וצבעים, כלומר להראות איך אנחנו ממשיכים את הצביעות ללוגיקה של תחשיב הפסוקים.

**הוכחת המשפט** (עבור  $k = 3$ ) –

בשלב הראשון, נראה איך אנחנו מעבירים את הבעיה משפה של גרפים וצבעים לשפה של תחשיב הפסוקים. נראה זאת עבור  $k = 3$ , אבל באותו אופן יכולנו לעשות זאת עבור מספר  $k$  כללי כלשהו.

לכל קדקוד  $i$  נייצר שלושה משתנים:

- $p_i$ , שאומר שהקדקוד ה- $i$  צבוע בכחול.
- $q_i$ , שאומר שהקדקוד ה- $i$  צבוע באדום.
- $r_i$ , שאומר שהקדקוד ה- $i$  צבוע בירוק.

אנחנו רוצים ש- $p_i, r_i, q_i$  יהיו מודל של הגרף אמ"מ הם צביעה טובה, לכן נבנה קבוצת פסוקים בתחשיב הפסוקים שהיה לה מודל אמ"מ לגרף הזה יש צביעה, והמשתנים שלה יהיו  $p_i, q_i, r_i$  של כל הקדקודים. נשים לב שאם יש מספר סופי של קדקודים בגרף, זה גורר שיהיה מספר אינסופי של משתנים (שלוש פעמים מספר הקדקודים).

בשביל שקבוצת הפסוקים תייצג את הגרף כמו שצריך, נצטרך לאכוף שני דברים –

- לכל קדקוד יש צבע אחד בדיוק: זה אומר שעבור כל קדקוד  $i$  נוסיף את הפסוקים –
  - לכל קדקוד יש צבע

$$(p_i | (q_i | r_i))$$

- לכל קדקוד אין יותר מצבע אחד

$$(p_i \rightarrow \sim q_i)$$

$$(p_i \rightarrow \sim r_i)$$

$$(q_i \rightarrow \sim p_i)$$

$$(q_i \rightarrow \sim r_i)$$

$$(r_i \rightarrow \sim p_i)$$

$$(r_i \rightarrow \sim q_i)$$

- שני קדקודים סמוכים לא יכולים להיות באותו צבע: לכל צלע  $(i, j)$  –

$$\sim(p_i \& q_j)$$

$$\sim(p_i \& r_j)$$

$$\sim(q_i \& r_j)$$

בשלב השני, נקח גרף עם קבוצה סופית של קדקודים ונבצע עבודה את הבנייה. נטען עכשיו שיש לאוסף הפסוקים האלה שבנינו מודל אמ"מ יש צביעה חוקית בגרף.

- הוכחת הכיוון צביעה  $\Leftarrow$  מודל – נניח שיש צביעה בגרף. נבנה את המודל:

- אם הקדקוד ה- $i$  כחול אז  $q_i = T, p_i = F, r_i = F$

- אם הקדקוד ה- $i$  אדום אז  $q_i = F, p_i = T, r_i = F$

- אם הקדקוד ה- $i$  ירוק אז  $q_i = F, p_i = F, r_i = T$

וברור מחוקיות הצביעה שהמודל מקיים את הפסוקים שהגדרנו.

- הוכחת הכיוון מודל  $\Leftarrow$  צביעה – נניח שכל הפסוקים מתקיימים. אז, לפי הבנייה שעשינו של הפסוקים, לכל קדקוד  $i$  בהכרח מתקיים שאחד מהמשתנים  $\{p_i, q_i, r_i\}$  הוא אמת והשניים האחרים שקר. נקח צביעה שמתאימה לזה, ונקבל שזו צביעה חוקית כי שני התנאים לצביעה חוקית מתקיימים בה מחוקיות המודל (גם לכל קדקוד יהיה צבע אחד בדיוק, וגם אין שני שכנים באותו הצבע. אם אחד מהם לא היה מתקיים אז המודל כפי שבנינו אותו לא היה חוקי, וזו סתירה).

עכשיו נותר רק החלק האחרון של ההוכחה, והוא שימוש במשפט הקומפקטיות כדי להוכיח את המשפט שלנו (שהוא, כזכור, שאפשר לצבוע כל גרף אינסופי בשלושה צבעים אמ"מ אפשר לצבוע כל תת-גרף סופי שלו בשלושה צבעים). עבור גרף אינסופי כלשהו:

- נבנה ממנו קבוצת פסוקים בהתאם למה שעשינו בשלב הראשון.
- נשאל את עצמינו האם אפשר לצבוע כל תת-גרף סופי שלו במספר צבעים (למשל אם היינו מסתכלים על ארבעה צבעים ולא שלושה, היינו יכולים להוכיח את החלק הזה באמצעות משפט ארבעת הצבעים). כמו שראינו בהוכחה שבשלב השני, זה שקול לשאול האם לגרף יש מודל.
- בגלל הגרירה הזאת מהשלב השני, זה אומר שאפשר להשתמש במשפט הקומפקטיות על הפסוקים שבנינו, ולקבל שלפסוקים של הגרף האינסופי יש מודל רק אם לפסוקים של תתי-הגרפים שלו יש מודל.
- שוב, לפי הגרירה מהשלב השני, נקבל שלגרף הגדול יש צביעה חוקית רק אם לכל אחד מתתי-הגרפים שלו יש צביעה חוקית.

בכך הוכחנו את הכיוון של המשפט שלנו שאומר שאפשר לצבוע גרף אינסופי ב- $k$  צבעים אם אפשר לצבוע כל תת-גרף סופי שלו ב- $k$  צבעים. כאמור, הכיוון השני טריוויאלי (אם יש צביעה חוקית לגרף כולו נשתמש באותה צביעה לכל תת-גרף עבור הקדקודים המתאימים לו, ונקבל צביעה שגם היא חוקית), ובכך סיימנו את ההוכחה.

המשפט שהוכחנו הוא מאוד כללי, כי צביעות של גרפים יכולות לקודד הרבה דברים שונים במדעי-המחשב. באופן כללי, כל עוד התנאים הם לוקאליים (תנאים מהסוג של תנאי על שכנות של קדקודים), הלוגיקה מבטיחה שאפשר לעבור מהאינסופי לסופי.

## 8.1.2 בעיית צביעת המישור וסוגים שונים של אינסוף

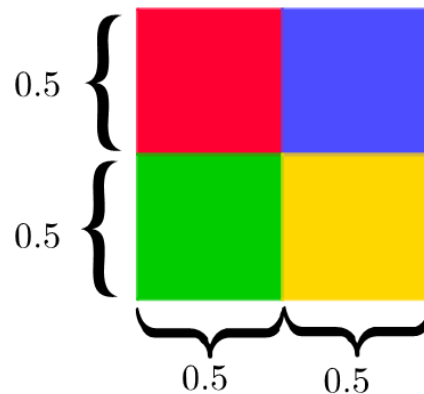
בכל הלוגיקה שעשינו עד עכשיו עדיין חסרה התייחסות יותר נקודתית לנקודה עדינה, שאותה נראה דרך דוגמא נוספת שקשורה לצביעה.

בעיה חדשה – נקח מישור בגודל מסויים, למשל  $100 \times 100$ , וכל נקודה על המישור נבצע באחד מהצבעים אדום, ירוק, כחול וצהוב  $(R, G, B, Y)$ . צביעה חוקית תהיה כזאת שבה לכל שתי נקודות שהמרחק האוקלידי שלהן הוא בדיוק 1 אין את אותו הצבע.

נשים לב שהצבעים עכשיו הם לא של איזורים מוגדרים מראש בגרף או של קדקודים, אלא של נקודות על פני המישור. בניסוח יותר מתמטי, זה אומר שאם המישור הוא בגודל של  $r^2$  למשל, פונקציית הצביעה תהיה פונקציה מהצורה  $r \times r \rightarrow \{R, G, B, Y\}$ .

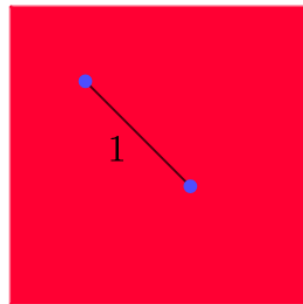
דוגמאות לצביעות חוקיות ובלתי חוקיות בגרף בגודל  $1 \times 1$  –

דוגמא לצביעה חוקית:



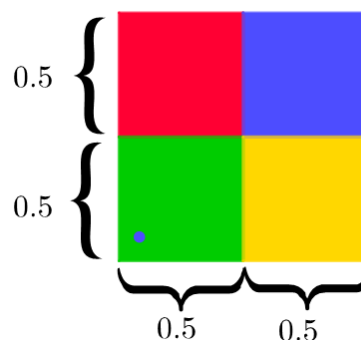
נשים לב שאין שתי נקודות בגרף שהן באותו צבע והמרחק ביניהן גדול מ-1 (כל שתי נקודות בעלות אותו הצבע נמצאות במרחק  $< 0.8$  אחת מהשנייה).

דוגמא לצביעה בלתי חוקית:



בגרף הזה כל הנקודות צבועות באדום, חוץ משתי נקודות שצבועות בכחול. הנקודות שצבועות בכחול נמצאות בדיוק במרחק 1 אחת מהשנייה, לכן הצביעה בלתי חוקית.

דוגמא נוספת לצביעה בלתי חוקית:



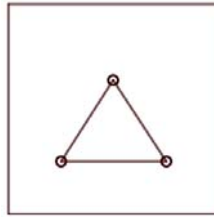
קיימות נקודות באיזור שצבוע כחול שהן בדיוק במרחק 1 מהנקודה הכחולה התחתונה, ולכן הצביעה לא חוקית.

נשאלת השאלה לכמה צבעים אנחנו זקוקים כדי לצבוע את המישור<sup>9</sup>.

<sup>9</sup> [https://en.wikipedia.org/wiki/Hadwiger%E2%80%93Nelson\\_problem](https://en.wikipedia.org/wiki/Hadwiger%E2%80%93Nelson_problem)

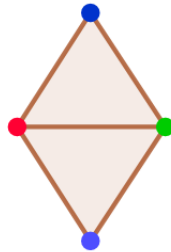


נטען שחייבים לפחות שלושה צבעים. בשביל להראות את זה, נסתכל על משולש שווה-צלעות במישור שאורך הצלע שלו הוא 1:

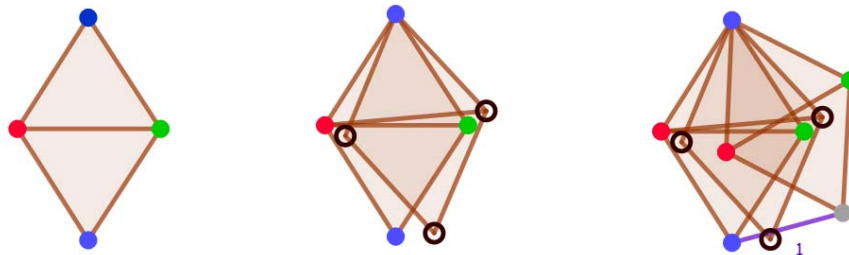


אם היו לנו רק שני צבעים, ברגע שהיינו צובעים שתיים מהנקודות בצבעים האלה לא היה לנו צבע לצבוע איתו את השלישית, כי היא הייתה במרחק 1 משתי הצלעות שכבר צבענו. לכן, חייבים לפחות שלושה צבעים.

באופן דומה, אפשר להראות שגם שלושה צבעים לא מספיקים. נניח שהם כן מספיקים. נקח את המשולש שווה הצלעות שלנו, ונשכפל אותו כך שיוצרו שני משולשים צמודים שביחד יהוו מעוין:



נשים לב שהקדקוד החדש שהוספנו חייב להיות צבוע באותו הצבע של הקדקוד הנגדי לו, כי גם הוא נמצא במרחק 1 משני קדקודי הבסיס. נקח את המעוין הזה, ונתחיל לסובב אותו עד שהקדקוד התחתון ביותר יהיה במרחק 1 מהקדקוד התחתון ביותר של המשולש המקורי:



נשאל את עצמנו באיזה צבע צריך לצבוע את הקדקוד התחתון של המעוין המסובב (מסומן באיור באפור). לא נוכל לצבוע אותו בירוק או באדום, כי הוא נמצא במרחק 1 משני הקדקודים של המעוין שאלה הצבעים שלהם (שחייבים להיות הצבעים שלהם כי הקדקוד העליון כופה את זה). אולם, הוא גם לא יכול להיות בצבע כחול, כי יש נקודה מהמעוין המקורי שלנו שהיא בצבע כחול ובמרחק 1 ממנו (זה המרחק שמסומן באיור בסגול). לכן, גם שלושה צבעים לא יספיקו, ונזדקק לפחות לארבעה.

הבעיה של כמות הקדקודים המינימלית שדרושה לצורך צביעה היא בעיה פתוחה. הוכיחו שאפשר לצבוע הכל באמצעות שבעה צבעים, אבל יתכן שאפשר להסתפק גם בפחות. אנחנו לא נראה כאן דוגמא של שבעה צבעים, אבל כן נתאר איך אפשר לצבוע למשל את כל המישור בתשעה צבעים:

- נחלק את המישור כולו לקוביות בגודל  $0.6 \times 0.6$ .
- נקח בלוק של תשע קוביות, ונצבע כל קובייה בו בצבע אחר.

- נחזור על הצביעה של הבלוק הזה עבור כל המישור.

באופן כזה נקבל שאין שתי נקודות באותו צבע שמרחקן אחת מהשנייה הוא 1, כי המרחק המינימלי בין שתי נקודות באותו הצבע יהיה של שתי משבצות שהוא 1.2.

מה שעשינו קודם כדי לפסול מספר מסויימת של צבעים הוא לתת דוגמא שבה צריך יותר צבעים, מה שמוכיח שצריך יותר צבעים במקרה הכללי. היינו רוצים להגיד שאם אי אפשר אז גם חייבת להיות דוגמא קטנה שמראה שאי אפשר. המשפט שנותן לנו את זה הוא משפט הקומפקטיות – המשפט הזה אומר לנו מידית שאם אי אפשר לצבוע את כל המישור במספר מסויים של צבעים אז בהכרח קיים גרף סופי שיוכיח את זה, שהוא תת-גרף כלשהו של הגרף הזה (כי אם כל תתי-הגרף של הגרף הזה היו ניתנים לצביעה במספר הצבעים הזה, ממשפט הקומפקטיות גם הגרף כולו היה). זה לא דווקא מאוד עוזר לנו תמיד, אבל זה כן נותן לנו מושג שתמיד נוכל למצוא דוגמא נגדית סופית במקרים של אי קיום.

בתרגום לפסוקים של גרפים אינסופיים יש נקודה עדינה שעד כה התעלמנו ממנה – נחשוב כמה פסוקים מתקבלים בכל תרגום של גרף. אם נקח נגיד את בעיית הנקודות במישור שצריך לצבוע, לכל נקודה במישור  $i$  אנחנו מתאימים ארבעה משתנים, אחד לכל צבע. הנקודות במישור הם צמדים של מספרים ממשיים  $x, y$ , כלומר  $i = (x, y)$ . עד כה בכל מה שעשינו בקורס שמות של פסוקים כללו רק מספרים שלמים ( $p_1, p_2, p_{54}$  וכו'), ופתאום אנחנו רוצים להעניק גם שמות לנקודות של מספרים ממשיים (נניח  $i = (\pi, 4.2)$ ). מה קורה כאן?

כדי להמשיך את הדיון הזה, נדבר קודם כל קצת באופן כללי על קבוצות אינסופיות –

לא כל הקבוצות האינסופיות הן אותו דבר, יש קבוצות שנחשבות יותר גדולות או יותר קטנות. המצב האינסופי יותר מסובך מאשר בקבוצות סופיות.

לדוגמא – מה יש יותר, מספרים טבעיים או זוגיים? תשובה נאיבית תהיה שיש פחות זוגיים מטבעיים, כי כל מספר זוגי הוא טבעי אבל לא להפך, אבל בפועל מבחינה מתמטית יש אותו מספר. אפשר להראות את זה ע"י בניית מיפוי: בונים פונקציה חח"ע ועל מקבוצת הטבעיים לקבוצת הזוגיים (לדוגמא פונקציה שממפה כל מספר  $n \in \mathbb{N}$  למספר  $2n$ ).

מסתבר שגם מספרים רציונליים הם בעלי אותה עצמה כמו הטבעיים<sup>10</sup>. אולם, קנטור גילה שלא כל האינסופים הם אותו הדבר, ושלא תמיד נוכל למפות בין כל שתי קבוצות אינסופיות<sup>11</sup>. בפרט, הוא הראה שאין פונקציה חח"ע ועל מהטבעיים לממשיים (קבוצת הממשיים "גדולה" מקבוצת הטבעיים)<sup>12</sup>.

מה העצמה של אינסוף הפסוקים אצלינו? האינסוף הוא בן מנייה (כלומר מאותה עצמה של המספרים הטבעיים), כי כל פסוק הוא באורך סופי ומעל א"ב סופי. קבוצת המספרים הממשיים היא לא בת מנייה, לכן (אם נחזור לבעיה של תרגום הנקודות על המישור לפסוקים) אין דרך בשפה שלנו אפילו רק לתת שם משתנה לכל נקודה במרחב. כל הלוגיקה שתכנתנו להתמודד רק עם בדברים שלהם מספר בן מנייה של פסוקיות אטומיות.

אולם, אם היינו מטפלים מלכתחילה במתמטיקה שלנו בצורה קצת אחרת, היינו מקבלים תוצאה שמאפשרת לנו להתמודד עם זה מבחינה מתמטית. בשיעור הראשון, כשהגדרנו מהי נוסחא בנוייה היטב, אמרנו מה הצורה של פסוקים מותרים. אפשר היה גם להגדיר את הנוסחא באופן אחר – הגדרה מעל קבוצת פסוקיות  $X$ , שמשמעותה שכל דבר בקבוצה  $X$  יכול להיות פסוק. בהגדרה הזאת של מהי נוסחא, אין שום בעיה – נקח את  $X = \{p_{\alpha, \beta}\}$  עבור כל  $\alpha, \beta \in \mathbb{R}$ . את הלוגיקה שנובעת מזה אי אפשר לכתוב בסטרינגים סופיים, אבל היא כן תסתדר מבחינה מתמטית עם מה שאנחנו רוצים לעשות במישור.

<sup>10</sup> לקריאה בנושא:

<https://math.stackexchange.com/questions/7643/produce-an-explicit-bijection-between-rationals-and-naturals>

<sup>11</sup> [https://en.wikipedia.org/wiki/Cantor%27s\\_theorem](https://en.wikipedia.org/wiki/Cantor%27s_theorem)

<sup>12</sup> [https://en.wikipedia.org/wiki/Cantor%27s\\_diagonal\\_argument](https://en.wikipedia.org/wiki/Cantor%27s_diagonal_argument)

אם יש מספר גדול של פסוקיות, בפרט לא בן מנייה, גם אוסף הנוסחאות לא יהיה בן מנייה (כי אפילו הפסוקים עצמם לא בני מנייה), ואז אפשר לעשות את כל הלוגיקה שרצינו לעשות בבעיית הצביעה במישור. את הנקודות הפעם נתרגם לפסוקים כמו שעשינו עד עכשיו, רק שהפעם הפסוקים יהיו מעל הקבוצה X.

ההגדרה החדשה של פסוקים לא משנה לנו כמעט בשום דבר, למעט במקום אחד. המקום הזה הוא ההוכחה של משפט השלמות, שם צעדים מסויימים שעשינו בהוכחה מושפעים מהשינוי. כחלק מההוכחה של משפט השלמות הייתה לנו מטרה של לבנות קבוצה מקסימלית עקבית של פסוקים. איך בנינו קבוצה מקסימלית – לקחנו קבוצה עקבית של פסוקים, והוספנו אליה פסוק בכל פעם כל עוד הוא לא מקלקל את העקביות. זה לא הולך אם מספר הפסוקים הוא לא בן מנייה, כי הרעיון של לעבור איבר-איבר לפי הסדר ולהוסיף כל פעם איבר אחד זה בדיוק מנייה של האיברים.

אולם, מסתבר שאפשר להגיע לקבוצה מקסימלית עקבית של פסוקים גם בקבוצות כלליות (לאו דווקא בנות מנייה). אמנם אי אפשר להוכיח את זה ע"י הוספה אחד אחד, אבל יש דרך אחרת, שהיא הלמה של צורן<sup>13</sup> (שחשוב לציין שהיא שקולה לאקסיומת הבחירה, כלומר כדי לקבל את הדברים שלנו לקבוצות פסוקים שהן לא בנות מנייה צריך לקבל את אקסיומת הבחירה). לא נוכיח את זה. נסתפק בלהגיד שאפשר לעשות את זה, כלומר אם הולכים להוכחה של משפט השלמות ומוותרים על הקטע שמוסיף אחד אחד ורק משתמשים בזה שקיימת קבוצה מקסימלית זה יעבוד.

המסקנה היא שמשפט השלמות והקומפקטיות נכונים לא רק ללוגיקה עם מספר בן מנייה של פסוקיות אטומיות, אלא לתחשיב הפסוקים באופן כללי לכל קבוצת פסוקיות (ההבדל היחידי הוא שעכשיו צריך להיות מוכנים לקבל גם את אקסיומת הבחירה בתור אקסיומה של המתמטיקה).

עכשיו משתיקנו את משפט השלמות ומשפט הקומפקטיות כך שיעבדו גם על קבוצות פסוקים לא בנות מנייה, נחזור לדוגמא שלנו של צבעית המישור, ונחיל את משפט הקומפקטיות כדי להראות שבכל מצב שבו אי אפשר לצבוע את המישור בארבעה צבעים יש גם תת-גרף סופי שאי אפשר לצבוע בארבעה צבעים. נפעיל את משפט הקומפקטיות על קבוצות לא בנות מנייה, ונקבל את התוצאה הזאת.

לסיכום הנושא הזה, הראנו שני דברים –

1. כל מה שלמדנו על קבוצות פסוקים אטומים בנות מנייה נכון גם לקבוצות לא בנות מנייה, בפרט משפט הקומפקטיות ומשפט השלמות (רק עם הוכחה קצת שונה עם אקסיומת הבחירה).
2. ראינו אפליקציה של משפט הקומפקטיות לגרפים אינסופיים: בעיית צביעת המפות, והבעיה הפתוחה של צביעת קדקודים כך שלא יהיו שניים באותו צבע במרחק 1 זה מזה, שם ראינו שאם אי אפשר לצבוע במספר מסויים של צבעים חייבת להיות דוגמא סופית לזה.

## 8.2 תרגיל 8

נחזור עכשיו לתחשיב הפסוקים, ונדבר על דברים שרלוונטים לתרגיל 8.

כשמגדירים פורמט של תחשיב כלשהו, בין אם זה תחשיב הפסוקים או הפרדיקטים, תמיד יש משחק בכמה אנחנו קמצנים בהגדרות שלנו. לדוגמא, אנחנו מתקמצנים בפורמט של  $\&$ , ודורשים סוגריים מסביב לביטויים שכוללים אותם. מצד שני, אפשר גם את  $\&$  וגם את  $\&$  אפילו שלא חייבים את שניהם.

אותו הדבר עם אקסיומות – הוכחנו את תרגיל 6 מקבוצה של 14 אקסיומות, כשבפועל ואפשר היה להורי 5 מהן. הטרייד אף כאן הוא בין פורמט שמספיק דומה למתמטיקה אמיתית, לבין הקלה במידת האפשר על הכתיבה של הקוד. כמובן שבאופן עקרוני זה הכל אותו הדבר, כל הבחירות הן שקולות, ואפשר לעבור מהאחת לשנייה.

<sup>13</sup> [https://en.wikipedia.org/wiki/Zorn%27s\\_lemma](https://en.wikipedia.org/wiki/Zorn%27s_lemma)

היום נדבר על שקיבלנו בתחשיב הפרדיקטים שלא היו חייבים לתת לנו אותם. למה נתנו לנו אותם – כי יהיה יותר נח כשמדברים על מתמטיקה להוכיח דברים עם זה, וגם כי זה הקל על העבודה עד עכשיו. נרצה להפטר מהם כי לפעמים זה יהיה יותר נח, לדוגמא את משפט השלמות נרצה להוכיח על דברים יותר פשוטים שההוכחה תהיה פחות מייגעת.

שני הדברים הלאה הם פונקציות ושיוויון. נראה עכשיו איך לקחת משהו מעולם שיש בו פונקציות ויש בו שיוויון, ולתרגם אותו למשהו שקול בלי פונקציות ובלי שיוויון.

### 8.2.1 פונקציות

מבחינה מתמטית, פונקציה היא מקרה פרטי של יחס. את הפונקציה  $f(x) = y$  אפשר לתרגם ליחס  $R(y, x)$ , כך שכל הזוגות  $(y, x)$  ששייכים ליחס מקיימים  $y = f(x)$   $\Leftrightarrow (y, x) \text{ is True in } R$ . באופן דומה, נוכל לתרגם כל פונקציה שהיא ליחס מתאים.

לדוגמא, נסתכל על הביטוי הבא שכולל פונקציה:

$$\forall x [\exists z [plus(x, z) = 0]]$$

נחליף את הפונקציה ליחס בשלבים הבאים (ההסבר לאחר השלבים):

- במקום הפונקציה  $plus(x, z)$  נקח את היחס  $Plus(y, x, z)$ .
- נדרוש  $(Plus(y, x, z) \rightarrow y = 0)$ .
- נדרוש שהגרירה הזאת תתקיים לכל  $y$ .
- נקבל:

$$\forall x [\exists z [\forall y [Plus(y, x, z) \rightarrow y = 0]]]$$

הסבר:

- בשלב הראשון, עשינו החלפה של הפונקציה על שני משתנים ליחס על שלושה משתנים. באופן כללי, נקודד כל פונקציה על  $k$  משתנים ליחס על  $k + 1$  משתנים, שבו האיבר הראשון בקלט של היחס הוא התוצאה של הפעלת הפונקציה על שאר האיברים. נרצה גם שהשינוי הסינטקטי הזה יעשה בצורה שתשמר את המשמעות, כלומר שהיחס הזה מוגדר כך שהוא מתאים לפונקציה. בפרט, אם יהיה מודל לאחד מהם נרצה שיהיה גם מודל לשני, ואם מודל מסויים מתאים לאחד נרצה שהוא יתאים גם לשני.
- לא מספיק להפעיל את היחס, אנחנו גם רוצים לדרוש שה- $y$  שהוספנו יהיה שווה למה שהפונקציה המקורית אמורה להיות שווה אליו. לכן הוספנו את הגרירה.
- עכשיו נותר להבין את הכמת. ברור שאנחנו צריכים להוסיף משהו לפני הגרירה, כי אחרת  $y$  הוא משתנה חופשי והוא מאבד מהמשמעות שרצינו להעניק לו (שהיא המשמעות שלו כתוצאה של הפונ'). בחרנו דווקא בכמת "לכל" כי אנחנו רוצים שאם הקלט יהיה שייך ליחס, זה בהכרח יאמר שהאיבר הראשון בקלט הוא התוצאה הרצויה של הפעלת הפונקציה על שאר איברי הקלט. הכי קל להבין את זה ע"י דוגמא – נניח שמתקיים  $plus(7, 5) = 0$ . אנחנו רוצים שביחס שנגדיר הביטוי  $Plus(0, 7, 5)$  יהיה שייך ליחס, וכל ביטוי דומה שכולל מספר אחר במקום אפס (לדוגמא  $Plus(1, 7, 5)$ ,  $Plus(2, 7, 5)$  וכו') לא יהיה שייך ליחס. זה בדיוק אומר שאנחנו דורשים לעבור אחד אחד על כל האיברים בעולם, ובכל פעם ששלשה של מספרים היה שייכת ליחס זה בהכרח אומר שהאיבר הראשון בתוכה היה 0 (הרי אנחנו רוצים שרק  $Plus(0, 7, 5)$  יהיה ביחס, ולכל  $y \neq 0$  הביטוי  $Plus(y, 7, 5)$  לא יהיה ביחס). לכן, נדרוש שהגרירה הזאת תתקיים עבור כל איבר בעולם. בפרט, נשים לב שהכמת "קיים" לא היה עובד כאן. כיוון שקיים  $y$  כך ש- $Plus(y, 7, 5)$  הוא ביחס,  $y = 0$  אז היינו מקבלים ערך אמת לביטוי כולו גם אם  $(1, 7, 5)$  היה גם ביחס, וזה לא מייצג לנו את הפונקציה, שמחזירה תוצאה אחת בדיוק עבור כל קלט.

לאחר שבחנו את הדוגמא הזאת לעומק, נדבר על מה הוא באופן כללי התהליך שאנחנו הולכים לעשות:

הולך להיות לנו עולם דו־צדדי, בצד אחד עולם עם פונקציות ובצד שני בלי. לכל פונקציה  $f(x_1, \dots, x_n)$  נתאים יחס  $F(y, x_1, \dots, x_n)$ , כשהמשמעות של זה היא ש- $y = f(x_1, \dots, x_n)$ . זו התאמה לוגית גם מבחינת המודלים וגם מבחינת הנוסחא, גם מבחינת הסינטקס וגם מבחינה הסמנטיקה, שיוצרת התאמה בין שניהם.

עם פונקציות		בלי פונקציות
$f(x_1, \dots, x_n)$	$\longleftrightarrow$	$F(y, x_1, \dots, x_n)$
נוסחא	$\longrightarrow$	נוסחא
מודל	$\longleftrightarrow$	מודל

הולכים להיות שלושה תרגילים שמטפלים בדבר הזה:

1. סינטקס – להפוך נוסחא בעולם בלי פונקציות לנוסחא בעולם עם פונקציות.
2. להראות שמבחינת המודלים הכל בסדר, כלומר לקחת מודל בכל עולם ולהראות:
  - a. איך בונים ממודל עם פונקציות מודל בלי פונקציות (בפרט רצוי שיקיימו את הנוסחא אמ"מ השני מקיים).
  - b. להראות תרגום ממודל בלי פונקציות למודל עם פונקציות, כדי לראות שלא התווספו לנו מודלים חדשים שלא מתאימים.

בשביל להפוך מודל עם פונקציות לבלי פונקציות נקבל את המשמעות של הפונקציות, ונצור יחס בדיוק באותה צורה כמו שעשינו עבור  $plus \rightarrow plus$ . נשים לב שכדי שהיחס שהתקבל באמת יתאים לפונקציה צריך שלכל סט של ביטויים  $x_1, \dots, x_n$  שהם קלט לפונקציה יהיה רק  $y$  אחד שיקיים ש- $(y, x_1, \dots, x_n)$  שייך ליחס.

מבחינת הכיוון השני, צריך לוודא שלא הוספנו מודלים חדשים בעולם הזה. יגידו לנו אילו יחסים רוצים שנתרגם מחדש להיות פונקציות, וכל עוד היחס מתאים להיות פונקציה (צריך לוודא את זה) אפשר לתרגם אותו חזרה באופן דומה למה שעשינו כאן, רק הפוך.

השאלה היותר קשה היא איך עושים את התרגום מנוסחא עם פונקציה לנוסחא בלי.

לדוגמא, נסתכל על  $R(f(x))$ . נתרגם אותו לצורה בלי פונקציות באופן הבא:

$$\forall y [F(y, x) \rightarrow R(y)]$$

אנחנו תמיד מוסיפים משתנה חדש  $y$  שיקבל את הערך של הפונקציה שאנחנו רוצים להעלים, ודואגים שרק כשהמשתנה החדש הוא באמת הערך של הפונקציה אז הקלט יהיה שייך ליחס, ואז היחס החדש שהגדרנו יעבוד.

בנוסף, כדי להבטיח ש- $F$  הוא יחס שבאמת מתאים לפונקציה, אז ממה שנעשה לכל פסוק נצטרך להוסיף עוד פסוקים שדואגים ש- $F$  באמת יתאים ל- $f$ . מה צריך לעשות –

1. להבטיח שלכל  $x$  יש  $y$  שמתאים לו:

$$\forall x [\exists y [F(x, y)]]$$

2. להבטיח שיש רק  $y$  אחד שמתאים לכל  $x$ :

$$\forall x \left[ \forall y_1 \left[ \forall y_2 \left[ ((F(y_1, x) \& F(y_2, x)) \rightarrow y_1 = y_2) \right] \right] \right]$$

מלבד ההתאמה של היחס לפונקציה, יש כאן עוד קושי, המיקום של  $R(f(x))$  בתוך הנוסחא הכללית.

$R(f(x))$  זה רק חלק אחד של הנוסחא, אבל את זה עושים רגיל ברקורסיה. החלק היותר מסובך זה מה יכול להיות בתוך  $R$ , לדוגמא:

$$R(f(g(1), h(0, u))s(w))$$

המשימה שלנו היא לתרגם זה יהיה כמו שקומפיילר היה עושה – מבפנים החוצה. נתרגם כל ביטוי מהנוסחא הזו לפי הסדר הבא:

$$\begin{aligned} z_1 &= g(1) \\ z_2 &= h(0, u) \\ z_3 &= f(z_1, z_2) \\ z_4 &= s(w) \\ R(z_3, z_4) \end{aligned}$$

נתרגם כל הפעלה של פונקציה לנוסחא:

$$\begin{aligned} z_1 &= g(1) \Rightarrow G(z_1, 1) \\ z_2 &= h(0, u) \Rightarrow H(z_2, 0, u) \\ z_3 &= f(z_1, z_2) \Rightarrow F(z_3, z_1, z_2) \\ z_4 &= s(w) \Rightarrow S(z_4, w) \end{aligned}$$

ונקבל  $R(z_3, z_4)$ .

עכשיו, התרגום של זה לנוסחא יהיה:

$$\forall z_1 \left[ \forall z_2 \left[ \forall z_3 \left[ \forall z_4 \left[ ((G(z_1, 1) \& H(z_2, 0, u) \& \dots) \rightarrow R(z_3, z_4)) \right] \right] \right] \right]$$

זה בדיוק סוג החישובים שקומפיילר עושה. באופן כללי, יש שתי דרכים לעשות קומפילציה – אחת זה להכניס את הערכים למחשנית<sup>14</sup>, והשנייה זה להגיד לאיזה רגיסטרים מכניסים את תוצאות הביניים, והקומפיילר מנהל את הרגיסטרים לבד. מה שאנחנו עושים כאן זה כמו הדרך השנייה, ואצלינו אין בעיה, כי יש לנו אינסוף רגיסטרים  $(z_1, z_2, z_3, \dots)$ .

בזאת סיימנו להראות דרך שקולה לפונקציות.

## 8.2.2 יחס השיוויון

נותר לנו לראות איך מחליפים את יחס השיוויון. נסתכל לדוגמא על:

$$\forall x [\exists y [x = y \rightarrow \dots]]$$

נתחיל מלשאול את עצמינו למה בכלל הוגדרה שיוויון כחלק מהלוגיקה של השפה, שהרי שיוויון זה מקרה פרטי של יחס. אם חיבור למשל לא הגדרנו בצורה מיוחדת, למה דווקא שיוויון הוגדר בנפרד? את התשובה לשאלה הזאת נקבל בהמשך.

באופן כללי, הצורה שבה נחליף את השיוויון היא ע"י הכנסת יחס מתאים, שנקרא לו  $SAME$ . בכל מקום שבו נראה  $x = y$  נחליף את זה פשוט ב- $SAME(x, y)$ . נשים לב ששיוויון היה מילה שמורה בלוגיקה, אבל היחס הזה הוא לא.

בינתיים  $SAME$  הוא סתם יחס, וצריך להגדיר לו את התכונות שיבטיחו שהוא אכן יהיה יחס השיוויון. התכונות הן:

1. רפלקסיביות –

$$SAME(x, x)$$

2. סימטריה –

<sup>14</sup> כמו שעושים בקורס *Nand to Tetris*.

$$(SAME(x, y) \rightarrow SAME(y, x))$$

3. טרנזיטיביות –

$$((SAME(x, y) \& SAME(y, z)) \rightarrow SAME(x, z))$$

בשביל להבטיח ש- $SAME$  יעשה מה שאנחנו רוצים, נצטרך שכל הביטויים האלה יקבלו ערך אמת.

יש עוד תכונה של יחס השיוויון שעוד לא תפסנו כאן – אם שני ביטויים שווים, יש להם אותו מודל. זה אומר ש- $SAME$  צריך להתאים גם לשאר היחסים. כלומר, צריך שלכל יחס  $R(x_1, \dots, x_k)$  יתקיים:

$$((SAME(x_1, y_1) \& (SAME(x_2, y_2) \& \dots \& SAME(x_k, y_k))) \rightarrow (R(x_1, \dots, x_k) \rightarrow R(y_1, \dots, y_k)))$$

אולם, נשים לב שזה עדיין לא מספיק על מנת לתפוס את המהות של השיוויון במלואה. אם מתקיים  $x = y$  אז בהכרח  $x$  ו- $y$  הם אותו איבר בעולם, אבל  $SAME(x, y)$  לא מחייב את זה. כל מה שעשינו עד עכשיו הכריח את  $x$  ו- $y$  להתנהג אותו הדבר, לא גרם להם להיות אותו האיבר.

דוגמא להמחשה – ראשית, נסתכל על:

$$\forall x [\forall y [x = y]]$$

מה אפשר להגיד על עולם שמקיים את הביטוי הזה – יש בו רק איבר אחד, אחרת היה אפשר לקחת את  $x$  ו- $y$  להיות שני איברים שונים, והביטוי לא היה מתקיים בעולם הזה.

כעת, נסתכל על:

$$\forall x [\forall y [SAME(x, y)]]$$

עכשיו לא בהכרח יש רק איבר אחד בעולם. לדוגמא, נסתכל על העולם הבא עם הגדרת היחס הבאה:

$$u = \{1, 2\}$$

$$SAME = \{(1, 1), (2, 2), (1, 2), (2, 1)\}$$

וכאן בדיוק בא לידי ביטוי ההבדל – במקרה הראשון, יכולנו להסיק שמדובר על אותו איבר ממש מהעולם, ואילו במקרה השני זה לא דווקא אותו האיבר.

בלי יחס השיוויון המפורש, שיוויון על שני איברים לא יגרור בהכרח שהם בדיוק אותו האיבר, וזו בדיוק הנקודה שבגללה יחס השיוויון הוגדר מלכתחילה בנפרד. אולם, גם אם אי אפשר לעשות את זה במדויק, אפשר כמעט לעשות את זה, והכמעט הזה יספיק לנו.

נסתכל על הדוגמא, ונבין למה בכל זאת המודל השני כן מתאים לנו – מבחינתנו, אפשר פשוט להתייחס ל-1 ו-2 בעולם הזה כאילו הם אותו האיבר. אפשר לעשות את זה כי הם  $SAME$  אחד של השני, ולכל אחד מהיחסים הם מתנהגים אותו הדבר. לכן, הם באמת מתנהגים לכל דבר ועניין כאותו האיבר, ונוכל להתייחס אליהם כאל איבר אחד.

בניסוח מתמטי – היחס  $SAME$  הוא יחס שקילות. זה אומר שהוא מחלק את העולם למחלקות שקילות. כל האיברים באותה מחלקת שקילות מתנהגים באותה דרך עבור היחסים שיש. מכאן נובע שאפשר לקחת מודל בעולם של  $SAME$  ולהעביר אותו להיות מודל בעולם שכולל את יחס השיוויון באופן הבא – נקח מחלקות שקילות של  $SAME$ , ומתוך כל מחלקה נבחר נציג אחד שיהיה איבר בעולם שכולל את יחס השיוויון. קיבלנו שהויתור על השיוויון פשוט אומר שאנחנו צריכים להסתכל על מחלקות שקילות בתור איברים יחידים ולא על האיברים עצמם.

**9 שיעור 9 – 24.12.17****9.1 הוכחות בתחשיב הפרדיקטים**

נתחיל היום לדבר על הוכחות בתחשיב הפרדיקטים. הדבר הראשון שצריך לדבר עליו הוא מהי המערכת האקסיומטית שלנו. אפשר היה לעשות כל מיני בחירות שונות שהיו מאפשרות לנו לעשות מה שאנחנו רוצים, אנחנו נבחר מערכת מסוימת דומה לסטדרנט.

בדומה למה שהיה לנו בתחשיב הפסוקים, המערכת שלנו צריכה להיות כזאת שבאמצעותה נוכל להוכיח (פעולה סינטקטית) רק דברים נכונים (נכונות היא סמנטית) בתחשיב הפרדיקטים, ושכל מה שנכון בתחשיב נוכל להוכיח באמצעותה.

במערכת שלנו יהיו שלושה רכיבים: כללי היסק, "כל הטאוטולוגיות" (של תחשיב הפסוקים) ואקסיומות.

**כללי היסק**

הולכים להיות לנו שני כללי היסק –

**1. מודוס פוננס (MP):**

$$\frac{\varphi, (\varphi \rightarrow \psi)}{\psi}$$

זה MP כפי שאנחנו מכירים אותו, מלבד העובדה שעכשיו הנוסחאות האלה יכולות להיות כל נוסחא בתחשיב הפרדיקטים.

**2. *Universal Generalization (UG)*:**

$$\frac{\varphi}{\forall x[\varphi]}$$

לדוגמא (מקרה פרטי של הכלל):

$$\frac{(F(x) \& G(y))}{\forall z[(F(x) \& G(y))]}$$

**"כל הטאוטולוגיות" (של תחשיב הפסוקים)**

בנוסף לכללי ההיסק, עוד משהו שנוכל להשתמש בו יהיה "כל טאוטולוגיה (של תחשיב הפסוקים)". כלומר, נוכל להשתמש בכל טאוטולוגיה של תחשיב הפסוקים, לדוגמא נקח את הטאוטולוגיה:

$$((p \rightarrow q) \rightarrow p)$$

ונחליט ש- $\forall x[F(x)] \equiv p$  ו- $y = 7 \equiv q$ . נקבל:

$$((\forall x[F(x)] \rightarrow y = 7) \rightarrow \forall x[F(x)])$$

ובזה נוכל להשתמש.

נשים לב שבהחלפה שעשינו, כל אות בתחשיב הפסוקים עמדה בתור נוסחא שלמה בתחשיב הפרדיקטים: במקום המשתנים האטומים, שמנו נוסחאות מתחשיב הפרדיקטים. נוכל לעשות את זה עם כל טאוטולוגיה מתחשיב הפסוקים.

נעיר שטאוטולוגיה זה הרי מונח סמנטי, ואנחנו רוצים לעשות כאן משהו סינטקטי (לבנות הוכחה). איך זה מסתדר? מהחלק הראשון של הקורס אנחנו יודעים לתרגם את כל הסמנטיקה של תחשיב הפסוקים (טבלאות האמת) למשהו סינטקטי, להוכחות. לכן, היינו אמנם יכולים לקחת במקום כל הטאוטולוגיות של תחשיב הפסוקים את כל האקסיומות



של תחשיב הפסוקים וככה לפתור את הבעיה, אבל כבר ראינו שמתוך האקסיומות האלה אפשר להוכיח את כל הטאוטולוגיות. לכן, עם ההבנה שקיבלנו ממשפט השלמות של תחשיב הפסוקים, את "כל טאוטולוגיה" הפכנו כבר בעינינו למשהו סינטקטי. כל טאוטולוגיה של משפט הפסוקים, אפילו שהיא נראית משהו סמנטי, אפשר לתרגם אותה להוכחה מהאקסיומות של תחשיב הפסוקים. כלומר, יש הצדקה טובה להשתמש בטאוטולוגיות, וכדאי לנו לעשות את זה כיוון שזה הולך להקל עלינו מבחינה טכנית.

## אקסיומות

### 1. *Universal Instantiation (UI)*:

$$(\forall x[\varphi(x)] \rightarrow \varphi(\tau))$$

לכל שם עצם  $\tau$  ולכל פסוק  $\varphi$ .

הסבר: האקסיומה הזאת מבטיחה שהמשמעות של הכמת "לכל" היא באמת מה שאנחנו רוצים. במילים אחרות, אם משהו נכון לכל ה- $x$ ים הוא נכון ל- $x$  ספציפי, והדבר הספציפי שמדברים עליו הוא  $\tau$ . כשאנחנו כותבים  $\varphi(\tau)$  אנחנו מניחים שלאחד המשתנים של  $\varphi$  אנחנו מתייחסים בתור הפרמטר שלנו.

דוגמא:

$$(\forall x[F(x, y)] \rightarrow F(g(0, y), y))$$

כאן  $\varphi = F(x, y)$ , ומחליפים אותה בביטוי  $F(g(0, y), y)$ .

הערות על צורות רישום שונות:

- לפעמים רושמים ככה בספרי לוגיקה  $(\forall x[\varphi(\frac{x}{v})] \rightarrow \varphi(\frac{\tau}{v}))$ , כשהכוונה היא  $x$  מחליף את  $v$  ו- $\tau$  מחליף את  $v$ .
- לפעמים ה- $x$  מוצב לתו עצמו, ואז במקום לכתוב  $\varphi(\frac{x}{x})$  כותבים  $\forall x[\varphi(x) \rightarrow \varphi(\frac{\tau}{x})]$ .
- אנחנו נכתוב את זה בצורה יותר תכנותית,  $(\forall x[\varphi(x)] \rightarrow \varphi(\tau))$ , כמו קריאה לפונקציה.

עוד דוגמא:

$$(\forall y[G(y, y)] \rightarrow G(0, 0))$$

כאן  $\varphi(v) \equiv G(v, v)$ , ואז כשמציבים  $y$  בתוך  $\varphi$  יוצא  $\forall y[G(y, y)]$ , וכשמציבים  $\tau = 0$  מתקבל  $G(0, 0)$ .

הערות נוספות:

- יתכן של- $\varphi$  יש עוד משתנים חופשיים. למשל,  $\varphi(v) = F(v, y)$ . עבור הדוגמא הזאת נקבל:  
 $(\forall x[F(x, y)] \rightarrow F(0, y))$
- צריך לשים לב שאסור להציב בתוך  $\varphi$  משתנה חסום. הכוונה היא שאסור לדוגמא לעשות את ההחלפה  $\varphi(v) = F(v, x)$  עבור  $(\forall x[\varphi(x)] \rightarrow \varphi(\tau))$ , כי בסקופ בנוסחא שבו נמצאת  $\varphi$  המשתנה  $x$  הוא משתנה חסום, ובביטוי שאליו מחליפים הכוונה היא ש- $x$  הוא משתנה חופשי (כלומר, ב- $\forall x[\varphi(x)]$  ה- $x$  הוא משתנה חסום, וב- $F(v, x)$  הוא חופשי, לכן זה אסור).

### 2. *Existential Introduction*:

$$(\varphi(\tau) \rightarrow \exists x[\varphi(x)])$$

$\varphi$  הוא כל נוסחא (כמבין שאסור שיהיה לה משתנה חופשי בשם  $x$  חוץ מהפרמטר),  $\tau$  יכול להיות כל שם עצם.

הסבר: זו המשמעות של כמת הקיים.

**3. Universal Simplification**

$$(\forall x[\phi \rightarrow \varphi(x)] \rightarrow (\phi \rightarrow \forall x[\varphi(x)]))$$

הסבר: אם לכל  $x$  מתקיימת הגרירה  $\phi \rightarrow \varphi(x)$  (משהו שלא תלוי ב- $x$  גורר משהו שכן תלוי ב- $x$ ), אז  $\phi$  גורר קיום לכל  $x$  של  $\varphi(x)$ .

הערה: יש לשים לב של- $\phi$  אסור שיהיה את  $x$  בתור משתנה חופשי.

**4. Existential Simplification**

$$((\forall x[(\varphi(x) \rightarrow \phi)] \& \exists x[\varphi(x)]) \rightarrow \phi)$$

הסבר: אם לכל  $x$  מתקיימת הגרירה  $\varphi(x) \rightarrow \phi$  אז נרצה להגיד ש- $\phi$  נכון, אבל נצטרך לדרוש גם שקיים  $x$  כזה  $\exists x[\varphi(x)]$  (כלומר שזה לא נכון רק באופן ריק). אם שני אלה מתקיימים, נוכל כבר להגיד  $\phi$ .

הערה: יש לשים לב של- $\phi$  אסור שיהיה את  $x$  בתור משתנה חופשי.

בנוסף לאלה, יש עוד שתי אקסיומות שקשורות לשיוויון, שעליהן נדבר יותר לעומק בשיעור הבא.

5. אומרת שכל ביטוי שווה לעצמו:

$$\tau = \tau$$

6. מדברת על המשמעות של שיוויון כמו שראינו בשיעור שעבר (כשהחלפנו שיוויון בפונקציה SAME):

$$(\tau = \sigma \rightarrow (\varphi(\tau) \rightarrow \varphi(\sigma)))$$

עם האקסיומות האלה + כללי ההיסק + "כל הטאוטולוגיות" אנחנו הולכים להוכיח דברים.

גולת הכותרת שלקראתה אנחנו מתקדמים היא שוב משפט השלמות, רק הפעם לתחשיב הפרדיקטים. משפט השלמות בפרדיקטים יותר מפתיע מאשר בפסוקים, כי בפסוקים הכל סופי (אפשר לבדוק את כל ההצבות האפשריות ולבדוק אם משהו נכון נכון), אבל בפרדיקטים אי-אפשר אפילו לבדוק את כל האפשרויות (יש כמות אינסופית של עולמות שאפשר להתייחס אליהם).

כל המתמטיקה בעולם וגם כל הטיעונים הלוגיים הנכונים בפילוסופיה, כולם נמצאים כאן. את כולם נוכל להוכיח באמצעות ניסוחם בתחשיב הפרדיקטים, ואין שום דבר אחר שצריך לדעת על הוכחות בשביל לעשות את זה. אין שום נימוק נכון שאי אפשר בסופו של דבר לתרגם אותו להוכחה באמצעות התחשיב האלה.

### 9.1.1 דוגמא להוכחה

אחד מהדברים הממוכמים שהיוונים הקדמונים גילו זה הקונספט של הוכחה סינטקטית. הם קראו לזה סילוגיזם. בצורה היוונית היו כמה שבלונות שבעזרתן הוכיחו הכל, וכל השבלונות שלהם הם מקרים פרטיים של מה שראינו כאן. נראה דוגמא:

- כל היוונים בני אדם
- כל בני האדם בני תמונה

- מסקנה: כל היוונים בני תמותה

זה דוגמא לסילוגיזם הכי קלאסי, שאומר שאם כל  $A$  הוא  $B$  וכל  $B$  הוא  $C$ , אז כל  $A$  הוא  $C$ . אנחנו רוצים לנסח את זה בפורמליזם שלנו ולהוכיח את זה.

נתחיל מלנסח את הטענות:

$$\forall x[(G(x) \rightarrow H(x))]$$

$$\forall x[(H(x) \rightarrow M(x))]$$

והמטרה שלנו היא להוכיח  $\forall x[(G(x) \rightarrow M(x))]$ .

הוכחה:

מספר שורה	הצדקה	מסקנה
1		$\forall x[(G(x) \rightarrow H(x))]$
2		$\forall x[(H(x) \rightarrow M(x))]$
3	האקסיומה $UI$	$(\forall x[(G(x) \rightarrow H(x))]) \rightarrow (G(x) \rightarrow H(x))$
4	$MP$ של 1 ו-3	$(G(x) \rightarrow H(x))$
5	האקסיומה $UI$	$(\forall x[(H(x) \rightarrow M(x))]) \rightarrow (H(x) \rightarrow M(x))$
6	$MP$ של 2 ו-5	$(H(x) \rightarrow M(x))$
7	טאוטולוגיה	$((G(x) \rightarrow H(x)) \rightarrow ((H(x) \rightarrow M(x)) \rightarrow (G(x) \rightarrow M(x))))$
8	$MP$ של 4 ו-7	$((H(x) \rightarrow M(x)) \rightarrow (G(x) \rightarrow M(x)))$
9	$MP$ של 6 ו-8	$(G(x) \rightarrow M(x))$
10	האקסיומה $UG$	$\forall x[(G(x) \rightarrow M(x))]$

הסברים על בניית ההוכחה:

- 1-2: רשמנו את ההנחות.
- 3-4: אנחנו רוצים עכשיו להגיע בשני שלבים ממה שיש לנו ל- $G(x) \rightarrow H(x)$ . לכן:
  - 3: נשתמש באקסיומה  $UI$  עם  $\tau = x$  ו- $\varphi = (G(x) \rightarrow H(x))$ .
  - 4: נפעיל  $MP$  לקבלת הביטוי המבוקש.
- 5-6: נחזור על מה שעשינו בשני השלבים הקודמים, הפעם עם ההנחה השנייה.
- 7-10: אנחנו רוצים שבשלב האחרון יהיה  $\forall x[(G(x) \rightarrow M(x))]$ , שזו המסקנה שאנחנו אמורים להגיע אליה.
  - 7: מתחשיב הפסוקים אנחנו יודעים ש- $(G(x) \rightarrow M(x))$  זו מסקנה מ-4,6. לכן, נרצה להשתמש בטאוטולוגיה מתחשיב הפסוקים.
  - נכתוב כותה כמו שעשינו בשורה 7 (הערה: השתמשנו ב-12 מתחשיב הפסוקים, אבל בשלב הזה לא אכפת לנו מאיזו אקסיומה של תחשיב הפסוקים זה נבע, רק אכפת לנו שזו טאוטולוגיה. אפשר אפילו רק לבדוק את כל האפשרויות כדי לראות שזה מתקיים, הנקודה היא שלא אכפת לנו בשלב הזה איך הגיעו לזה אלא רק שזה נכון).
  - 8-9: נפעיל פעמיים  $MP$ .
  - 10: נשתמש ב- $UG$  בשביל לסיים את ההוכחה.

## הערות –

- נשים לב שבהוכחה שלנו לא הגבלנו את עצמינו למודל מסויים או לעולם מסויים. זה נכון עבור כל עולם, גם עולמות סופיים וגם אינסופיים.
  - נשים לב שכל השורות שאפשר לכתוב בהוכחה הן נאותות, כלומר כולן נכונות בכל מודל. זה גם נכון לאקסיומות שלנו, לכללי ההיסק ולטאוטולוגיות. אם שורה בהוכחה היא משפט (כלומר נוסחא בלי משתנים חופשיים) אז ברור למה זה נכון, צריך להבין גם למה זה נכון עבור שורות שאינן משפטים, שגם הן שורות מותרות בהוכחה.
- את זה אנחנו יכולים להבין באמצעות  $UG$ , שאומר לנו שאם אנחנו כותבים משהו כללי שיש לו משתנה חופשי, זה כאילו אמרנו שהדבר הזה נכון עבור כל האיברים באותו העולם. כלומר, אם אנחנו רושמים  $\psi(x)$  אנחנו מתכוונים  $\forall x[\psi(x)]$ . כלומר, אם יש נוסחא עם משתנים חופשיים אז המשמעות היא שזה מתקיים לכל משהו. זה אומר שכל מה שהוכחנו הוא נאות, ולכן זה נכון לכל עולם שהוא.
- היינו יכולים לחשוב על שיטה אחרת שלא תרשה הוכחות עם משתנים חופשיים. אבל זה מאוד נח כאן, כי זה נותן לנו לעשות מניפולציות לוגיות של טאוטולוגיות בתוך הכמת. זה הדרך הטכנית שהמערכת הזאת מאפשרת לעשות הוכחות מסובכות. אם היינו מאפשרים רק לשורות להיות רק משפטים, אז היינו צריכים לכתוב את זה אחרת.

## 9.2 תרגיל 9

יש לו שני חלקים קונספטואליים. החלק השני עוסק בוידוא הוואלידיות של ההוכחה, והוא בעצם לכתוב את המתודה  $is\_valid$  ה- $is\_valid$  יכול לקבל אחד מארבעה דברים:  $UI, MP$ , טאוטולוגיה או הנחה (שזה יכול להיות אחת ההנחות בהוכחה או אחת האקסיומות שלנו).

כל אחת מהאקסיומות האלה מייצגת לא נוסחא יחידה אלא משפחה של נוסחאות, **סכמות של נוסחאות**. זה משהו שנראה כמו נוסחא, אבל יש בו *wildcards*:  $\varphi$  שיכולה להיות כל נוסחא,  $\tau$  שיכול להיות כל שם עצם ו- $x$  שיכול להיות כל משתנה. החלק הראשון של התרגיל עוסק בלתפוס את הרעיון הזה.

המחלקה הראשון שנגדיר היא סכמה, שמקבלת שני דברים: נוסחא שיכולה לכלול טמפלטים, ורשימה של מי נחשב טמפלט. לדוגמא:

$$(\forall x[R(x)] \rightarrow R(c))$$

עם הרשימה  $\{R, c, x\}$  אומר ש- $R$  יכול להיות כל נוסחא,  $x$  יכול להיות כל משתנה ו- $c$  יכול להיות כל שם עצם.

באופן כללי, יש שלושה דברים שיכולים לשמש כטמפלט:

- קבוע: אפשר לשים במקומו כל שם עצם.
- משתנה: אפשר לשים במקומו כל שם של משתנה.
- שם של פרדיקט: אפשר לשים במקומו כל נוסחא.

במשימות 1 ו-2 מתחילים עם החלק הקל של ההצבה – מוסיפים למחלקות  $Term$  ו- $Formula$  מתודות בשם *substitute* (מתודה נפרדת לכל אחד מהם), שמקבלות מילון שאומר אילו החלפות לעשות. זה דבר סינטקטי בסיסי של להחליף עלה בביטוי יותר גדול.

לדוגמא – נניח שיש לנו את הנוסחא:

$$f = Formula.parse(' \forall y[GT(y, c)]')$$

ואת המילון:

$$d = \{c': Term.parse('g(x)')\}$$

אם נכתוב  $f.substitute(d)$  הוא יחזיר:  $\forall y[GT(y, g(x))]$ .

אלה החלפות יחסית פשוטות, החלק היותר מסובך הוא החלפה של יחס. הפונקציה המעניינת שלנו, אולי הכי קשה, זה פונקציה שנקראת  $instantiate\_formula$ , שמקבלת ארבעה דברים:

- נוסחא (שהיא בתפקיד הנוסחא של הסכמה)
- שני מילונים שונים:
  - $dcv$ , שאומר אילו משתנים להחליף בנוסחא הזאת ואיך
  - $dr$ , שאומר אילו יחסים להחליף בנוסחא הזאת ואיך
- משתנים אסורים (הסבר בהמשך)

נסביר זאת דרך דוגמא:

$$f = (\forall x[(R() \rightarrow Q(x))] \rightarrow (R() \rightarrow \forall x[Q(x)]))$$

נניח שאנחנו לא רוצים לעשות החלפות של משתנים, ומבחינת יחסים אנחנו רוצים לעשות את שתי ההחלפות הבאות:

- $R(): z = 8$
- $Q(v): T(v, w)$

ההחלפה הראשונה פשוט אומרת לנו שבכל מקום שבו אנחנו רואים את הנוסחא  $R()$  אנחנו צריכים להחליף אותה בנוסחא  $z = 8$ . ההחלפה השנייה כוללת פרמטר, והיא אומרת לנו שבכל מקום שבו אנחנו רואים הפעלה של  $Q$  על משהו אנחנו צריכים להחליף אותה בהפעלה של  $T$  על אותו המשהו ועל  $w$ .

מה התוצאה צריכה להיות:

$$f = (\forall x[(z = 8 \rightarrow T(x, w))] \rightarrow (z = 8 \rightarrow \forall x[T(x, w)]))$$

$dcv$  יהיה ריק, כי אנחנו לא רוצים לעשות שום החלפות של משתנים או קבועים. ב- $dr$  יהיו שני דברים עבור כל יחס שאנחנו רוצים להחליף, גם הרשימה של הפרמטרים של היחס וגם את הנוסחא עצמה שצריך לשים במקום:

$$\{R': ([], 'z = 8'), Q': ([v], 'T(v, w)')\}$$

איך נראה אלגוריתם ההחלפה של יחסים:

- יורדים ברקורסיה של העץ עד שרואים משהו מעניין, קריאה ליחס.
- אז יש שתי אפשרויות:
  - או שהוא לא נמצא בכלל במילון ומחזירים את מה שיש.
  - אם הוא כן נמצא במילון, מבצעים את ההצבה: מחזירים את הנוסחא שכתובה במילון במקום אותו היחס, אבל עם הצבה של מה שצריך במקום הפרמטרים. לדוגמא, אם נגיע ל- $Q(x)$  נצטרך להציב במקום  $T(x, w)$ .

יש מקרה שבו ההצבה שמבקשים לא תהיה חוקית, והוא אם מבקשים להציב משהו שהוא משתנה חסום (לדוגמא אם היינו מנסים לעשות את ההצבה  $R: x = 8$ ). לכן, יש עוד קלט לפונקציה שהוא משתנים אסורים. בכל פעם שאנחנו מגיעים למשתנה חסום ברקורסיה, אנחנו מעדכנים את הרשימה הזאת במשתנה החדש. אם נתקל בהצבה שמבקשת מאיתנו להציב משתנה אסור, נזרוק אקספצן.

בהקשר הזה, עוד נקודה היא שצריך לשים לב שאם אנחנו מחליפים נגיד את  $\forall x$  ב- $\forall z$ , אנחנו צריכים להכניס את  $z$  בתור המשתנה האסור ולא את  $x$ . לכן, צריך לשים לב שקודם כל צריך לעשות את ההחלפות של המשתנים (זה מוסבר בצורה מפורטת בהוראות של התרגיל).

השלב הביא היא מתודה של סכמה שנקראת *instantiate*. היא מקבלת מילון שכולל בתוכו גם את *dccv* וגם את *dr*, כלומר כולל את ההחלפות לכל משתנה, קבוע ויחס. הפורמט שלה הוא פורמט שנראה יותר אלגנטי, אבל פחות נח לעבודה. דוגמא:

$$\{ 'c': 'g(0)', 'x': 'z', 'Q(v)': 'T(v, w)' \}$$

בתרגיל צריך להפריד את המילון לשני החלקים, ולעביר את זה לפורמט היותר נח של המשימה הקודמת.

כל העבודה הזאת נועדה כדי שנוכל להתייחס לא רק לנוסחא אלא למשפחת נוסחאות, סכמה של נוסחאות, ולדעת מתי נוסחא היא מקרה פרטי של נוסחא אחרת.

הערות –

- נקודה עדינה בנוגע משתנים אסורים: נניח שבנוסחא שלנו מופיע  $\forall x [Q(x)]$ . ההחלפה  $Q: ([v], T(v, x))$  היא לא חוקית. אך לעומת זאת ההחלפה  $Q: ([x], T(x, w))$  היא בסדר, כי כאן הוא משתנה שמחליפים. במילים אחרות, נוכל להגיד שהמשתנים האסורים הם משתנים שלא יכולים להופיע במקום המשתנים החופשיים של  $Q$ .
- מטרת החוקים של ההחלפות: החוקים האלה נועדו לשמור על הנאותות של האקסיומות, זה מוודא שבאמת כל אינסטנס של האקסיומות האלה יהיה נכון.

נציין עוד כמה דברים בנוגע ל-*is\_valid*. הפונקציה הזאת, מעבר לכך שהיא רואה שהמסקנה היא מה שצריך להיות, שכל שורה מסתמכת רק על שורות שכבר היו וכו', צריכה לבדוק שכל שורה היא אחד מארבעה דברים:

1. *MP*, ואז צריך לוודא שהיא נכונה. כלומר, לדוא שבאמת במקום הראשון יש משהו שנראה כמו נוסחא, אחר כך משהו שנראה כמו גרירה של הנוסחא הזאת לנוסחא אחרת, ובשורה האחרונה הנוסחא האחרת כמסקנה.
  2. *UI*, ואז לפי אותו רעיון בודקים שזה באמת *UI*, ושהשורות שצריכות לבוא קודם באמת באות קודם.
  3. טאוטולוגיה. במקרה הזה, כדי לבדוק את האלידיות נרצה להשתמש במה שכבר בנינו בתחשיב הפסוקים שבדק נכונות של נוסחא בתחשיב הפסוקים. בשביל לעשות את זה, נצטרך להשתמש במתודה שנכתוב עבור המחלקה של נוסחא, שלוקחת נוסחא בתחשיב הפרדיקטים ומוציאה נוסחא בתחשיב הפסוקים שמתארת את הנוסחא הזו.
- אם הנוסחא אצלינו היא למשל מהצורה של משהו גורר משהו, גם הנוסחא בתחשיב הפסוקים צריכה להיות מהצורה הזאת. דברים כמו יחסים וכמתים יהיו כבר הסוף מבחינת הרקורסיה שלנו, כבר נחליף אותם פשוט בשם של משתנה (יש לנו גנרטור שמייצר את השמות).
- דוגמא:

$$(x = 0 \& \forall x [(R(x) \& R(y))])$$

מתורגם ל:

$$(z_1 \& z_2)$$

4. אקסיומה/הנחה. במקרה של אקסיומה יהיה רשום בהוכחה איזו מהאקסיומות זו, ואיזו הצבה עושים לה. צריך לבדוק שההצבה שדורשים באמת מתאימה, וכן שלא מנסים לעשות הצבה אסורה.

*is\_valid* צריך לראות שההוכחה היא נכונה מבחינה סינטקטית. בתרגיל נקבל כבר את המעטפת מוכנה, ומה שנשאר זה הליבה של לבדוק האם ארבע השורות האלה נכונות.

## 10 שיעור 10 – 31.12.17

### 10.1 תרגיל 10 (הוכחות בתחשיב הפרדיקטים)

#### 10.1.1 הקדמה

בתרגיל 10 נוכיח דברים במערכת האקסיומטית שלנו. כזכור, המערכת כוללת שני כללי היסק: מודוס פוננס ו- *Universal Generalization*, ואת כל הטאוטולוגיות:

$MP$	$\frac{\varphi, (\varphi \rightarrow \psi)}{\psi}$
$UG$	$\frac{\varphi}{\forall x[\varphi]}$
$T$	טאוטולוגיה

בנוסף, היו לנו 6 אקסיומות:

$UI$	$(\forall x[\varphi(x)] \rightarrow \varphi(\tau))$
$EI$	$(\varphi(\tau) \rightarrow \exists x[\varphi(x)])$
$US$	$(\forall x[\varphi \rightarrow \psi(x)] \rightarrow (\varphi \rightarrow \forall x[\psi(x)]))$
$ES$	$((\forall x[\varphi(x) \rightarrow \phi] \& \exists x[\varphi(x)]) \rightarrow \phi)$
$RX$	$\tau = \tau$
$ME$	$(\tau = \sigma \rightarrow (\phi(\tau) \rightarrow \phi(\sigma)))$

שתי האקסיומות הראשונות:

- $UI$ : אם אנחנו יודעים ש- $\varphi(x)$  נכון לכל  $x$ , אפשר להסיק את  $\varphi$  על כל שם עצם שרוצים.
- $EI$ : באותה מידה, אם אנחנו יודעים ש- $\varphi(\tau)$  נכונה עבור  $\tau$  כלשהו, אנחנו יודעים שקיים  $x$  שמקיים  $\varphi(x)$ .

יש שתי אקסיומות שמאפשרות לנו לעשות פישוט:

- $US$ : אם לכל  $x$  מתקיים שמהו שלא תלוי ב- $x$  גורר משהו שכן, אפשר להוציא את המשהו הלא תלוי החוצה.
- $ES$ : אם משהו שתלוי ב- $x$  גורר מסקנה לכל  $x$  ויש לפחות מקרה אחד שזה נכון לגביו, אז המסקנה נכונה.

ועוד שתי אקסיומות שמטפלות בשיוויון:

- $RX$ : כל עצם שווה לעצמו.
- $ME$ : אם דברים שווים, אפשר להציב אותם בכל נוסחא ולקבל שקילות.

נזכור שהתייחסנו ל- $\varphi, \phi, \psi$  בתור כל נוסחא, ול- $\tau$  בתור כל שם עצם.

התרגיל מורכב משני חלקים: החלק הראשון כולל לוגיקה קלאסית (ולא מתמטיקה אחרת). כדי לעזור בהוכחות וכדי לפרמל טכניקות לוגיות שימושיות בהוכחות, נכתוב כמה פונקציות עזר שיעזרו לנו בהמשך. בחלק השני יש הוכחות שקשורות לתחומים אחרים במתמטיקה – שדה, חבורה וכו'.

כשמבקשים מאיתנו להוכיח משהו, יש שני אלמנטים חשובים: להבין איך צריך להוכיח, ולהבין איך לכתוב את ההוכחה אצלינו. אפילו הוכחות של דברים פשוטים (דברים מהשיעור הראשון של אינפי 1) הן כבר לא הוכחות קלות, ובנוסף מה שאפשר במשפט אחד באינפי במערכת שלנו עשוי להיות ארוך.

הצורה שבה בודקים בתרגיל אם פונקציות העזר שכתבנו נכונות היא להוכיח הוכחה כלשהי באמצעותן, ולראות שההוכחה עובדת עם פונקציות העזר שלנו. פירוט טקסטואלי של ההוכחות אפשר למצוא בתיאור התרגיל, ופירוט בפייתון אפשר למצוא ב-*provers\_test*.

## 10.1.2 הוכחת סילוגיזם נוסף

בשיעור הקודם הוכחנו את הסילוגיזם שאם כל היוונים הם בני אדם וכל בני האדם בני תמותה, כל היוונים בני תמותה. נוכיח עכשיו עוד סילוגיזם קלאסי:

- כל בני האדם הם בני תמותה
- קיים בן אדם
- מסקנה: קיים בן תמותה

ואם ננסח בסינטקס שלנו:

- $\forall x[(Man(x) \rightarrow Mortal(x))]$
- $\exists x[Man(x)]$
- מסקנה:  $\exists x[Mortal(x)]$

נכתוב את ההוכחה בשלמותה, ולאחר מכן נסביר יותר בפירוט על כל שלב. כמו כן, עבור כל טכניקה לוגית שאנחנו נתקלים בה במקבץ מסויים של שורות והיא תהיה שימושית לנו בהמשך, נרשום איזו פונקציית עזר בתרגיל רלוונטית לתמרון שעשינו.

ההוכחה:

מספר שורה	הצדקה	מסקנה
1	הנחה	$\forall x[(Man(x) \rightarrow Mortal(x))]$
2	הנחה	$\exists x[Man(x)]$
3a	UI	$(\forall x[(Man(x) \rightarrow Mortal(x))]) \rightarrow (Man(x) \rightarrow Mortal(x))$
3	MP על 1 ו-3a	$(Man(x) \rightarrow Mortal(x))$
4	EI	$(Mortal(x) \rightarrow \exists x[Mortal(x)])$
5a	טאוטולוגיה	$((Man(x) \rightarrow Mortal(x)) \rightarrow ((Mortal(x) \rightarrow \exists x[Mortal(x)]) \rightarrow (Man(x) \rightarrow \exists x[Mortal(x)])))$
5b	MP על 3 ו-5a	$((Mortal(x) \rightarrow \exists x[Mortal(x)]) \rightarrow (Man(x) \rightarrow \exists x[Mortal(x)]))$
5	MP על 4 ו-5b	$(Man(x) \rightarrow \exists x[Mortal(x)])$
6a	UG עם 5	$\forall x[(Man(x) \rightarrow \exists x[Mortal(x)])]$
6b	ES	$((\forall x[(Man(x) \rightarrow \exists x[Mortal(x)])] \& \exists x[Man(x)]) \rightarrow \exists x[Mortal(x)])$
6c		...
6d		...
6		$\exists x[Mortal(x)]$

### • שורות 2 – 1:

○ הסבר: הנחות.



• **שורה 3a:**

- הסבר: השורה הזאת היא הפעלה של  $UI$  עם המיפוי  $\tau \equiv x, \varphi(v) \equiv (Man(v) \rightarrow Mortal(v))$ . נשים לב שיש הבדל גדול בין ה- $x$  לפני הגרירה השנייה (הבחולה) ואחריה:
 
$$(\forall x[(Man(x) \rightarrow Mortal(x))] \rightarrow (Man(x) \rightarrow Mortal(x)))$$
 לפני הגרירה הזאת, ה- $x$ ים שמופיעים הם חסומים, ואחרי לא חסומים.
- למה השורה הזאת מעניינת בכלל: אנחנו רוצים להגיע למה שכתוב בשורה 3, ומה שיש לנו בהנחות זה כמו שורה 3, רק עם כמת אוניברסלי. ה- $UI$  הוא בדיוק מה שמאפשר לנו להפטר מהכמת, כי אחרי שנפעיל אותו נוכל להפעיל  $MP$  ולקבל את מה שאנחנו רוצים (שורה 3 עצמה).
- פונקציית עזר בתרגיל:  $add\_universal\_instantiation$  (משימה 1). הפונקציה מאפשרת לנו לדלג על 3a בכך שהיא מקבלת משהו עם כימות ומורידה את הכימות כמו שעשינו כאן. אנחנו רואים כאן שזה מאוד פשוט – צריך לעשות  $UI$  עם מפה נכונה ואז  $MP$ .
- הערה על  $\forall$ : אנחנו הרבה פעמים רוצים לעבוד בלי הכמת הזה, כי הוא לא מאפשר לנו לעבוד עם טאוטולוגיות. ברגע שיש "לכל" בשביל הטאוטולוגיה כל מה שבתוך הכמת הוא פסוק אטומי והטאוטולוגיה לא תוכן להתייחס אליו, לכן נרצה להפטר מה"לכל".
- זו פשוט שיטה טכנית בהוכחה, ונשים לב שאנחנו תמיד יכולים להעביר כימות של לכל עם  $UI$  ולהחזיר עם  $UG$ .

• **שורה 4:**

- הסבר: נפעיל את  $EI$  עם המפה  $\tau \equiv x, \varphi(v) \equiv Mortal(\varphi)$ .
- הערה על  $\exists$ : בניגוד לזה שראינו שב"לכל" אפשר בקלות להוריד ולהחזיר עם הכמת, עם "קיים" זה קצת יותר מייגע, ואין דרך בהירה להסביר אילו תמרונים נעשה בשביל להחזיר "קיימים". מה שעשינו בשלב הזה זו דוגמא לדרך מסוימת נוחה להוסיף את הכמת הזה.

• **שורה 5:**

- הסבר: נקפוץ ל-5 ונראה איך עשינו את הקפיצה. אנחנו רוצים להסיק:
 
$$(Man(x) \rightarrow \exists x[Mortal(x)])$$
 זו הסקה טאוטולוגית. אין לנו הסקה טאוטולוגית בין כללי ההיסק שלנו, רק טאוטולוגיה, אז צריך לממש אותה. בשביל זה נכתוב את מה שיש ב-5a, וזו טאוטולוגיה (בתחשיב הפסוקים קראנו לה  $I2$ ). לאחר מכן אפשר להפעיל  $MP$  פעמיים, ולהגיע לתוצאה הרצויה.
- פונקציית עזר בתרגיל:  $add\_tautological\_inference$  (משימה 2). במשימה הזאת נקח מסקנה שנובעת טאוטולוגית מכמה שורות ונגיע אליה באמצעות השורות האלה. הפעם יכולים להיות יותר משני שלבים, זה תלוי בכמה פסוקים משתמשים, אבל הפונקציה מאפשרת לנו להוסיף את השורות האלה באמצעות שורת קוד אחת. באופן כללי, אם משהו נובע טאוטולוגית אז רוצים להגיד ששורות  $x, y, z$  גוררות את מה שרוצים. בשביל לכתוב את זה בהוכחה אפשר לכתוב ששורה  $x$  גוררת ששורה  $y$  גוררת ששורה  $z$  גוררת את מה שרוצים.

• **שורה 6:**

- הסבר: מה שנרצה לעשות עכשיו זה להשתמש ב- $ES$ , ואז נגיע כמעט למה שאנחנו רוצים. בשלב הראשון, נשתמש ב- $UG$  על שורה 5 (שורה 6a). אחרי זה נפעיל את  $ES$  עם המפה  $\varphi \equiv Man(x)$  ו- $\phi \equiv \exists x[Mortal(x)]$ . צריך לזכור של- $\phi$  אסור שיהיה את איקס כמשתנה חופשי (כי הוא נמצא בתוך כמת), ובמקרה הזה אנחנו אכן עומדים בתנאי הזה – ה- $x$  שמופיע ב- $\phi$  הוא משתנה חסום. מכאן ההגעה ל-6 היא כבר היסק טאוטולוגי, אז נשתמש שוב בפונקציה ממשימה 2 ונקבל בסופו של דבר את המסקנה של שורה 6.

**פונקציית עזר בתרגיל:** `add_existential_derivation` (משימה 3). התמרון שהשתמשנו בו כדי להוכיח שמשהו קיים ע"י  $ES$  (של לעבור משורות  $2 + 5$  לשורה 6) יהיה לנו גם הוא שימושי בהמשך, וזה מה שנעשה בפונקציה הזאת, משהו שעושה את כל התמרון הזה ביחד. נשים לב שבדרך קראנו לפונקציה שכבר כתבנו, הפונקציה של הסקה טאוטולוגית (משימה 2), נוסף על אולי עוד צעדים.

### 10.1.2.1 אותה הוכחה בקוד

נרצה לקבל מושג איך הדבר הזה נראה בקוד. באופן כללי, כל פונקציות העזר יהיו מתודות של מחלקה בשם `Prover`, שבונה הוכחות בצורה נוחה, ובתוכה יש מתודות עזר. את ההוכחות שצריך להוכיח בתרגיל כותבים ב-`some_proofs`, וזה משתמש ב-`Provers`.

הקוד המלא של ההוכחה שנעשה נמצא ב-`sylogism_all_exists_proof_with_existential_derivation` בתוך `provers_test`. נסקור אותו:

```
def sylogism_all_exists_proof_with_existential_derivation(print_as_proof_forms=False):
```

התפקיד הכללי של הפונקציה הוא להוכיח את התוצאה מתוך ההנחות. לפונקציה פרמטר שאומר האם להדפיס כל שורה בזמן ההוספה (לצורכי דיבאגינג).

```
prover = Prover(['Ax[(Man(x)->Mortal(x))]', 'Ex[Man(x)]', 'Ex[Mortal(x)]', true)
```

הבנאי של `Prover` מקבל רשימה של הנחות + מסקנה (בנוסף לפרמטר הדיבאגינג), ומייצר אובייקט של הוכחה שכולל בסופו של דבר את ההוכחה המלאה. למחלקה יש שדה בשם `proof`, שכל מה שנעשה הוא להוסיף אליו עוד שורות, ואת ההוכחה שמכיל השדה הזה נצטרך להחזיר בסוף.

ערך ההחזרה של המתודות ב-`Prover` הוא מספר השורה האחרונה של מה שהוספנו. במספר הזה נוכל להשתמש בשורות הבאות בהוכחה כדי להסיק דברים על סמך שורות קודמות.

```
step1 = prover.add_assumption('Ax[(Man(x)->Mortal(x)) ]')
step2 = prover.add_assumption('Ex[Man(x)]')
```

בשתי השורות האלה אנחנו רואים איך להוסיף הנחות. למעשה, יש שתי דרכים להוסיף הנחות: מתודה להנחה קלה ומתודה להנחה מסובכת. לפעמים יש הנחות שצריך להוסיף אותן כמו שהן, בלי לאתחל שום טמפלט, ואלה ההנחות הקלות. אותן נוסיף עם הפונקציה `add_assumption`, כמו שעשינו כאן.

לעומת זאת, יש מקרים שבהם ההנחה שנרצה להוסיף כוללת טמפלט, ונצטרך לאתחל אותו לפני שאנחנו מוסיפים אותה. לשם כך נשתמש ב-`add_instantiated_assumption`, ונגיד מה המפה של האתחול.

```
step3 = prover.add_universal_instantiation('(Man(x)->Mortal(x))', step1, 'x')
```

בשלב 3 אנחנו כבר רוצים להשתמש ב-`add_universal_instantiation`, שמקבלת את מה שהיא צריכה להוסיף (אצלנו זה  $(Man(x) \rightarrow Mortal(x))$ ), מתוך מה היא צריכה לגזור את זה (שלב 1) ואת מי צריכים להציב בתור  $\tau(x)$ .

```
step4 = prover.add_instantiated_assumption(
    '(Mortal(x)->Ex[Mortal(x)])', Prover.EI, {'R(v)': 'Mortal(v)', 'c': 'x'})
```

שלב 4 זה `EI`, וזו הוספה של הנחה יותר מסובכת שדיברנו עליה. צריך להגיד לו מה ההנחה, מי ההאקסיומה, ומי המפה שהופכת את הסכמה לנוסחא הכתובה.

```
step5 = prover.add_tautological_inference(' (Man(x)->Ex[Mortal(x)]) ',
[step3, step4])
```

בשלב 5 נשתמש ב-`add_tautological_inference`. צריך לתת לו דבר ראשון כמו תמיד את מה שאנחנו רוצים להסיק (כל שורה 5), ובסוף את ההצדקה. מה ההצדקה שלנו הולכת להיות: שזה נובע טאוטולוגית מ-3,4, אז שמים ברשימה האינדקסים שלהם.

```
step6 = prover.add_existential_derivation('Ex[Mortal(x)]', step2, step5)
```

אחנו רוצים לקפוץ לשלב 6 ישר מ-2+5, אז צריך לתת ל-`add_existential_derivation` את מה שאנחנו רוצים להגיע אליו ואת מספרי השורות האלה. בערך ההחזרה של השלב האחרון בהוכחה לא משתמשים אף פעם, אז הוא יהיה צבוע באפור.

```
return prover.proof
```

החזרת ההוכחה.

## 10.2 הוכחות של מבנים אלגבריים

בחלק השני של התרגיל עוברים להוכחות של מבנים אלגבריים.

המבנה הראשון שנדבר עליו הוא של חבורה לא בהכרח קומוטטיבית. חבורה היא מבנה אלגברי עם פעולה אחת (אצלינו היא תהיה חיבור/חיסור), שמקיימת את הכללים:

כתיבה מתמטית	כתיבה אצלינו	
$0 + x = x$	$plus(0, x) = x$	1 איבר נייטרלי
$-x + x = 0$	$plus(minus(x), x) = 0$	2 איבר הופכי
$(x + y) + z = x + (y + z)$	$plus(plus(x, y), z) = plus(x, plus(y, z))$	3 אסוציאטיביות (קיבוץ)

מה אפשר להוכיח מתוך זה שזו חבורה? מסתבר שכל מיני דברים, לדוגמה ש- $x + 0 = x$ . נזכור: החבורה היא לא בהכרח קומוטטיבית, אז אנחנו יודעים ש- $0 + x = x$ , אבל לא נובע מזה ש- $x + 0 = x$ .

### 10.2.1 הוכחת נייטרליות מימין בחבורה לאו דווקא קומוטטיבית

למה:  $x + 0 = x$  (האיבר הנייטרלי הוא לא רק נייטרלי משמאל, אלא גם נייטרלי מימין)

הוכחה (ניסוח מתמטי):

הצדקה	מסקנה
	$x + 0 =$
קיום נייטרלי	$0 + x + 0 =$
קיום הופכי	$(- - x + -x) + x + 0 =$
קיבוץ	$- - x + (-x + x) + 0 =$
קיום הופכי	$- - x + 0 + 0 =$
קיום נייטרלי	$- - x + 0 =$
קיום הופכי	$- - x + (-x + x) =$
קיבוץ	$(- - x + -x) + x =$
קיום הופכי	$0 + x = 0$

נהפוך את זה להוכחה אצלינו.

הוכחה (ניסוח שלנו):

נתחיל מכמה שורות שיעזרו לנו בהמשך:

מספר שורה	צעד	הצדקה
1	$0 + x = x$	הנחה
2	$-x + x = 0$	הנחה
3	$(x + y) + z = x + (y + z)$	הנחה
4	$x = 0 + x$	סימטריות השוויון עם 1 (משימה 6)
5	$0 = -x + x$	סימטריות השוויון עם 2 (משימה 6)
6	$x + (y + z) = (x + y) + z$	סימטריות השוויון עם 3 (משימה 6)

מה שאנחנו עושים כאן זה להוכיח את הסימטריות של שוויון: אם  $x = y$  אז  $y = x$ . כמובן שאנחנו צריכים שהדבר הזה יתקיים לכל  $x$  ו- $y$  (כלומר, לכל  $x$  ו- $y$  מתקיים שאם  $x = y$  אז  $y = x$ ), אבל לא חייבים לציין את כמת ה"לכל" אצלינו. נשים לב שאין לנו אקסיומה מפורשת של סימטריה של שוויון, ונצטרך להוכיח את זה במשימה 6 באמצעות ME.

בהוכחה בניסוחה הקודם, בכל מיני מקומות אמרנו דברים כמו: נקח את האקסיומה השנייה ונציב  $-x$  לתוך  $x$ . איך נעשה את זה אצלינו: נניח שהיה לנו חוק החילוף  $x + y = y + x$ , והיינו רוצים לגזור ממנו  $2 + f(5) = f(5) + 2$ . נעשה את זה בשלבים:

- אנחנו זוכרים שהשוויון הזה בעצם כולל כמת "לכל", כלומר הוא  $\forall x [\forall y [x + y = y + x]]$ . נוסיף את הכמתים באמצעות UG.

- נשתמש ב-add\_instantiated\_assumption כדי להציב את  $x \rightarrow 2, y \rightarrow f(5)$ .

עכשיו מקשים עלינו ומבקשים מאיתנו לכתוב משהו שלא רק מטפל במשתנה אחד, אלא בסדרת משתנים, ומחליף את כולם בבת אחת (זה יקל עלינו אח"כ). הקושי העיקרי הוא שיתכן שנרצה להחליף בין המשתנים, למשל להציב  $y \rightarrow f(x)$  ו- $x \rightarrow g(y)$ , ואז אם נעשה את ההצבות אחת אחרי השנייה נקבל תוצאה לא רצויה. הפתרון הוא פשוט: נעשה קודם את החילוף  $x \rightarrow z_1, y \rightarrow z_2$ , ורק אז נעשה את החילוף המבוקש. כל הסיפור הזה נועד כדי שנצליח להציב משהו בתוך נוסחא קודמת (משימה 7).

ברגע שיש לנו את את ההצבה, נוכל להתקדם הלאה:

מספר שורה	צעד	הצדקה
7	$0 = -x + -x$	לקחנו את 5 והפעלנו עליו הצבה $x \rightarrow -x$ (משימה 7)
8	$-x + -x = 0$	לקחנו את 2 והפעלנו עליו הצבה $x \rightarrow -x$ (משימה 7)
9	$(-x + -x) + x = -x + (-x + x)$	לקחנו את 3 והפעלנו עליו הצבה $x \rightarrow -x, y \rightarrow -x, z \rightarrow x$ (משימה 7)
10	$0 + 0 = 0$	לקחנו את 1 והפעלנו עליו הצבה $x \rightarrow 0$ (משימה 7)
11	$x + 0 = 0 + x + 0$	לקחנו את 4 והפעלנו עליו הצבה $x \rightarrow x + 0$ (משימה 7)
12	$0 + (x + 0) = (0 + x) + 0$	לקחנו את 6 והפעלנו עליו הצבה $x \rightarrow 0, y \rightarrow x, z \rightarrow 0$ (משימה 7)

הדבר הבא שאנחנו רוצים לעשות הוא שבהנתן שוויון כלשהו, לדוגמא  $0 = -x + x$ , נוכל לקחת ביטוי מהצורה:

$$(v + x + 0) = (v + x + 0)$$

שהוא נכון מ- $RX$ , ולעשות בו חילוף כך שיתקבל:

$$(0 + x + 0) = (-x + x + x + 0)$$

כלומר להציב בפעם הראשונה את  $v \rightarrow 0$  ובפעם השנייה את  $v \rightarrow -x$ .

את זה נעשה במשימה 8, וזה מאפשר לנו לעשות גם בקוד שלנו את ההצבות, שבמתמטיקה הן מאוד ברורות. עם זה נתקדם עוד בהוכחה:

מספר שורה	צעד	הצדקה
13	$(0 + x) + 0 = ((-x + -x) + x) + 0$	התקבל מכך שלקחנו $(0 + x) + 0 = 0$ ויש לנו משהו שאומר ש- $(-x + -x) + x = 0$ (משימה 8)
14	$((-x + -x) + x) + 0 = (-x + (-x + x)) + 0$	לקחנו את $f(v) = f(v)$ עבור $f(v) \equiv v + 0$ . החלק הפנימי הוא בדיוק שורה 9, ועכשיו עוד פעם מציבים עם משימה 8: אם $\tau_1 = \tau_2$ , אז $\tau_1 + 0 = \tau_2 + 0$
...	...	מופיע בתיאור תרגיל 10
20	$(-x + -x) + x = 0 + x$	שורה 8 עם משימה 8

כשכתבנו את ההוכחה בניסוח היותר מתמטי רשמתי  $A = B = C = \dots$  עד למסקנה. אצלינו כל שורה היא שיוויון אחד, וננסה לבנות את זה ככה שהשורות ישתרשרו יפה, כלומר החלק השמאלי של כל שורה יהיה החלק הימני של השורה הקודמת.

הצעד האחרון שנותר לנו הוא לשרשר את הדבר הזה, וזה צריך לנבוע משורות 11-20 ושורה 1. יש לנו משהו מהצורה  $A = B, B = C, C = D$  וכו'... ובסוף  $Z_1 = Z_2$ , ואנחנו רוצים לשרשר את השיוויונים ולקבל  $A = Z_2$ . כלומר, מה שאנחנו רוצים זו בעצם טרנזיטיביות. אין לנו אקסיומה של טרנזיטיביות, אבל אפשר לקבל טרנזיטיביות ע"י שימוש ב- $RX$  וב- $ME$ .

מספר שורה	צעד	הצדקה
21	$x + 0 = x$	שורות 11-20 ושורה 1

## 10.2.2 הוכחה שיש רק איבר נייטרלי אחד לחיבור

נרצה להוכיח הוכחה נוספת על חבורות: אפשר להוכיח שאפשר להוסיף אותו ולקבל את אותו האיבר, כלומר אם  $a + c = a$  אז  $c = 0$ . זה תרגיל במתמטיקה, ונצטרך להוכיח אותו עם הכלים שלנו. יש כאן שני קשיים: איך מוכיחים את זה מתמטית, ואז איך כותבים את זה טכנית. בשביל לפתור את הקושי הטכני, נוכל להעזר בכל הפונקציות שכתבנו עד עכשיו.

באוסף התרגילים הזה פחות או יותר כיסינו את הפער בין המתמטיקה כמו שאנחנו מכירים אותו לבין הלוגיקה.

## 10.2.3 הוכחה בשדה

עכשיו נוסיף מבני אלגבי נוסף: שדה. השדה הוא כמו חבורה רק עם עוד פעולה שנסמן אותה ב- $times$  + אקסיומות השדה שנוגעות לכפל + חוק החילוף לחיבור. המשפט הראשון שלומדים בשדות:

$$0 \cdot x = 0$$

זו לא אקסיומה, אבל אפשר להוכיח אותה מתוך תשע האקסיומות של השדה.

רמז להוכחה: ההוכחה שעשינו של אם  $a + c = a$  אז  $c = 0$  היא מאוד דומה (דומה מבחינת מה שעושים בה, לא במובן שהפונקציה שכתבנו אז תהיה שימושית כאן).

#### 10.2.4 אקסיומות פיאו

אחרי שעברנו על המבנים האלגבריים הרגילים של אלגברה עוברים לשתי מערכות אקסיומות מעניינות.

בשלב הזה אנחנו יורדים ליסודות המתמטיקה, ונוגעים במספרים טבעיים. ברגע שיש לנו מספרים טבעיים אנחנו לאט לאט יודעים לבנות את הרציונליים, לאחר מכן את הממשיים וכו'.

נשאלת השאלה מה האקסיומות של הטבעיים. הדרך המקובלת לעשות את זה היא האקסיומות של פיאו. האקסיומות האלה מכילות שלושה אלמנטים בשפה:

- $s(x)$  שהוא העוקב של  $x$  (או במילים יום יומיות יותר הוא  $x + 1$ )
- $plus(x, y)$  ו- $times(x, y)$
- קבוע יחיד שנקרא אפס

מאקסיומות פיאו אפשר להוכיח כל מה שנרצה על הטבעיים, וברגע שיש את זה על הטבעיים אפשר להתרחב משם לכל השאר. האקסיומות:

- אם שני מספרים שונים, העוקב שלהם שונה:  

$$s(x) = s(y) \rightarrow x = y$$
- לכל מספר חוץ מאפס יש מישהו שבא לפניו:  

$$(x \neq 0 \rightarrow \exists y[s(y) = x])$$

$$s(x) \neq 0$$
- הקשר בין העוקב לפעולת החיבור, שזו בעצם הגדרה רקורסיבית של חיבור:  

$$x + 0 = x$$

$$x + s(y) = s(x + y)$$
- כפל:  

$$x \cdot 0 = 0$$

$$x \cdot s(y) = x \cdot y + x$$
- האקסיומה המרכזית, אקסיומה האינדוקציה:  

$$((\phi(0) \wedge \forall x[\phi(x) \rightarrow \phi(s(x))]) \rightarrow \forall x[\phi(x)])$$

אקסיומת האינדוקציה היא סכמה לכל נוסחא  $\phi$ , והיא אומרת שאינדוקציה עובדת. זו כמעט ההגדרה של הטבעיים: הטבעיים מוגדרים ע"י זה שאינדוקציה עובדת עליהם. אם הוכחנו שמהו עובד על אפס ואם הוכחנו שאם זה עובד על מספר זה עובד על המספר העוקב שלו, אז זה עובד על כל מספר.

מה שאנחנו צריכים לעשות בתרגיל זה להוכיח משפט אחד לגבי הטבעיים. בפיאו, אין לנו אקסיומה שאומרת ש- $x + y = y + x$ . את זה נוכיח כמו כל דבר בפיאו: באינדוקציה. הצעד הראשון יהיה עבור אפס:  $x + 0 = 0 + x$ . איך נראה את צעד הבסיס: גם באינדוקציה, עכשיו על  $x$ . זה התרגיל שלנו, להוכיח את התכונה הראשונה של המספרים הטבעיים.

#### 10.2.5 אקסיומות צרמלו-פרנקל

לכאורה, זה הבסיס של המתמטיקה, אבל מסתבר שזה לא מספיק. אקסיומות פיאו מספיקות כדי לדבר על מספרים, אבל אין להן מספיק כח כדי לדבר על קבוצות של מספרים. לכן, משתמשים במערכת אקסיומות אחרת שנקראות אקסיומות צרמלו-פרנקל, שמדברות על קבוצות. מתוכן אפשר להוכיח את אקסיומות פיאו, ולקודד מספרים ע"י קבוצות. לא נראה את כל האקסיומות האלה, שהם יותר מסובכות מאקסיומות פיאו.

בעולם של צרמלו-פרנקל יש יחס יחיד שהוא יחס השייכות  $x \in y$ , ואנחנו נסמן אותו ב-

$$In(x, y)$$

אם נזכר בשיעור הראשון, דיברנו על הפרדוקס של ראסל. הסיבה שיש יותר קושי בצרמלו-פרנקל זה בדיוק בגלל זה: אנחנו צריכים להגדיר את האקסיומות של המתמטיקה בצורה מספיק טובה כדי לא לקבל סתירות פנימיות. עד שראסל הציג את הפרדוקס שלו, לקחו כמובן מאליו את הדבר הבא כאקסיומה: לכל כלל אפשר למצוא את קבוצת כל האיברים שמקיימים את הכלל הזה. אבל מסתבר שזו לא אקסיומה טובה, כי זה לא קונסיסטנטי: כמו שהפרדוקס של ראסל מראה, לא כל דבר יכול להיות קבוצה, כי אם כן אז מגיעים מזה לסתירה.

מה שנעשה בתרגיל זה להראות שאם אומרים שכל דבר יכול להיות קבוצה אז מגיעים לסתירה, כלומר להראות שלכל נוסחא  $\phi$ , אם:

$$\exists y [\forall x [x \in y \leftrightarrow \phi(x)]]$$

אז אפשר להוכיח מזה גם  $z = z$  וגם  $z \neq z$ .

**11 שיעור 11 – 7.1.18****11.1 משפט הדדוקציה**

בתרגיל 11 נפתח כמה כלים מאוד שימושיים, שהם גם חשובים בפני עצמם, וגם ישמשו אותנו לקראת תרגיל 12, שיהיה גולת הכותרת של הקורס – משפט השלמות עם תחשיב הפרדיקטים.

הכלי הראשון הוא ואריציה לכלי שעשינו כבר בתחשיב הפסוקים, והוא משפט הדדוקציה. לפני שנעבור להגדרות פורמליות, נזכר מה אומר משפט הדדוקציה בתחשיב הפסוקים: אם יש לנו הרבה הנחות ואנחנו יודעים להוכיח מסקנה  $b$  מתוכן, אפשר מכל ההנחות חוץ מהנחה כלשהי  $a$  להוכיח את  $a \rightarrow b$ . ראינו שמשפט הדדוקציה הוא מעין ההפך של  $MP$ , שאומר לנו שאם יש הנחה כלשהי  $a$  ואנחנו יודעים להוכיח את  $a \rightarrow b$  אז אפשר להוכיח את  $b$ .

להוכיח את משפט הדדוקציה בתחשיב הפסוקים היה קשה מבחינה טכנית, כאן ההוכחה תהיה קצת יותר קלה מהבחינה הזאת, כי יש לנו בחינם טאוטולוגיה כבר בשלב הזה, ונוכל להשתמש בגרירות טאוטולוגיות.

לפני שננסח את המשפט בתחשיב היחסים, נזכר בניסוח שלו בתחשיב הפסוקים:

**משפט הדדוקציה לתחשיב הפסוקים** – תהיינה  $\varphi_1, \dots, \varphi_n, \psi, \xi$  נוסחאות של תחשיב הפסוקים, ויהא  $\Delta$  אוסף כללי היסק הכוללים את  $MP$ ,  $I_1$  ו- $I_2$  כך שכל שאר כללי היסק ב- $\Delta$  הם ללא הנחות. אם מתוך  $\varphi_1, \dots, \varphi_n, \psi$  ניתן להוכיח את  $\xi$  באמצעות  $\Delta$ :

$$\varphi_1, \dots, \varphi_n, \psi \vdash_{\Delta} \xi$$

$$\varphi_1, \dots, \varphi_n \vdash_{\Delta} (\psi \rightarrow \xi)$$

נשים לב שהייתה לנו כאן הנחה שכל כלל היסק מלבד  $MP$  הם ללא הנחות.

במשפט הדדוקציה של תחשיב הפסוקים השתמשנו להוכחות קטנות, והמקום הכי קריטי שהוא הופיע בו היה בהוכחה של משפט הטאוטולוגיה, שם היינו חייבים את משפט הדדוקציה וזה מה שגרם למשפט הטאוטולוגיה לפעול. גם בתחשיב היחסים משפט הדדוקציה ישחק תפקיד, והוא יעזור לנו בסופו של דבר להוכיח את משפט השלמות.

נעבור עכשיו להגדרה בתחשיב היחסים:

**משפט הדדוקציה לתחשיב היחסים** – תהיינה  $\varphi_1, \dots, \varphi_n$  סכמות ותהיינה  $\psi, \xi$  נוסחאות. אם  $\xi$  ניתנת להוכחה מתוך  $\varphi_1, \dots, \varphi_n, \psi$  ללא שימוש ב- $UG$  על משתנה שהוא חופשי ב- $\psi$ , אז  $(\psi \rightarrow \xi)$  ניתנת להוכחה מתוך  $\varphi_1, \dots, \varphi_n, US$ .

נבין מה רשום כאן:

- אנחנו כבר רואים הבדל ראשון מתחשיב הפסוקים:  $\varphi_1, \dots, \varphi_n$  הן סכמות ו- $\psi, \xi$  לא סכמות אלא נוסחאות. אנחנו לא רוצים ש- $\psi, \xi$  תהיינה סכמות כי אנחנו רוצים להוכיח את הגרירה ביניהן.
- ובמקום לכתוב ש- $\psi \rightarrow \xi$  ניתנת להוכחה מתוך  $\varphi_1, \dots, \varphi_n, US$  יכולנו גם לדרוש ש- $US$  יהיה אחד ה- $\varphi$ ים.
- בתחשיב הפסוקים היה תנאי שאומר שכלל הכללים הם ללא הנחות. אין לנו כבר את התנאי הזה, כי במערכת ההוכחה שהגדרנו בתרגיל 9 הגדרנו בדיוק שני כללי היסק עם הנחות ( $UG, MP$ ), וכל שאר כללי היסק הם סכמות, בלי הנחות. זה אומר שקיבלנו מראש את המגבלה הזאת, ולא נצטרך לדרוש אותה כאן בצורה מפורשת.



- נוספה לנו כאן מגבלה חדשה לגבי השימוש ב- $UG$ , שלא הייתה קודם כי אין מקביליה לזה בתחשיב הפסוקים. זו מגבלה שבלעדיה דברים בהוכחה שלנו לא היו נכונים, היא לא מגבלה טכנית. כדי להבין את המגבלה, נסתכל על דוגמא של משהו שאפשר להוכיח בשדות:

בהנתן  $(x + 1) \cdot 1 = 0$  אפשר להוכיח  $x = 0$  (כלומר, אם לכל  $x$  מתקיים  $(x + 1) \cdot 1 = 0$  אז לכל  $x$  מתקיים  $x = 0$ ).

למה זה נכון: להגיד  $(x + 1) \cdot 1 = 0$  זה שקול מבחינה לוגית ללהגיד  $x \cdot 1 = 0$ , כי אפשר להוריד 1, להפעיל את הההנחה ואז לחזור. מכאן אנחנו מסיקים שיש לנו כאן שדה שיש בו רק איבר אחד, איבר האפס. אם היינו מפעילים את משפט הדדוקציה בצורה חסרת אבחנה, היינו מקבלים  $x = 0 \rightarrow (x + 1) \cdot 1 = 0$ , וזה כבר לא נכון.

בשביל להבין למה זה לא נכון, נצטרך לשים לב להבדל בין מה שאנחנו רוצים להוכיח לבין מה שקיבלנו:  
 ○ אנחנו רוצים להוכיח:

$$(\forall x[(x + 1) \cdot 1 = 0] \rightarrow \forall x[x = 0])$$

○ מה שקיבלנו:

$$\forall x[(x + 1) \cdot 1 = 0 \rightarrow x = 0]$$

וזה כמובן לא אותו דבר.

ההגבלה של ה- $UG$  באה למנוע מאיתנו לעשות דברים כאלה. לא הוכחנו כאן עד הסוף למה אם לא עושים את זה אנחנו בסדר, אבל קצת השתכנענו שאם אנחנו עושים את זה אז בטוח זה לא בסדר.

האסטרטגיה הכללית לכתיבת ההוכחה תהיה דומה לתרגיל 5, שם עבור כל שורה של ההוכחה המקורית הוספנו שורה או אוסף שורות חדשות להוכחה החדשה, כך שאם השורה המקורית הוכיחה  $f$  אז סט השורות של ההוכחה החדשה מוכיח  $(\psi \rightarrow f)$ . זה בדיוק מה שנעשה גם כאן.

בשביל להבין מה לעשות עבור כל מקרה, נסתכל על ההוכחה הבאה:

$\forall x[(R(x) \rightarrow Q(x))]$	$A$	1
$(\forall x[(R(x) \rightarrow Q(x))] \rightarrow (R(x) \rightarrow Q(x)))$	$A, UI$	2
$(R(x) \rightarrow Q(x))$	$MP$	3
$(R(x) \rightarrow Q(x)) \rightarrow (\sim Q(x) \rightarrow \sim R(x))$	$T$	4
$(\sim Q(x) \rightarrow \sim R(x))$	$MP$	5
$\forall x[(\sim Q(x) \rightarrow \sim R(x))]$	$UG$	6

ההוכחה היא מתוך שתי הנחות,  $UI$  ו- $\forall x[(R(x) \rightarrow Q(x))]$  (ההנחה השנייה היא עבור  $R, Q$  ספציפיים, לא סכמה), והמסקנה היא  $\forall x[(\sim Q(x) \rightarrow \sim R(x))]$ .

אנחנו רוצים לקחת את ההוכחה הזאת, ולהפוך את זה להוכחה שמוכיחה רק מתוך  $UI$  את:  
 $(\forall x[(R(x) \rightarrow Q(x))] \rightarrow \forall x[(\sim Q(x) \rightarrow \sim R(x))])$

נסתכל קודם כל האם ההוכחה הזאת מקיימת את ההנחות של משפט הדדוקציה. אמנם יש בה  $UG$  על משתנה  $x$ , אבל הוא לא חופשי ב- $\psi$  (אלא הוא קשור ב- $\psi$ ), אז זה בסדר. באופן כללי, אם בהנחה שלנו יש כימות על כל המשתנים ואין משתנים חופשיים אז נדע מיד שאפשר להפעיל את משפט הדדוקציה ולא תהיה בעיה.

נבנה כעת את ההוכחה החדשה. כאמור, אנחנו רוצים לעבור שורה-שורה, ועבור כל אחת מהן להוכיח הנחה  $\leftarrow$  שורה. נעיר שכדאי לבנות את זה מומלץ מאוד להשתמש באובייקט  $Prover$ , שיקל על התהליך.

נפרט עבור כל שלב מה תהיה השורה האחרונה באוסף השורות שנוסיף, ואיך אפשר להגיע אליה –

1. השורה האחרונה:

$$prover.add\_('(\forall x[(R(x) \rightarrow Q(x))] \rightarrow \forall x[(R(x) \rightarrow Q(x))])')$$

איך נגיע אליה: השורה הזאת היא טאוטולוגיה, אז נוכל פשוט להשתמש ב- $add\_tautology$ .

2. השורה האחרונה:

$$prover.add\_('(\forall x[(R(x) \rightarrow Q(x))] \rightarrow (\forall x[(R(x) \rightarrow Q(x))] \rightarrow (R(x) \rightarrow Q(x))))')$$

איך נגיע אליה: בדומה למה שעשינו בתרגיל 5, לא נרחיב על זה עכשיו.

3. השורה האחרונה:

$$prover.add\_('(\forall x[(R(x) \rightarrow Q(x))] \rightarrow (R(x) \rightarrow Q(x)))')$$

איך נגיע אליה: זו שורה שהגיעו אליה עם  $MP$ , ונרצה להבין איך לתרגם אותה. נבין קדם מה יש לנו כאן ולמה אנחנו רוצים להגיע: בהוכחה המקורית היה לנו  $(A \rightarrow B)$  והסקנו  $B$  עם  $MP$ . עכשיו יש לנו  $(\psi \rightarrow A)$  ו- $(\psi \rightarrow (A \rightarrow B))$  ואנחנו רוצים להסיק  $(\psi \rightarrow B)$ . במשפט הדדוקציה בתחשיב הפסוקים השתמשנו ב- $I_2$  בשביל זה, אבל כאן זה אפילו פשוט יותר: נוכל להשתמש בגרירה טאוטולוגית על  $(\psi \rightarrow A)$  ו- $(\psi \rightarrow (A \rightarrow B))$  ולהסיק את מה שאנחנו רוצים.

4. זו שורה של טאוטולוגיה, לא נפרט איך מתרגמים אותה.

5. השורה האחרונה:

$$prover.add\_('(\forall x[(R(x) \rightarrow Q(x))] \rightarrow (\sim Q(x) \rightarrow \sim R(x))))')$$

איך נגיע אליה: בדומה ל-3.

6. השורה האחרונה:

$$prover.add\_('(\forall x[(R(x) \rightarrow Q(x))] \rightarrow \forall x[(\sim Q(x) \rightarrow \sim R(x))])')$$

איך נגיע אליה: נרצה לקחת את מה שהגענו אליו במקום שורה 5:

$$(\forall x[(R(x) \rightarrow Q(x))] \rightarrow (\sim Q(x) \rightarrow \sim R(x)))$$

להשתמש ב- $UG$ :

$$\forall x[(\forall x[(R(x) \rightarrow Q(x))] \rightarrow (\sim Q(x) \rightarrow \sim R(x)))]$$

ואז להשתמש ב- $US$ :

$$\forall x[(\forall x[(R(x) \rightarrow Q(x))] \rightarrow (\sim Q(x) \rightarrow \sim R(x))) \rightarrow (\forall x[(R(x) \rightarrow Q(x))] \rightarrow \forall x[(\sim Q(x) \rightarrow \sim R(x))])]$$

לבסוף נשתמש ב- $MP$  עם שני אלה, לקבלת השורה שאנחנו רוצים:

$$(\forall x[(R(x) \rightarrow Q(x))] \rightarrow \forall x[(\sim Q(x) \rightarrow \sim R(x))])$$

נעיר שני דברים בהקשר הזה –

a. אין לנו בעיה להשתמש ב- $UG$  בהוכחה שלנו, אין על זה הגבלה, המגבלה של  $UG$  במשפט הדדוקציה נוגעת להוכחה המקורית ולא להוכחה שאנחנו בונים.

b. בשביל להשתמש ב- $US$  על ביטוי כלשהו, אנחנו חייבים ש- $x$  יהיה לא חופשי בביטוי. לכן, אנחנו חייבים

שב- $\psi$  (שהיא ההנחה שאנחנו רוצים להוציא החוצה, במקרה שלנו  $\psi = \forall x[(R(x) \rightarrow Q(x))]$ ) יתקיים ש- $x$  הוא לא משתנה חופשי.

זה מובטח לנו מתוך ההנחה של משפט הדדוקציה: אנחנו יודעים שבהוכחה המקורית אם נתקלנו בהפעלה של  $UG$  היא בהכרח על משתנה שהוא לא חופשי ב- $\psi$ , אז נקבל שאין בעיה להשתמש ב- $US$ .

השורה האחרונה בשלב השישי נותנת לנו בדיוק את מה שרצינו להוכיח.

### 11.1.1 נאותות ההוכחה בשלילה מתוך משפט הדדוקציה

בחשיב הפסוקים ראינו שאחת התוצאות של משפט הדדוקציה היא המשפט שאומר למה הוכחות בשלילה פועלות. גם כאן נקבל משפט כזה:

☞ **משפט הנאותות של הוכחות בשלילה** – תהיינה  $\varphi_1, \dots, \varphi_n$  סכמות, תהא  $\psi$  נוסחא. אם ניתן להוכיח סתירה מתוך  $\psi, \varphi_1, \dots, \varphi_n$  מבלי להשתמש ב-UG על משתנה שחופשי ב- $\psi$ , אז  $\sim\psi$  ניתנת להוכחה מתוך  $\varphi_1, \dots, \varphi_n, US$ .

הסבר – אנחנו רוצים להוכיח מ- $\varphi_1, \dots, \varphi_n$  (ו- $US$ ) את  $\sim\psi$ . מה שאנחנו עושים זה להניח בשלילה ש- $\psi$  ולקבל סתירה, מה שאומר שאנחנו יודעים להוכיח סתירה מתוך  $\varphi_1, \dots, \varphi_n$  ו- $\psi$ . אם אפשר להוכיח סתירה מתוך  $\psi, \varphi_1, \dots, \varphi_n$  אז אפשר להוכיח: סתירה  $\rightarrow \psi$  (משפט הדדוקציה). התרגיל בבית זה לחשוב איך מ-סתירה  $\rightarrow \psi$  אפשר להוכיח  $\sim\psi$ .

הערה: החל מהתרגיל הזה והלאה כדאי להכיר את הפונ' *add\_proof* של האובייקט *Prover*. הפונקציה מאפשרת לקחת הוכחה ולהוסיף אותה לתוך ההוכחה הנוכחית, ומחזירה את מספר השורה בתוך ההוכחה שלנו שהוא המסקנה של ההוכחה שהוספנו. זה כמו *inline\_proof* רק בלי הנחות.

### 11.2 משפט צורת הקידומת הנורמלית (*Prenex Normal Form*)

כעת נעבור לדבר על החלק השני של תרגיל 11. בשביל זה נדרש להגדרה:

☞ **נוסחא בצורת קידומת נורמלית (prenex normal form)** – נוסחא  $\varphi$  נקראית בצורת קידומת נורמלית אם בראש העץ שלה קיימת קבוצת קדקודים שכולם קדקודי כמתים, ומלבד קדקודים אלה אין עוד קדקודי כמתים ב- $\varphi$ .

זו דרך מסובכת להגיד שכל ה- $\forall$  וה- $\exists$  בנוסחא נמצאים בהתחלה. דוגמאות:

- הנוסחא  $\forall x [\exists y [(R(x, y) | Q(x, c))]]$  היא בצורת קידומת נורמלית.
- הנוסחא  $\forall x [(R(x, y) | \exists y [Q(x, c)])]$  היא לא בצורת קידומת נורמלית, כי הכמת  $\exists$  נמצא מתחת ל- $|$ .
- הנוסחא  $\forall x [(\exists y [Q(x, c)] | R(x, y))]$  היא לא בצורת קידומת נורמלית, כי גם כאן הכמת  $\exists$  נמצא מתחת ל- $|$ .

למה זה מעניין אותנו: מסתבר שלכל נוסחא יש נוסחא שקולה בצורת קידומת נורמלית. מה הכוונה בשקולה שקולה: אפשר להוכיח שהנוסחא הראשונה גוררת את השנייה וגם השנייה גוררת את הראשונה. ההוכחה שלנו של משפט השלמות תשתמש בצורה חזקה בכך שכל נוסחא אפשר להביא למצב של קידומת נורמלית, ושאפשר להוכיח שהיא שקולה.

#### 11.2.1 תהליך המעבר לצורת קידומת נורמלית

בשביל לעשות את המעבר לצורת קידומת נורמלית, נעזר ברשימה של שקילויות:

$\sim\forall x[\phi(x)] \leftrightarrow \exists x[\sim\phi(x)]$	1
$\sim\exists x[\phi(x)] \leftrightarrow \forall x[\sim\phi(x)]$	2
$(\forall x[\phi(x)] \& \psi) \leftrightarrow \forall x[(\phi(x) \& \psi)]$	3
$(\psi \& \forall x[\phi(x)]) \leftrightarrow \forall x[(\psi \& \phi(x))]$	4
$(\exists x[\phi(x)] \& \psi) \leftrightarrow \exists x[(\phi(x) \& \psi)]$	5
$(\psi \& \exists x[\phi(x)]) \leftrightarrow \exists x[(\psi \& \phi(x))]$	6
$((\phi(x) \leftrightarrow \psi(x)) \rightarrow (\forall x[\phi(x)] \leftrightarrow \forall y[\psi(y)]))$	15
$((\phi(x) \leftrightarrow \psi(x)) \rightarrow (\exists x[\phi(x)] \leftrightarrow \exists y[\psi(y)]))$	16

הקבוצה הראשונה של השקילויות (1-14) מסבירה איך מוציאים כמתים החוצה מאופרטורים לוגיים. הרשימה המלאה של כל ארבע עשרה השקילויות מופיעה בתרגיל 11.

את כל השקילויות אפשר להוכיח מתוך שש האקסיומות של *Prover* (ולמעשה אפילו רק מתוך הארבע הראשונות). אנחנו נוכל בתרגיל להשתמש בהן כמו שהן, נקח אותן כאקסיומות. הצידוק לזה הוא כמו מה שדיברנו עליו בשיעור 6, אז דיברנו על משפט הטאוטולוגיה, ועבדנו עם סט מסויים של אקסיומות. גם אז אמרנו שיכולנו למעשה לקחת סט יותר קטן, אבל הפואנטה הייתה שמתוך מספר סופי של אקסיומות אפשר להוכיח הכל, לכן לא היה לנו ממש קריטי להגביל את עצמינו לסט היותר מצומצם, והעדפנו לעבוד עם הסט הנוח. כאן זה אותו הדבר.

נתחיל מלדבר על ארבע עשרה האקסיומות הראשונות, ונראה איך אפשר להפוך נוסחא לצורת קידומת נורמלית באמצעותן. נסתכל על הנוסחא:

$$\sim(z = x \mid \forall z[(\exists x[(x = z \& \forall z[z = x]]) \rightarrow \forall x[x = y]])]$$

הדבר הראשון שאנחנו רוצים לעשות זה להפוך את כל הכימותים לכימותים על משתנים עם שמות שונים:

$$\sim(z = x \mid \forall z_1[(\exists z_2[(z_2 = z_1 \& \forall z_3[z_3 = z_2]]) \rightarrow \forall z_4[z_4 = y]])]$$

את התהליך הזה נצטרך לעשות במשימה 4, ונצרך גם להוכיח שהשורה שקיבלנו שקולה למקור.

השלב הבא יהיה להתחיל להעביר את הכמתים להתחלה. בשביל לעשות את זה נוכל להעזר ב-14 האקסיומות הראשונות שלנו:

- נחליף את התוכן של  $\exists$  באמצעות אקסיומה 4:

$$\sim(z = x \mid \forall z_1[(\exists z_2[\forall z_3[(z_2 = z_1 \& z_3 = z_2)] \rightarrow \forall z_4[z_4 = y]])]$$

- נוציא החוצה את הכמתים שלפני ואחרי הגרירה:

$$\sim\left(z = x \mid \forall z_1\left[\forall z_2\left[\exists z_3\left[\forall z_4\left[\left((z_2 = z_1 \& z_3 = z_2) \rightarrow z_4 = y\right)\right]\right]\right]\right]\right]$$

- נוציא החוצה את הכמתים הנוותרים:

$$\exists z_1\left[\exists z_2\left[\forall z_3\left[\exists z_4\left[\sim\left(z = x \mid \left((z_2 = z_1 \& z_3 = z_2) \rightarrow z_4 = y\right)\right)\right]\right]\right]\right]$$

את שני המעברים האחרונים עשינו באמצעות השקילויות שקשורות לגרירה (אפשר למצוא רשימה מלאה בתרגיל 11, כאמור). למה הכמתים הפכו למה שהם הפכו: לפי החוקים של הוצאת כמת מגרירה, אפשר לראות שכמתים מצד ימין נשארים אותו הדבר ומשמאל הופכים לכמת השני.

## 11.2.2 הוכחת השקילות לצורה המקורית

עכשיו, כשברור לנו התהליך של איך דברים הופכים לצורה נורמלית, נרד לפרטים של איך מוכיחים שהנוסחא שקיבלנו שקולה לנוסחא המקורית.

### 11.2.2.1 הפיכת שמות המשתנים ליחודיים והוכחת שקילות

השלב הראשון הוא, כאמור, להפוך את כל שמות המשתנים הקשורים לשמות יחודיים (משימה 4). המימוש שלנו יהיה מימוש רקורסיבי. המקרים שאנחנו יכולים להתקל בהם:

(1) אופרטור בינארי – לדוגמא, נניח שנתון:

$$(\forall x[\forall y[R(x, y)]] \mid \exists y[\forall x[Q(x, y)]])$$

נקרא רקורסיבית לעצמנו על צד שמאל של האינדיקטור (זה הופך את כל המשתנים משמאל ליחודיים ומחזיר הוכחת

שקילות עבור צד שמאל) ואז נקרא לעצמנו על צד ימין (כנ"ל רק לצד ימין). נקבל את הביטוי:

$$(\forall z_3 [\forall z_4 [R(z_3, z_4)]] \exists z_1 [\forall z_2 [Q(z_2, z_1)]]])$$

ובנוסף תהיה לנו הוכחה אחת שצד שמאל שקול למה שהיה קודם, ואחת שצד ימין שקול למה שהיה קודם. את שתי ההוכחות אפשר לחבר עם גרירה טאוטולוגית, אז נקרא ל-*add\_proof* ונחבר:

(2) אופרטור אונרי – לדוגמא, נניח שנתון:

$$\sim \forall x [\forall y [R(x, y)]]$$

נקרא לעצמנו רקורסיבית עם מה שבתוך השלילה. נקבל חזרה:

$$\forall z_1 [\forall z_2 [R(z_1, z_2)]]$$

והוכחה לשקילות  $\forall z_1 [\forall z_2 [R(z_1, z_2)]] \leftrightarrow \forall z_1 [\forall z_2 [R(z_1, z_2)]]$  עכשיו אנחנו צריכים להוכיח ש-

$\forall x [\forall y [R(x, y)]] \leftrightarrow \sim \forall z_1 [\forall z_2 [R(z_1, z_2)]]$  ואת זה אפשר לעשות באמצעות גרירה טאוטולוגית (כי אם אנחנו יודעים  $((a \rightarrow b) \& (b \rightarrow a))$  אז נובע מזה ש-  $((\sim a \rightarrow \sim b) \& (\sim b \rightarrow \sim a))$ ).

(3) כמתים – זה המקרה היותר קשה. לדוגמא, נניח שנתון:

$$\forall x [\forall y [R(x, y)]]$$

אנחנו הולכים לקרוא רקורסיבית (הסדר חשוב):

1. קריאה רקורסיבית עם  $\forall y [R(x, y)]$ .

2. נקבל חזרה  $\forall z_1 [R(x, z_1)]$  והוכחת שקילות של  $\forall y [R(x, y)] \leftrightarrow \forall z_1 [R(x, z_1)]$ .

3. נייצר משתנה חדש  $z_2$ . הנוסחא שנחזיר היא  $substitute(x, z_2)$ .  $\forall z_2 + \forall z_1 [R(x, z_1)]$  (כדי לוודא ה- $x$  הקשורים לכמת  $\forall$  שהוחלף ל- $\forall z_2$  יהפכו ל- $z_2$ ).

4. אנחנו רוצים להוכיח  $\forall x [\forall y [R(x, y)]] \leftrightarrow \forall z_2 [\forall z_1 [R(z_2, z_1)]]$ . נסתכל על אקסיומה 15:

$$((\phi(x) \leftrightarrow \psi(x)) \rightarrow (\forall x [\phi(x)] \leftrightarrow \forall y [\psi(y)]))$$

זה בדיוק מה שאנחנו צריכים.

(4) יחס או שיוויון – זה מקרה הבסיס שלנו, במקרה כזה נחזיר פשוט את היחס והשיוויון כמו שהם, וההוכחה תהיה שהביטוי שקול לעצמו (שזה קל לעשות – טאוטולוגיה).

### 11.2.2.2 מעבר לצורת קידומת נורמלית והוכחת שקילות

לאחר שצלחנו את השלב הראשון של העברת הכמתים להיות יחודיים, נתקדם לקראת המעבר לצורת קידומת נורמלית והוכחת השקילות אליה. משימות 5-7 הן משימות עזר לקראת 8, שבו נוכיח את זה.

במשימה 5 צריך להוציא אוסף של כמתים מתוך אופרטור שלילה, דבר שאפשר לעשות באמצעות שתי האקסיומות הראשונות. לדוגמא, עבור הנוסחא:

$$\sim \forall x [\forall y [\forall z [R(x, y, z)]]]$$

נחזיר:

$$\exists x [\exists y [\exists z [\sim R(x, y, z)]]]$$

את זה נעשה את זה ברקורסיה:

1. נקח את הנוסחא ונקרא לעצמינו רקורסיבית עם שלילה של מה שבפנים, כלומר עם  $\sim \forall y [\forall z [R(x, y, z)]]$ .

2. נקבל חזרה הוכחה ש-  $\sim \forall y [\forall z [R(x, y, z)]] \leftrightarrow \exists y [\exists z [\sim R(x, y, z)]]$ .

3. נוסיף כמת קיים על שני הצדדים של השקילות. יהיה לנו:

$$\exists x [\sim \forall y [\forall z [R(x, y, z)]]]$$

-1

$$\exists x [\exists y [\exists z [\sim R(x, y, z)]]]$$

4. בהוכחה משלב 2 ראינו שקילות בין ביטויים. באמצעות אקסיומה 16 נוכל לקבל שקילות בין הביטויים עם כמת קיים לפני כל אחד מהם, כלומר נקבל:

$$\exists x [\sim \forall y [\forall z [R(x, y, z)]]] \leftrightarrow \exists x [\exists y [\exists z [\sim R(x, y, z)]]]$$

5. באמצעות אקסיומה 1 (או אקסיומה 2 במקרים אחרים) נקבל:

$$\exists x [\sim \forall y [\forall z [R(x, y, z)]]] \leftrightarrow \sim \forall x [\forall y [\forall z [R(x, y, z)]]]$$

6. לסיום, נשתמש בשתי השקילויות משלב 4 ומשלב 5 לקבלת מה שנחנו רוצים:

$$\sim \forall x [\forall y [\forall z [R(x, y, z)]]] \leftrightarrow \exists x [\exists y [\exists z [\sim R(x, y, z)]]]$$

משימה 6 מאוד דומה למשימה 5, רק שבמקום שלילה צריך לגרור החוצה מצד שמאל ומצד ימין של אופרטור בינארי.

במשימה 7 נדרשים למשוך אוסף של כמתים גם מצד ימין וגם מצד שמאל של אופרטור בינארי. לדוגמא, נגיד שנתון:

$$(\forall x [\forall y [R(x, y)]] \& \forall z [\forall w [Q(z, w)]])$$

אנחנו יודעים בשלב הזה למשוך כמת מכל צד של האופרטור, ורוצים למשוך את הכמתים משני הצדדים ולהוכיח שקילות. איך נעשה את זה:

1. נשתמש במשימה 6 כדי להראות שזה שקול ל:

$$\forall x [\forall y [(R(x, y) \& \forall z [\forall w [Q(z, w)]])]]$$

2. עכשיו רוצים להוציא החוצה את הכמתים מצד ימין. קודם כל נשתמש במשימה 6 כדי להראות שאם לא היה את הכמתים החיצוניים הכל היה בסדר, כלומר להראות ש:

$$(R(x, y) \& \forall z [\forall w [Q(z, w)]]) \leftrightarrow \forall z [\forall w [(R(x, y) \& Q(z, w))]]$$

3. עכשיו אנחנו רוצים לקחת את הדבר הזה, ולהגיד שאם שני אלה שקולים הם יהיו שקולים גם אם נכתוב  $\forall y$  בהתחלה, ואז שני הדברים שנקבל יהיו שקולים אם נכתוב  $\forall x$  בהתחלה. את זה באמצעות האקסיומות שקשורות לגרירה, ספציפית אקסיומה 15:

$$(\varphi(x) \leftrightarrow \psi(x)) \rightarrow (\forall x [\varphi(x)] \leftrightarrow \forall y [\psi(y)])$$

בזה אפשר לסיים את ההוכחה –

a. קיבלנו:

$$(\forall x [\forall y [R(x, y)]] \& \forall z [\forall w [Q(z, w)]]) \leftrightarrow \forall x [\forall y [(R(x, y) \& \forall z [\forall w [Q(z, w)]])]]$$

b. קיבלנו:

$$\forall x [\forall y [(R(x, y) \& \forall z [\forall w [Q(z, w)]])]] \leftrightarrow \forall x \left[ \forall y \left[ \forall z \left[ \forall w [(R(x, y) \& Q(z, w))] \right] \right] \right]$$

c. ומשני אלה נסיק את מה שצריך להוכיח:

$$(\forall x [\forall y [R(x, y)]] \& \forall z [\forall w [Q(z, w)]]) \leftrightarrow \forall x \left[ \forall y \left[ \forall z \left[ \forall w [(R(x, y) \& Q(z, w))] \right] \right] \right]$$

כעת, אנחנו כבר יכולים לפתור את משימה 8: להפוך נוסחא שכל המשתנים בה ייחודיים לנוסחא בקידומת נורמלית. זה כבר יהיה פשוט אחרי שיש לנו את כל המשימות הקודמות – אם נקבל שני דברים עם אופרטור בינארי ביניהם, נקרא לעצמנו ברוקורסיה על כל אחד מהם כדי שיהפוך להיות ב-prenex normal form, מזה נקבל שהנוסחא המקורית שקולה

לנוסחת ביניים שהיא הפעלת האופרטור הבינארי על כל אחד מהביטויים ב-prenex normal form (שחזרו אלינו מהרקורסיה), ועכשיו מה שנשאר זה להשתמש במשימה 7 כדי להראות שמנוסחת הביניים הזו אפשר למשוך החוצה את כל הכמתים ושזה ישאר שקול. בדומה, אם יש שלילה של משהו, נקרא לעצמנו ברקורסיה על ה"משהו" כדי שיהפוך להיות ב-prenex normal form, מזה נקבל שהנוסחא המקורית שקולה לנוסחת ביניים שהיא שלילה של הביטוי ב-prenex normal form (שחזר אלינו מהרקורסיה), ועכשיו מה שנשאר זה להשתמש במשימה 5 כדי להראות שמנוסחת הביניים הזו אפשר למשוך החוצה את כל הכמתים ושזה ישאר שקול.

## 12 שיעור 12 – 14.1.18

### 12.1 משפט השלמות בתחשיב היחסים

#### 12.1.1 ניסוח המשפט והוכחת הכיוון הפשוט

היום נדבר על משפט השלמות בתחשיב היחסים. נתחיל מהגדרת המשפט –

☞ **משפט השלמות לתחשיב היחסים** – קבוצה (אולי אינסופית) של נוסחאות היא עקבית (קונסיסטנטית) אם"מ יש לה מודל.

מה זאת אומרת "יש לה מודל" – יש מודל שבו אם עוברים על כל אחת מהנוסחאות בקבוצה הזאת ועושים לה *evaluate* במודל מקבלים אמת.

נזכר מהו מודל בתחשיב היחסים – בתרגיל 7 כתבנו מחלקת מודל. מודל מכיל עולם ( $universe$ ), מכיל משמעות עבור כל קבוע (לאיזה עצם מהעולם הקבוע ממופה) ומכיל משמעות עבור כל יחס (על כל  $n$ -יה של איברים מהעולם, אומר האם היחס הוא אמת הוא שקר עליהם). בשיעור הזה אנחנו הולכים להניח שאין לנו פונקציות ואין לנו את האופרטור שווה (ראינו בתרגיל 8 שאנחנו לא מאבדים ככה כח הבעה). לכן, כשנרצה לבנות מודל נצטרך למצוא עולם, משמעות לכל קבוע ומשמעות לכל קשר.

כמו בתחשיב הפסוקים, יש כאן את הכיוון הקל, של הנאותות, ואת הכיוון הקשה.

- → אם יש מודל לקבוצה אזי היא עקבית: זה הכיוון הקל. אנחנו כבר יודעים מה זה אומר שקבוצה לא עקבית, זה אומר שאפשר להוכיח ממנה סתירה. אנחנו רוצים להראות שאם יש לה מודל לא ייתכן שהיא לא עקבית:
  - נניח בשלילה שקיימת קבוצה שיש לה מודל והיא לא עקבית.
  - חוסר העקביות אומר שאפשר להוכיח מתוכה סתירה.
  - משפט הנאותות אומר שאם אנחנו מוכיחים נוסחא מתוך קבוצת נוסחאות, אזי הנוסחא שהוכחנו נכונה בכל מודל עבור קבוצת הנוסחאות שמתוכה הוכחנו את הנוסחא.
  - כלומר, זה שקיים מודל שהסתירה נכונה בו, וזה בלתי אפשרי (כי סתירה זה פסוק שלא נכון באף מודל).
- לכן, אם יש לקבוצה מודל אז נובע שאי-אפשר להוכיח מתוכה סתירה, כלומר נובע שהיא עקבית.
- ← אם הקבוצה עקבית אזי יש לה מודל: זה הכיוון הכבד והפחות מובן מאליו, ואותו נוכיח היום.
 

הערה: אנחנו מתייחסים לעקבי בתור מה שמקומות אחרים קוראים לפעמים עקבי סינטקטית, כלומר אי-אפשר להוכיח ממנו סתירה.

בסופו של דבר, אנחנו רוצים לדון בשאלה האם כל מה שנכון אפשר להוכיח. דיברנו על זה בהקשר של משפט הטאוטולוגיה, שאומר שכל טאוטולוגיה אפשר להוכיח. אמרנו אז שמעניין אותנו לדעת האם למשל כל דבר שנכון בכל שדה אפשר להוכיח עם אקסיומות השדה. נוכיח באמצעות משפט השלמות בדיוק את זה, שכל מה שנכון אפשר להוכיח.

#### 12.1.2 הוכחת משפט נוסף

☞ **משפט** – תהא  $F$  קבוצת נוסחאות ותהא  $\phi$  נוסחא. אם  $\phi$  נכונה בכל מודל של  $F$  אז אפשר להוכיח את  $\phi$  מתוך ההנחות  $F$ .

מה אומר המשפט: נחשוב למשל על  $F$  בתור הקבוצה של אקסיומות השדה. המשפט הזה אומר שאם יש הצהרה שנכונה בכל שדה אז אפשר להוכיח אותה מתוך אקסיומות השדה. זו למעשה גולת הכותרת של הקורס: לא רק שהשתכנענו



כבר שכל מה שאנחנו מוכיחים הוא נכון, אלא שעכשיו נשתכנע גם שעבור כל תכונה שקיימת במקרה בכל השדות, שזה מספר אינסופי, קיימת הוכחה שמצדיקה אותה.

זה מסביר למה במתמטיקה חוקרים את העולם סביבנו באמצעות הכלי הזה של הוכחות, שהוא כלי סינטקטי לחלוטין. הקשר בין נייר שכתובה עליו הוכחה בכתב יד לבין הנכונות של תכונה כלשהי בכל המודלים בעולם לא מובן מאליו.

הסברים נוספים על המשפט:

- מהי הקבוצה  $F$  – קבוצת נוסחאות שיכולה להיות אינסופית. אם למשל מדובר על אקסיומות פיאנו, שאת מהן היא סכמה,  $F$  מכילה את כל האינסטנסטים של הסכמות שיש בהנחות שלנו.
- מה הכוונה ב- $\phi$  נכונה בכל מודל של  $F$  – אם למשל נקח את  $F$  להיות אקסיומות השדה, אז כל המודלים של  $F$  זה כל השדות. אם  $\phi$  נכונה בכל שדה זה אומר שאפשר להוכיח אותה באמצעות אובייקט  $Proof$  מתוך אקסיומות השדה.
- נעיר שכדי להוכיח את המשפט הזה לא צריך לעבור מודל-מודל ולהראות שהנוסחא נכונה בכל אחד מהמודלים. יש כאן ניסוי מחשבתי – נניח שהייתה נוסחא שנכונה בכל מודל, אז היינו יכולים להוכיח אותה. הסיבה שמשפט השלמות חשוב זה כי הוא נותן את זה.

המשפט הזה אומר לנו שאין שום דבר שנכון בכל שדה שאיננו תוצאה סינטקטית הוכחתית של אקסיומות השדה. אין "צירופי מקרים" ודברים שמתקיימים בטעות בשדות – כל מה שאפשר להוכיח הוא נכון (משפט הנאותות), וכל מה שנכון אפשר להוכיח (הגרסא הזאת של משפט השלמות).

כשהיינו בתחשיב הפסוקים, קראנו למקבילה של המשפט הזה משפט הטאוטולוגיה עבור כללי היסק, ולמקבילה של המשפט הראשון שראינו קראנו משפט השלמות. הרבה ספרים קוראים גם למשפט הזה לזה משפט השלמות, וגם למשפט הטאוטולוגיה קוראים לפעמים משפט השלמות.

נוכיח את המשפט הזה מתוך משפט השלמות, שאותו נוכיח בהמשך. בהוכחה שלנו נניח ש- $\phi$  נכונה בכל מודל של  $F$ , ונתן הוכחה של  $\phi$  מתוך ההנחות  $F$ .

נוכיח כעת את המשפט הזה למקרה ש- $\phi$  היא משפט (כלומר נוסחא בלי משתנים חופשיים), ולאחר מכן נראה איך אפשר להפוך כל נוסחא שאינה משפט למשפט.

הוכחה למקרה ש- $\phi$  היא משפט:

- נניח ש- $\phi$  משפט. היות ש- $\phi$  נכונה בכל מודל של  $F$ , אין מודל ל- $F \cup \{\sim\phi\}$  (כי בכל מודל של  $F$  מתקיים ש- $\phi$  נכונה, אז אין שום מודל של  $F$  שבו  $\sim\phi$  נכונה).
- ממשפט השלמות,  $F \cup \{\sim\phi\}$  לא עקבית (כי אין לה מודל), כלומר ניתן להוכיח סתירה מ- $F \cup \{\sim\phi\}$ .
- לכן, ממשפט הנאותות של הוכחות בשלילה, מ- $F$  ניתן להוכיח  $\sim\sim\phi$ .
- כלומר, מ- $F$  ניתן להוכיח את  $\phi$ , וזה מה שרצינו להוכיח.

השתמשנו בהוכחה משפט הנאותות של הוכחות בשלילה, אותו ראינו בשיעור הקודם. המשפט אומר שאם מאוסף נוסחאות אפשר להוכיח סתירה, מהאוסף של כל הנוסחאות חוץ מאחת מהן אפשר להוכיח את השלילה של הנוסחא הזאת.

למה היינו צריכים את ההנחה ש- $\phi$  היא משפט: כשכתבנו פונקציה להוכחת הנאותות בשלילה היינו צריכים שיתקיים תנאי טכני לגבי הוכחת הסתירה שקיבלנו כקלט, זאת כדי שנוכל להשתמש שם במשפט הדדוקציה. התנאי היה שאין  $UG$  בהוכחה על משתנים שחופשיים ב- $\phi$ . לכן הנחנו כאן ש- $\phi$  היא משפט, ואז אין בעיה, כי אין בה משתנים חופשיים.

מה אנחנו עושים אם  $\phi$  היא לא משפט: נהפוך אותו למשפט, נריץ את כל ההוכחה הזאת ואז נחזור חזרה.

נגיד שב- $\phi$  יש  $x$  חופשי. כדי להפוך אותו ל- $\phi'$  שאין בו  $x$  חופשי:

- נפעיל עליו  $UG$  לקבלת  $\phi'$ . עכשיו יש לנו  $\phi' = \forall x[\phi(x)]$ , כלומר ה- $x$  כבר לא משתנה חופשי.
- נוכיח את  $\phi'$  כמו שהסברנו.
- נחזור מ- $\phi'$  ל- $\phi$  באמצעות  $UI$ .

כמו שראינו בשיעורים קודמים, זה הייתרון של הכמת האוניברסלי – אפשר לעבור מנוסחא בלי כימות אוניברסלי לנוסחא עם כימות אוניברסלי באמצעות  $UG$ , ואפשר לחזור חזרה באמצעות  $UI$ .

עכשיו אנחנו מבינים למה משפט השלמות חשוב: אם נצליח להוכיח את משפט השלמות, הצלחנו להוכיח שמאקסיומות החבורה אפשר להוכיח מה שנכון בכל חבורה, מאקסיומות השדה אפשר להוכיח כל דבר שנכון בכל שדה וכו'.

### 12.1.3 הוכחת משפט השלמות

נעבור עכשיו להוכיח עכשיו את משפט השלמות. בתור התחלה, אנחנו הולכים לעשות כמה הנחות מפשטות, ולהניח שכל הנוסחאות בקבוצה שקיבלנו הן:

1. משפטים
2. ב- $prenex normal form$

בהמשך נסביר איך משתמשים במה שעשינו בתרגיל 11 כדי להראות שזה נכון לכל נוסחא שהיא.

מה שנרצה לעשות בהוכחה זה לקחת קבוצה עקבית ולהראות שיש לה מודל. נעשה זאת ע"י כך שנבנה מודל לקבוצה, ואז נוכיח שהקבוצה נכונה במודל הזה.

#### 12.1.3.1 הקדמה להוכחה

כדי להבין יותר טוב את האסטרטגיה שלנו בהוכחה, נתחיל מלהסביר איך אנחנו הולכים לבנות את המודל.

בניית העולם ומתן משמעות הקבועים – היות שאין לנו שיוויון, אנחנו הולכים לנסות משהו שנשמע מאוד נאיבי ומסתבר שהוא מאוד חזק: ננסה לבנות מודל שהעולם שלו הוא קבוצת כל הקבועים שבמשפטים שקיבלנו, כך שהמשמעות של כל קבוע היא הקבוע עצמו.

הסבר על בניית העולם: נתונה לנו קבוצה של משפטים  $F$ . נסמן ב- $C$  את קבוצת כל שמות הקבועים שבתוכה. ננסה לבנות מודל (נזכיר שהעולם יכול איזה איברים שבא לנו: מספרים, קבוצות, מה שנרצה) שבו העולם הוא בדיוק כל השמות של הקבועים מתוך הנוסחאות האלה.

הסבר על משמעות הקבועים: ברגע שקבענו את זה להיות העולם, צריך להחליט מה המשמעות של כל קבוע, כלומר לכל קבוע שמופיע איפשהו בנוסחאות צריך להגיד איזה איבר בעולם הוא המשמעות שלו. אם לדוגמא מופיע באחת הנוסחאות הקבוע  $d50$ , נקח את המשמעות שלו להיות האיבר בעולם שהוא  $d50$ .

כדי שיהיה איזשהו סיכוי שהשיטה הזאת תצליח, זה קריטי להניח שאין אופרטור שווה. אם כן היינו מאפשרים אופרטור שיוויון, ייתכן שבאחת הנוסחאות היה כתוב לדוגמא  $c80 = d50$ . במקרה כזה היינו חייבים שלשני הקבועים האלה תהיה אותה המשמעות במודל כדי שהנוסחא תהיה נכונה בו, וזה אומר שהמודל שאנחנו בונים כבר לא מתאים לנוסחא (כי הרי אמרנו שהוא נותן לכל קבוע את המשמעות שהיא האיבר בעולם שהשם שלו הוא כמו של הקבוע). נזכיר בהקשר הזה את הדקות שהתעכבנו עליה כשהחלפנו את סימן השיוויון ביחס  $SAME$ : היחס יכול לכפות על שני איברים להתנהג אותו הדבר, אבל הוא לא יכול לכפות עליהם להיות בדיוק אותו האחד.

מתן משמעות ליחסים – לאחר שבנינו עולם ונתנו משמעות לקבועים, צריך להחליט מה עושים עם המשמעות של יחסים.

נניח שיש לנו יחס על שני איברים  $R$ , ואנחנו רוצים להחליט אם  $R(c1, d50)$  יקבל במודל שלנו אמת או שקר. ישנה סיטואציה מסויימת שבה הבחירה תהיה קלה במיוחד: אם במקרה בקבוצת הנוסחאות שקיבלנו אחת הנוסחאות היא  $R(c1, d50)$  או אחת הנוסחאות היא  $\sim R(c1, d50)$ . במקרה כזה, נפעל כך:

-  $R(c1, d50) \in F$ : אנחנו רוצים לבנות מודל שכל אחת מהנוסחאות בקבוצה תקבל ערך אמת. אם אחת מהנוסחאות היא  $R(c1, d50)$ , הדרך היחידה שבה הנוסחא הזאת תקבל אמת במודל היא אם  $R(c1, d50)$  יהיה אמת.

לכן, במקרה כזה נבחר  $R(c1, d50) = True$ .

-  $\sim R(c1, d50) \in F$ : בדומה, אם אחת הנוסחאות היא  $\sim R(c1, d50)$  חייבים להחליט ש- $R(c1, d50)$  יחזיר שקר, אחרת לא נקבל את המודל שאנחנו רוצים. לכן, במקרה כזה נבחר  $R(c1, d50) = False$ .

אנחנו יודעים שלא יכול להיות שגם  $R(c1, d50) \in F$  וגם  $\sim R(c1, d50) \in F$ , כי הקבוצה היא עקבית. זה שלקחנו קבוצה עקבית מבטיח שאין לנו את שתיהן. לכן, במקרה הפרטי הזה יש דרך אחת בדיוק שאפשר לבנות את המודל הזה.

האסטרטגיה שלנו בבניה – אם כן, האסטרטגיה הכללית שלנו להוכחה של משפט השלמות תהיה שנקח יחס על קבועים, ונוסיף נוסחאות לקבוצה שלנו כך שאו היחס על הקבועים או שלילתו ימצאו בקבוצה. כמו שראינו, באופן כזה יהיה לנו קל לבנות מודל.

עיקר הדיון שלנו בהמשך השיעור יהיה איך לוקחים קבוצה ומוסיפים לה את אחת משתי הנוסחאות האלה. נראה בהמשך שנצטרך גם עוד כמה תנאים כדי שהכל יפעל כמו שצריך.

### 12.1.3.2 הגדרות: קבוצה סגורה פרימיטיבית, אוניברסלית וקיומית

הגדרות – יהיו  $F$  קבוצת משפטים ב-*prenex normal form* ו- $C$  קבוצת הקבועים שב- $F$ .

1. נאמר ש- $F$  **סגור פרימיטיבית** ביחס ל- $C$  אם לכל יחס  $k$ -מקומי  $R$  שמופיע ב- $F$  ולכל  $\lambda_1, \dots, \lambda_k \in C$  אחת משתי הנוסחאות הבאות נמצאת ב- $F$ :

$$\begin{aligned} &a. R(\lambda_1, \dots, \lambda_k) \\ &b. \sim R(\lambda_1, \dots, \lambda_k) \end{aligned}$$

2. נאמר ש- $F$  **סגורה אוניברסלית** ביחס ל- $C$  אם לכל נוסחא ב- $F$  שמתחילה בכמת  $\forall$ :  $\forall x[\phi(x)]$  ולכל  $\lambda \in C$  מתקיים ש- $\phi(\lambda) \in F$ .

3. נאמר ש- $F$  **סגורה קיומית** ביחס ל- $C$  אם לכל נוסחא ב- $F$  שמתחילה בכמת  $\exists$ :  $\exists x[\phi(x)]$  קיים  $\lambda \in C$  כך ש- $\phi(\lambda) \in F$ .

הסבר לסגירות פרימיטיבית: אם יש קבוצת משתנים שסגורה פרימיטיבית ביחס לקבועים שלה, מאוד כל להגיד מה המשמעות של כל יחס כשבונים את המודל: לכל יחס  $k$ -ארי ולכל  $k$  איברים מהעולם, בודקים איזו מהנוסחאות מופיעה ב- $F$ : הנוסחא מ- $1a$  או הנוסחא מ- $1b$ . במקרה הראשון, מגדירים את היחס על האיברים האלה כאמת, ובמקרה השני מגדירים אותו כשקר.

האסטרטגיה הכללית שלנו תהיה להוסיף עוד ועוד נוסחאות לקבוצה עד שהיא תהיה סגורה פרימיטיבית ביחס לכל היחסים שלה. אבל נצטרך עוד שני תנאים חוץ מסגירות פרימיטיבית: סגירות קיומית ואוניברסלית. ההגדרה של סגירות אוניברסלית וסגירות קיומית מאוד קשורה לאיך שהגדרנו את הכמתים האלה.

הסבר לסגירות אוניברסלית: אם יש נוסחא כמו  $\forall x[\text{משהו}]$ , אפשר לקחת כל קבוע שקיים באיזושהי נוסחא, להציב אותו במשהו הזה והנוסחא הזאת גם תהיה ב- $F$ .

הערה: אנחנו כבר יודעים שאם  $\forall x[\phi(x)]$  נכון אז גם  $\phi(\lambda)$  נכון, אבל מה שאנחנו אומרים כאן זה משהו קצת אחר – אם הראשון מופיע בסט הנוסחאות שלנו אז גם השני מופיע.

הסבר לסגירות קיומית: בדומה לסגירות אוניברסלית, רק עם הקמת הקיומי. אנחנו דורשים שאם לדוגמא יש ב- $F$  את הנוסחא  $\exists x[R(x)]$  יהיה איזושהו קבוע,  $c500$  נגיד, כך ש- $R(c500) \in F$ , כי הנוסחא הזאת אומרת שקיים קבוע כך שזה מתקיים עבורו.

### 12.1.3.3 הוכחת משפט השלמות עם ההנחות המקלות

**משפט** – תהא  $F$  קבוצת משפטים ב- $PNF$  שהיא סגורה (כלומר סגורה פרימיטיבית, סגורה אוניברסלית וסגורה קיומית). אם  $F$  עקבית אז יש לה מודל.

זה משפט השלמות, פשוט לא לגבי קבוצה  $F$  כללית של נוסחאות, אלא לגבי קבוצה  $F$  שהיא ב- $PNF$  וסגורה. נוכיח את זה קודם, ואז נראה איך לוקחים כל קבוצה כללית של נוסחאות ומעבירים אותה לצורה הזאת (כבר ראינו בשבוע שעבר איך מעבירים ל- $PNF$ , אז נותר להראות איך מוסיפים לה נוסחאות כך שהיא תהיה סגורה).

מבחינת חיבור לתרגיל 12, משימה 1 צריך לכתוב פונ' שבודקת האם קבוצה סגור פרימיטיבית, אוניברסלית וקיומית, משימות 2-3 מוכיחות את המשפט הזה ומשימות 4-9 לוקחת קבוצה ומגדילות אותה עד שהיא הופכת לקבוצה סגורה.

#### הוכחה –

נבנה מודל  $M$  כך:

1. העולם יהיה  $C$ .
  2. לכל שם של קבוע  $\lambda$  נגדיר שמשמעותו היא  $\lambda \in C$ .
  3. לכל יחס  $k$ -מקומי  $R$  ולכל  $\lambda_1, \dots, \lambda_k$  שמות של קבועים, נגדיר ש- $\lambda_1, \dots, \lambda_k$  במשמעות של  $R$  אמ"מ  $R(\lambda_1, \dots, \lambda_k) \in F$ .
- (הערה: מה הכוונה ב- $\lambda_1, \dots, \lambda_k$  במשמעות של  $R$  – זה אומר שהמודל מחליט ש- $R(\lambda_1, \dots, \lambda_k) = \text{True}$ )

כעת, אפשר לחשוב על שני מקרים:

- אם  $M$  מודל עבור  $F$  – סיימנו. (כי אנחנו צריכים להוכיח שיש ל- $F$  מודל)
- אם  $M$  לא מודל עבור  $F$  – כלומר שקיימת  $\phi \in F$  שלא מסתפקת במודל (אם נקח את  $\phi$  ונעשה לה  $evaluate$  במודל אז נקבל  $False$ ). אנחנו נוכיח שמשמעות הדבר היא ש- $F$  קבוצה לא עקבית, מה שיביא אותנו לסתירה עם ההנחה על העקביות של  $F$ , ולכן יאמר שהמקרה הזה לא אפשרי.

טענת עזר: אם  $M$  לא מודל עבור  $F$ , קיימת  $\phi' \in F$  חסרת כמתים שלא מסתפקת ב- $M$ .

הוכחה: אמרנו שבמקרה כזה יש  $\phi \in F$  שלא מסתפקת ב- $F$ . אם ב- $\phi$  אין כמתים אז סיימנו, אחרת נראה שיש  $\phi' \in F$  עם כמת אחד פחות מאשר ב- $\phi$  שלא מסתפקת. את זה נוכל להפעיל עד שיגמרו כל הכמתים. כלומר, מספיק להראות שאם  $\phi \in F$  לא מסתפקת ב- $M$  אז יש  $\phi' \in F$  עם כמת אחד פחות שלא מסתפקת ב- $F$ . זה מספיק כי כל נוסחא היא סופית, לכן יש בה מספר סופי של כמתים, ואחרי מספר סופי של הפעלות נקבל נוסחא ללא כמתים שלא מסתפקת ב- $F$ . נחלק למקרים:

1.  $\phi$  מהצורה  $\forall x[\psi(x)]$ : כלומר, קיים איבר מהעולם של המודל כך ש- $\psi$  (האיבר) לא מסתפקת במודל (מה הכוונה ב- $\psi$  (האיבר): הפעלה של  $\psi$  על הקבוע שהשם שלו הוא כמו האיבר הזה). כלומר, קיים שם של קבוע  $\lambda \in C$  כך ש- $\psi(\lambda)$  לא מסתפקת ב- $M$ . מסגירות אוניברסלית, היות ש- $\forall x[\psi(x)] \in F$  ו- $\lambda \in C$ , גם  $\psi(\lambda) \in F$ . קיבלנו  $\psi(\lambda)$  שהוא ב- $F$  ולא מסתפקת במודל.
  2.  $\phi$  מהצורה  $\exists x[\psi(x)]$ : כלומר, לא קיים אף איבר מהעולם של המודל כך ש- $\psi$  (האיבר) מסתפקת במודל (כלומר, אין שום איבר מהעולם של המודל שאם נציב אותו ב- $\psi$  נקבל אמת, או בניסוח אחר: לכל איבר בעולם, האיבר)  $\psi$  לא מסתפקת במודל). מסגירות קיומית, היות ש- $\exists x[\psi(x)] \in F$  קיים  $\lambda \in C$  כך ש- $\psi(\lambda) \in F$ . קיבלנו  $\psi(\lambda)$  שלא מסתפקת במודל.
- (הערה: למה יש רק שני מקרים – כי  $F$  ב- $PNF$ ).

בשאלה 2 נתכנת בדיוק את הדבר הזה. אנחנו מקבלים  $\phi$ ,  $F$  כך ש- $\phi$  לא מסתפקת ב- $M$ , ורוצים לקבל  $\phi'$  חסרת כמתים שלא מסתפקת ב- $M$ . כדי למנוע מאיתנו לממש את זה בצורה של איטרציה על כל אחד מהאיברים ב- $F$  ובדיקה האם הוא נוסחא חסרת כמתים שלא מסתפקת, יש בתרגיל הגבלות תכנותיות שמבטיחות את זה. מה שמצופה מאיתנו לעשות במקום זה בדיוק את שני הדברים שעשינו עכשיו.

עכשיו נסיים, והסיום יהיה הפואנטה של כל ההוכחה הזאת, ויסגור לנו דברים.

הגדרה – נגדיר את הנוסחאות הפרימיטיביות שבונות את  $\phi'$  (שהיא נוסחא חסרת כמתים מ- $F$  שלא מסתפקת ב- $M$ ) להיות כל התת-נוסחאות של  $\phi'$  שבראשן יחס.

דוגמא להמחשת הכוונה: אם  $\phi' = (R(c, d) | (Q(a) \rightarrow \sim Q(d)))$  אז הנוסחאות הפרימיטיביות שבונות את  $\phi'$  הן:  $R(c, d), Q(a), Q(d)$ .

במילים אחרות, נוסחאות פרימיטיביות הן הפעלה של יחסים על קבועים (נזכור שכבר אין לנו פונקציות). להגיד ש- $\phi'$  בנויה על נוסחאות מסוימות זה להגיד ש- $\phi'$  מתקבלת מ- $\rightarrow, \sim, |, \&$  על הנוסחאות האלה. ההגדרה הזאת מניחה באופן חזק ש- $\phi'$  היא חסרת כמתים.

כעת נגדיר את סט הנוסחאות שמתאימות לנוסחאות הפרימיטיביות האלה מתוך  $F$ . אנחנו יודעים ש- $F$  סגורה פרימיטיבית, אז לכל נוסחא כזאת או היא או שלילתה ב- $F$ :

הגדרה – נסמן את קבוצת הנוסחאות הפרימיטיביות שבונות את  $\phi'$  ב- $G$ . נגדיר:

$$H = \{\psi \in F | \psi \in G \text{ או } \psi = \sim \xi \text{ for some } \xi \in G\}$$

זו בעצם קבוצת כל הנוסחאות הפרימיטיביות או השליליות שלהן מתוך  $F$ .

לדוגמא: אם יש נוסחא  $\phi' = (R(c, d) | (Q(a) \rightarrow \sim Q(d)))$  והקבוצה  $F$  כוללת את  $\sim R(c, d), Q(a), Q(d)$  אז  $H = \{\sim R(c, d), Q(a), Q(d)\}$ .

טענה – מ- $\{\phi'\} \cup H$  ניתן להוכיח סתירה.

למה זה יספיק: כי  $H$  זה תת-קבוצה של  $F$  ו- $\phi'$  זו נוסחא חסרת כמתים ב- $F$ , אז זו תהיה הוכחה של סתירה מתוך  $F$ , וזה יסיים להוכיח ש- $F$  לא עקבית.

למה זה נכון: נזכר בתרגיל 6, שם הייתה משימה שבה בנינו מתודה בשם *prove\_in\_model*. מה המתודה הזאת אומרת לנו – שבתחשיב הפסוקים, אם יש כמה נוסחאות אטומיות (נסמן ב- $G$  את סט הנוסחאות האטומיות) ויש מודל שבו כ"א

מקבלת ערך אמת או שקר, ובונים קבוצה  $H$  כך שכל אחד מהאיברים ב- $G$  נמצא בה אם הוא מקבל אמת והשלילה שלו נמצאת בה אם הוא מקבל שקר, כל דבר שנכון במודל הזה אפשר להוכיח מתוך  $H$ .

נטען שכאן יש כמעט אותו הדבר. נרצה להוכיח שמ- $H$  ניתן להוכיח את  $\phi'$  (נזכור ש- $\phi'$  לא מסתפקת ב- $M$ , אז השלילה שלה בן מסתפקת ב- $M$ ). יש לנו מודל שבנוי מהפסוקיות האטומיות שב- $G$ , יש לנו נוסחא שמסתפקת במודל, אזי אפשר להוכיח אותה מתוך ההנחות האלה. למה מותר להפעיל כאן דברים מתחשיב הפסוקים: כי זה בדיוק מה שיש לנו כאן – נוסחאות אטומיות עם קשרים ביניהם. אין לנו שיוויון או כמתים, לכן אפשר להפעיל את זה ככה כמו שהוא. פורמלית, אפשר להחליף כל אחד מה"פסוקיות האטומיות" האלה במשתנה  $z_i$ , אבל אנחנו לא נצטרך לעשות את זה בתרגיל, כי אפשר להשתמש בגרירות טאוטולוגיות ולהסיק שמ- $H$  ניתן להוכיח את  $\phi'$ .

אם אפשר להוכיח את  $\phi'$  מתוך  $H$  אז אפשר להוכיח אותה גם מתוך  $F$ , כי  $H \subseteq F$ . זה אומר שאפשר להוכיח את  $\phi'$  ואת  $\phi'$  מ- $F$ , וזו סתירה.

כך הוכחנו את המשפט שאומר שכל נוסחא סגורה ב- $PNF$ , אם היא עקבית אז יש לה מודל.

#### 12.1.4 תרגיל 12

כבר ראינו מה עושים במשימות 1-2. נדבר קצת על שאר התרגיל:

משימות 4-9: מה שנשאר לעשות, ונעשה בפירוט בשיעור הבא, זה להראות שאם אנחנו יכולים לקחת קבוצת נוסחאות ולהפוך אותה להיות סגורה.

סגירות פרימיטיבית: התחלנו עם קבוצה עקבית, רוצים להוסיף לה פרימיטיביים ושהיא תשאר עקבית. לכל נוסחא פרימיטיבית שאנחנו רוצים שתהיה שם, אנחנו רוצים להראות שאפשר להוסיף או אותה או את שלילתה לקבוצה המקורית כך שלפחות אחת מההוספות תשאיר את הקבוצה עקבית. קשה מאוד לבדוק במחשב איזו מהן להוסיף כדי שהיא תשאר עקבית, קל להוכיח שאפשר להוסיף את אחת מהן. מה שנוכיח זה שאם  $F \cup \{\phi\}$  לא עקבית וגם  $F \cup \{\sim\phi\}$  לא עקבית, אז מראש  $F$  לא עקבית (וזו כמובן סתירה לעקביות של  $F$ ).

משימה 5: יש  $F$  ויש נוסחא שמכילה את הכמת  $\forall$ . אנחנו רוצים להוסיף את כל האינסטנסטים שלה. משימה 5 מראה שאנחנו לא נגרום לסתירה אם נעשה את ההוספה הזאת. מה הכוונה – אם  $F$  מכילה נוסחא אונברסלית  $\forall x[\phi(x)]$ , אם  $F$  כשמוסיפים לה את  $\phi(\lambda)$  לא עקבית, אז גם קודם היא הייתה לא עקבית. אז זה עושים לכל  $\lambda$ .

משימה 6: מקבלים אוסף נוסחאות, צריך להפוך אותו לסגור אוניברסלי. כלומר, להוסיף את כל האינסטנסטים של הנוסחאות שכוללות  $\forall$ . גם חלק מהאינסטנסטים האלה עשויים לכלול כמת  $\forall$ , אז גם עליהם צריך לעבור ולהוסיף את כל האינסטנסטים שלהם וכך הלאה (כאמור, כל נוסחא היא באופן סופי, לכן נעשה את זה מספר סופי של פעמים).

משימה 8: נראה שמותר להוסיף עד קיומי: אם יש נוסחא  $\exists x[\psi(x)]$  ולוקחים קבוע חדש  $c500$  שלא מופיע באף אחת מהנוסחאות ב- $F$ , אפשר להוסיף את  $\psi(c500)$  ל- $F$  ושהיא תשאר עקבית. נעשה את זה כמו שעשינו במקרים הקודמים: נראה שאם אחרי ההוספה של  $\psi(c500)$  הקבוצה  $F$  לא עקבית אז גם קודם היא לא הייתה עקבית. במקרה הזה אנחנו לא רק מגדילים את סט הנוסחאות, אנחנו גם מגדילים את סט הקבועים  $C$  שהוא סגור ביחס אליו. בשבוע הבא נדבר על למה השלב הזה עושה בעיות, כלומר למה הוא מפריע למה שעשינו בשלבים הקודמים.

**13 שיעור 13 – 21.1.18****13.1 משפט השלמות והוכחתו**

נדבר כעת על גולת הכותרת של כל הקורס, משפט השלמות. המשפט מדבר על הקשר בין הסינטקס לסמנטיקה, הפעם עבור תחביר הפרדיקטים. את רוב העבודה עשינו בתרגיל 12, ועכשיו נסיים את ההוכחה עד הסוף.

✎ **משפט השלמות לתחשיב היחסים** – כל קבוצת פסוקים  $F$  עקבית אמ"מ יש לה מודל.

המילה עקבית על פניו נותנת לנו מידע סינטקטי: זה לא מדבר על האם משהו נכון או לא נכון, אלא על זה שאי אפשר להוכיח סתירה מתוך הקבוצה. משפט השלמות נותן לנו את הקשר לסמנטיקה, שאם קבוצה היא עקבית אז יש לה מודל. אילו לא היה מודל, כלומר משהו לא יכול להתקיים בעולם האמיתי, היינו רואים את זה מכך שאפשר להוכיח מתוך הקבוצה סתירה. כל דבר שהוא נכון אפשר להוכיח.

בשיעור שעבר ראינו את משפט השלמות עבור קבוצה  $F$  סגורה ב- $PNF$  (אלה משימות 3-1 בתרגיל 12). לגבי קבוצה מהסוג הזה הוכחנו שאם היא עקבית יש לה מודל ולהפך.

נגדיר סגירות של קבוצה לפי:

✎ **הגדרה** – קבוצת פסוקים עקבית  $F$  נקראית סגורה ביחס לקבוצת קבועים  $C$  אם:

1. סגירות פרימיטיבית: לכל יחס  $k$ -מקומי  $R$  ולכל  $c_1, \dots, c_k \in C$ :  
 $a. R(c_1, \dots, c_k) \in F$  או  
 $b. \sim R(c_1, \dots, c_k) \in F$
2. סגירות אוניברסלית: לכל  $\forall x[\varphi(x)] \in F$  ולכל  $c \in C$ :  $\varphi(c) \in F$
3. סגירות קיומית: לכל  $\exists x[\varphi(x)] \in F$  קיים  $c \in C$ :  $\varphi(c) \in F$

ראינו בשיעור שעבר שברגע שהסגירות הפרימיטיבית קיימת מאוד ברור מה הולך להיות המודל – עבור יחס  $R$  כמו שמופיע בהגדרה וכל קבוצה של  $k$  קבועים, אם  $R(c_1, \dots, c_k) \in F$  אז  $R(c_1, \dots, c_k) = True$  ואם  $\sim R(c_1, \dots, c_k) \in F$  אז  $R(c_1, \dots, c_k) = False$ . הסגירות האוניברסלית והקיומית סוגרות לנו את הפינה לגבי דברים שיש בהם כמתי לכל וקיים.

בשיעור ראינו שאם הקבוצה מקיימת את שלושת חוקי הסגירות האלה, אם היא עקבית יש לה מודל. את ההוכחה לזה עשינו בתרגיל 12.

כעת, מתוך זה אנחנו רוצים להסיק את משפט השלמות הכללי, בלי הגבלות על הסגירות של הקבוצה או על צורת הנוסחאות. נעשה את זה באמצעות המשפט הבא:

✎ **משפט** – לכל קבוצת פסוקים עקבית  $F$  וקבוצת קבועים  $C$  קיימת קבוצת פסוקים עקבית  $\bar{F} \subseteq F$  וקבוצת קבועים  $\bar{C} \subseteq C$  כך ש- $\bar{F}$  סגורה ביחס ל- $\bar{C}$ .

למה זה עוזר לנו: נוכל לקחת את קבוצת הפסוקים המקורית ולהרחיב אותה לקבוצת פסוקים סגורה. לפי המשפט שהוכחנו בתרגיל 12, לקבוצה הסגורה יש מודל. מכיוון שקבוצת הפסוקים המקורית שלנו מוכלת בקבוצת הפסוקים החדשה, המודל הזה הוא מודל גם לקבוצה המקורית, וזה מסיים את מה שאנחנו רוצים להוכיח.

איך נעשה את זה: ע"י הוספת קבועים ל- $F$  תוך שמירתה עקבית. אלה משימות 4-9 בתרגיל 12. בתרגיל הוכחנו את הלמות הבאות –

למה – תהי  $F$  קבוצת פסוקים עקבית. אזי:

- לכל  $\varphi = R(c_1, \dots, c_k)$  או  $F \cup \{\varphi\}$  או  $F \cup \{\sim\varphi\}$  עקבית.
- לכל  $\forall x[\varphi(x)] \in F$  ולכל  $c \in C$   $F \cup \{\varphi(c)\}$  עקבית.
- לכל  $\exists x[\varphi(x)] \in F$  וקיים  $c$  חדש:  $F \cup \{\varphi(c)\}$  עקבית.

איך הוכחנו את הנקודה הראשונה: בשלילה. אמרנו שנניח שיש סתירה מהוספה של  $\varphi$  ל- $F$  וגם יש סתירה מהוספה של  $\sim\varphi$  ל- $F$ , והראנו שזה אומר שאפשר לצור הוכחה של סתירה ישירות מ- $F$ .

נקודה שנייה: באופן דומה, הראנו שאם יש קבוצה עקבית ויש פסוק שמתחיל בכמת  $\forall$ , אפשר להוסיף את  $\varphi(c)$  ל- $F$  לכל קבוע  $c$  זה עדיין נשאר עקבי. גם כאן הגענו לזה על ידי הנחה בשלילה – לקחנו הוכחה של סתירה בעקבות הוספה כזאת של פסוק לקבוצה, ויצרנו בעזרתה הוכחה של סתירה מתוך  $F$ .

נקודה שלישית: הוספנו למערכת הקבועים שלנו קבוע חדש שלא קיים בעולם, והראנו שזה עקבי. גם כאן פעלנו בשיטה של הנחה בשלילה – לקחנו הוכחה של הוספה שגורמת לסתירה, והוכחנו שיש סתירה כבר ישירות מ- $F$ .

נוכיח עכשיו את המשפט שבעזרתו אמרנו שאפשר להוכיח את משפט השלמות.

הוכחה: נתחיל מבנייה –

- נקח  $F_0 = F$  ונבנה סדרה אינסופית של קבוצות פסוקים עקביות:

$$F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots$$

ונקח  $C = C_0$  ונבנה סדרה אינסופית של קבוצות קבועים:

$$C_0 \subseteq C_1 \subseteq C_2 \subseteq \dots$$

ובסוף נגדיר:

$$\bar{F} = \bigcup_i F_i, \quad \bar{C} = \bigcup_i C_i$$

(ככה אפשר להגדיר במתמטיקה את הסוף של תהליך אינסופי – מגדירים בסוף את האיחוד של הכל.)

- מעבר מ- $F_{i-1}$  ל- $F_i$  ו- $C_{i-1}$  ל- $C_i$ :

נזכור מה המטרה שלנו במעבר – לקבל משהו שהוא יותר סגור. איך נקבל משהו שהוא יותר סגור: לגבי כל אחד מהתנאים בלמה, נוסיף את מה שצריך. באופן יותר פורמלי:

נוסיף ל- $C_{i-1}$  את הדברים הבאים:

- לכל  $R(c_1, \dots, c_k) \in C_{i-1}$  כך ש- $c_1, \dots, c_k \in F_i$  נוסיף אותו את שלילתו ל- $F_i$  כך שישאר עקבי.
- לכל  $\forall x[\varphi(x)] \in F_{i-1}$  ולכל  $c \in C_{i-1}$  נוסיף את  $\varphi(c)$  ל- $F_{i-1}$ .
- לכל  $\exists x[\varphi(x)] \in F_{i-1}$  נוסיף  $\varphi(c^*)$  ל- $F_{i-1}$  כאשר  $c^*$  משתנה חדשה ונוסיף את  $c^*$  גם ל- $C_{i-1}$ .

ככה עוברים מ- $F_{i-1}$  ל- $F_i$  ומ- $C_{i-1}$  ל- $C_i$  תוך שמירה על עקביות של  $F_i$ .

נשים לב שבכל שלב אנחנו מנסים לשפר את המצב על ידי כך שאנחנו מתקדמים לסגירות, אבל מצד שני בכל שלב נוספים קבועים חדשים שצריכים להיות סגורים גם ביחס אליהם. כל הדברים האלה יפתרו באינסוף. נראה את זה עכשיו באמצעות הוכחה של שתי טענות:

- טענה א':  $\bar{F}$  עקבית.



• טענה ב':  $\bar{C}$  סגורה ביחס ל- $\bar{C}$ .

הנכונות של שתי הטענות האלה לא מובן מאליו: דבר ראשון, לא התייחסנו כאן בצורה מפורשת לאפשרות של כמתים מכוננים (בתרגיל כן התייחסנו לזה מפורשות). בנוסף, בכל פעם שאנחנו מגיעים לכמת קיים אנחנו מוסיפים משתנה חדש, אז צריך לוודא שעבור כל פסוקי הלכל שנתקלנו בהם קודם לכן ועבור כל היחסים תהיה התייחסות למשתנה הזה.

הוכחת טענה א': נוכיח את זה באופן דומה לאיך שהוכחנו את משפט השלמות בתחשיב הפסוקים:

- נניח בשלילה ש- $\bar{F}$  לא עקבית.
- זה אומר שיש הוכחה של סתירה מ- $\bar{F}$ .
- בגלל סופיות ההוכחה, אנחנו יודעים שיש מספר סופי של פסוקים מ- $\bar{F}$  שמופיעים בהוכחה.
- זה אומר שקיים  $i$  כך שכל פסוקי ההוכחה נמצאים כבר ב- $F_i$  (כי יש מספר סופי של פסוקים וכל קבוצה  $F_k$  מכילה את כל הקבוצות שלפניה  $F_{j < k}$  ועוד פסוקים).
- זה אומר ש- $F_i$  לא עקבית בסתירה לבנייה, שעשינו אותה כך ש- $F_i$  נשארת עקבית.

הוכחת טענה ב': נראה שאנחנו עומדים בכל אחד מסוגי הסגירות –

סגירות פרימיטיבית: יהיו  $\bar{C}$  ו- $c_1, \dots, c_k \in R$  יחס כלשהו. צריך להראות: או ש- $F_{i+1} \in R(c_1, \dots, c_k)$  או  $\sim R(c_1, \dots, c_k) \in F_{i+1}$  (כדי להראות את הסגירות הראשונה).

1. נמצא  $i$  כך ש- $c_1, \dots, c_k \in C_i$ .  
איך אנחנו יודעים שיש כזה: אנחנו יודעים שכל ה- $c_i$  נמצאים ב- $\bar{C}$ .  $\bar{C}$  הוא איחוד של כל הקבוצות  $C_k$ , לכן אנחנו יודעים שכל אחד מהקבועים בנפרד נמצא באיזשהו  $C_k$ . כל  $C_k$  כולל את כל הקבועים שהופיעו לפניו ועוד אולי קבועים חדשים, לכן בשלב מסוים נגיע לקבוצה שכוללת את כל הקבועים, ואותה נקח.
2. לכן, כבר ב- $F_{i+1}$  אחד מהפסוקים הנדרשים נמצא. זאת מהבנייה שלנו: שכשעברנו מ- $i$  ל- $i+1$  הוספנו בדיוק את הפסוק הזה.

מכאן הוכחנו שאנחנו עומדים בתנאי הסגירות הראשון.

סגירות אוניברסלית: צריך להראות שאם  $\forall x[\varphi(x)] \in \bar{F}$  ו- $c \in \bar{C}$  אז  $\varphi(c) \in \bar{F}$ .

1. נמצא  $i$  כך ש- $c \in C_i$  וכך ש- $\forall x[\varphi(x)] \in F_i$  (שייך ל- $F_i$  (שוב, למה בכלל אנחנו יודעים שיש כזה – בדיוק כמו קודם, כי במעבר מ- $i$  ל- $i+1$  אנחנו רק מרחיבים את הקבוצות  $F_i$  ו- $C_i$  ואנחנו יודעים שזה קיים באיחוד של כל הקבוצות).
2. זה אומר ש- $\varphi(c) \in F_{i+1}$ .

סגירות קיומית: אם  $\exists x[\varphi(x)] \in \bar{F}$ :

1. קיים  $i$  כך ש- $\exists x[\varphi(x)] \in F_i$ .
2. קיים  $c \in C_{i+1}$  כך ש- $\varphi(c) \in F_{i+1}$  (למה אנחנו יודעים את זה – כי זה בדיוק מה שעשינו בבנייה בשלב האחרון).

בזה הוכחנו שלוקחים קבוצה ואפשר להשלים אותה לקבוצה סגורה. במתמטיקה לא טורחים לדבר על קבוצה סגורה לרוב, אלא עושים את אותו טריק שעשינו בתחשיב הפסוקים: לוקחים קבוצה מקסימלית, ואז היא כבר כוללת את כל מה שאנחנו רוצים.

נעיר על הבדל בין מה שעשינו כאן לבין מה שהיה בתרגיל 12: בתרגיל טיפלנו בכמת הקיומי ובכמת האוניברסלי בנפרד, לכן מה שעשינו נגמר בזמן סופי. כאן אנחנו מערבבים אותם, אז זה לא דווקא ייגמר בזמן סופי.

**13.1.1 הערות של משפט השלמות – גודל המודל ומשפט הקומפקטיות**

נעיר שתי הערות, ובכך נסיים את גולת הכותרת של הקורס.

**13.1.1.1 גודל המודל שבנינו**

נניח שהתחלנו מקבוצת פסוקים שהיא סופית או בת־מנייה, ונשאל את עצמנו מה גודל המודל שיצרנו כאן.

התשובה תהיה שזה אינסוף שגם הוא בן־מנייה. התחלנו ממצב שבו הכל בן מבנייה ובכל שלב הוספנו מספר פסוקים שהוא בן־מנייה (כי  $C$  בן מנייה), ולכן קיבלנו מודל בן מנייה.

זה מעט משונה, כי אנחנו יכולים להסיק מזה שלצרמלו-פרנקל יש מודל שהוא בן מנייה. אמרנו שצרמלו-פרנקל זה כל המתמטיקה, אז איך יכול להיות שבנינו מודל בן־מנייה של כל המתמטיקה אם יש במתמטיקה גם דברים לא בני־מנייה?

התשובה לכך היא שאין כאן סתירה, אלא זה עניין של נקודת מבט. להיות בן־מנייה זה תלוי בעולם שלך, כי זה אומר שיש בעולם שלך פונ' חח"ע שממפה בין מספרים הטבעיים לבין קבוצה כלשהי. אם פונקציה חח"ע כזאת לא קיימת בתוך המודל שלנו, זה אומר שבתוך המודל שלנו הקבוצה הזאת היא לא בת־מנייה. אולם, כשאנחנו מסתכלים מנקודת מבט שהיא מחוץ למודל יש לנו יותר פונקציות חח"ע, וזה אומר שהמודל שלנו כן יכול להיות בן־מנייה. זה אומר שצריך לחשוב טוב כשיש מצבים של עולם בתוך עולם.<sup>15</sup>

שורה תחתונה: התחלנו עם מספר פסוקים וקבועים בן־מנייה, אז גם התוצאה בת־מנייה.

**13.1.1.2 משפט הקומפקטיות**

**משפט הקומפקטיות** – לקבוצת פסוקים יש מודל אם לכל תת־קבוצה סופית שלה יש מודל.

כיוון אחד ברור: אם לקבוצת פסוקים יש מודל, הוא מתאים גם לכל תת־קבוצה סופית שלה.

את הכיוון השני נוכיח בדיוק כמו בתחשיב הפסוקים: מסופיות ההוכחה. נניח בשלילה שיש קבוצת פסוקים כל שלכל תת־קבוצה סופית שלה יש מודל, אבל לקבוצה אין מודל. לפי משפט השלמות, אפשר להוכיח ממנה סתירה (כי אם היא הייתה עקבית היה לה מודל). ההוכחה של הסתירה היא משהו סופי, לכן היא משתמשת רק בתת קבוצה סופית של פסוקים. לכן זה אומר שלתת הקבוצה הזאת לא יכול להיות מודל, בסתירה.

**13.2 סיכום הקורס**

בקורס היו לנו 12 שיעורים ו-12 תרגילים. נעשה סקירה כוללת של מה שראינו.

**13.2.1 סיכום: תחשיב הפסוקים****13.2.1.1 שימוש בטאוטולוגיות מתחשיב הפסוקים בתחשיב היחסים**

מנקודת המבט שיש לנו עכשיו, לאחר שסיימנו גם את תחשיב היחסים, אנחנו יכולים להגיד שהסיבה העיקרית שעברנו דרכו היא כדי לדעת להוכיח טאוטולוגיות בתחשיב היחסים, שם הרשנו כחלק ממה מותר בהוכחה להגיד ששורה מסויימת היא טאוטולוגיה.

נשאלת השאלה למה זה היה בכלל צעד נכון – הבדיקה של האם שורה היא טאוטולוגיה היא בדיקה סמנטית של האם היא נכונה, והוכחות הן אובייקט סינטקטי. התשובה היא שאפשר היה לעשות את זה בצורה סינטקטית לחלוטין, לכן אין בעיה (בקורס לא עשינו זאת מטעמים של קוצר זמן וחסכון).

נראה כיצד אפשר היה לעשות זאת: עבור טאוטולוגיה שהשתמשנו בה כמו שהיא בתחשיב היחסים, אפשר היה להוכיח את השלד של ההוכחה בתחשיב הפסוקים, ואז לתרגם את ההוכחה לתחשיב היחסים.

<sup>15</sup> לקריאה נוספת בנושא: [https://en.wikipedia.org/wiki/Skolem%27s\\_paradox](https://en.wikipedia.org/wiki/Skolem%27s_paradox)

בשביל זה צריך שלכל האקסיומות שראינו בתחשיב הפסוקים תהיה סכמה מתאימה בתחשיב היחסים. לדוגמא, עבור:

$$I1: (p \rightarrow (q \rightarrow p))$$

אפשר היה לקחת את הסכמה:

$$(PQ \rightarrow (QQ \rightarrow P))$$

כש- $P, Q$  הם  $templates$ .

אם עבור כל אחת מאקסיומות תחשיב הפסוקים היינו מגדירים סכמה מתאימה בצורה כזאת, איתן (בנוסף ל- $MP$ ) אפשר היה להוכיח בהוכחה של תחשיב היחסים כל טאוטולוגיה בתחשיב הפסוקים. מבחינה טכנית אנחנו עדיין יכולים להוסיף את הפונקציונליות הזאת למה שבנינו: אפשר לקחת את מה שבנינו בתרגיל 12 ולהוסיף לו פונקציה שמחליפה כל שורת טאוטולוגיה (שורה שההצדקה שלה היא מסוג  $T$ ) בהוכחה שלמה מתוך הסכמות האלה. זה היה מאפשר להוכיח את הכל בצורה סינטקטית נטו.

### 13.2.1.2 נושאים ותרגילים בתחשיב הפסוקים

נסקור את מה שראינו בתחשיב הפסוקים לפי נושאים ושבועות:

1. סינטקסט של נוסחאות – אילו מחרוזות נחשבות נוסחאות בתחשיב הפסוקים.
2. סמנטיקה – מה זה מודל, ואיך בכל מודל אנחנו קובעים אם נוסחא היא אמת או שקר.
3. אופרטורים – דנו בלמה דווקא אנחנו לוקחים את סט אופרטורים מסויים ולא אחד אחר, ואילו סטים של אופרטורים מספיקים כדי להציג כל דבר שנרצה.
4. מהי הוכחה – זה מושג סינטקטי לחלוטין, אוסף אותיות שמגיעות אחת אחרי השנייה שיש חוקים שאומרים מתי הוא חוקי ומתי הוא לא (לא מסתכלים על מודלים או על נכונות).

בשני התרגילים הבאים הלכנו לכיוון הוכחת משפט הטאוטולוגיה, שאומר שכל טאוטולוגיה ניתנת להוכחה. אחרי שהגדרנו את כל המושגים, הוכחנו את משפט הטאוטולוגיה, השלמות והקומפקטיות.

5. משפט הדדוקציה – בתרגיל הזה הוכחנו את משפט הדדוקציה, שחץ מזה שהוא שימושי בפני עצמו, הוא כלי מאוד חשוב למשפט הטאוטולוגיה.
6. משפט הטאוטולוגיה – השתמשנו במשפט הדדוקציה לשם ההוכחה שלו, בעיקר ב- $reduce\_assumption$ , שם היה ממש צריך את משפט הדדוקציה, ולא היה אפשר להוכיח אותו באמצעות איזו אקסיומה ספציפית.

### 13.2.2 סיכום: תחשיב היחסים

#### 13.2.2.1 נושאים ותרגילים בתחשיב היחסים

שאר התרגילים עסקו כבר בתחשיב היחסים:

7. סינטקסט וסמנטיקה – הסינטקס זה נוסחא ושם עצם, סמנטיקה זה הגדרת מודל.
  8. לא צריך פונקציות ושיויונות – זה בעצם היה יכול להגיע גם יותר מאוחר, כי השתמשנו בזה רק בתרגיל 12, אבל זה עזר לנו קצת לקבל תחושה של מה זה מודל.
  9. מהי הוכחה – כאן נכנסת הנקודה שהרשנו שורות טאוטולוגיה בהוכחה. אם לא היינו מרשים, אז כאן זו הנקודה שבה היה נכנס משפט הטאוטולוגיה בדרך להוכחת משפט השלמות לתחשיב היחסים.
  10. תרגיל שבא להגיד: בואו נראה שבאמת עם הסכמות שהגדרנו אפשר לעשות מתמטיקה כמו שאנחנו מכירים אותה (גם אם בצורה איטית וסזיפית יותר).
  - ראינו שהוכחות בסיסיות בשדה ובחבורה, הוכחת טענות לוגיות ופרדוקס מפורסם – ההוכחות שלנו מספיק עשירות כדי לעשות את זה. זה נותן אינטואיציה שהסכמות שלנו והמבנה שלנו מספיק קרוב למה שאנחנו מכירים בתור הוכחות במתמטיקה. בנוסף, כתבנו בתרגיל הזה גם פונקציות עזר ששמשו אותנו בהמשך.
  11. היו שני חלקים – משפט הדדוקציה ו- $PNF$ .
- משפט הדדוקציה, מעבר להיותו שימושי בפני עצמו, שימש אותנו במיוחד בשני מקרים מרכזיים: למה הוכחות

בשיליה פועלות ופונקציות ה-*eliminate* בתרגיל 12. שם היה צריך להראות שאם מתוך כל ההנחות הראשונות אפשר להוכיח סתירה אפשר להוכיח את זה גם מההוכחות המקוריות, ואפשר לעשות את זה עם משפט הדדוקציה. גם כאן היינו צריכים את משפט הדדוקציה ולא יכולנו להוכיח את זה משום סכמה בודדת, כי זה לא משנה מאיזה  $F$  הצלחנו להוכיח  $\varphi$ , אפשר להוכיח  $\varphi \rightarrow F$ . 12. כדי לסכם את החשיבות של מה שעשינו בתרגיל 11, נבין עד הסוף למה ההוכחה של משפט השלמות שעשינו עבור קבוצות סגורות ב-*PNF* מוכיחה את המשפט הכללי. כמו שאמרנו בתחילת השיעור, אם יש קבוצת משפטים סגורה ב-*PNF*, או שיש לה מודל או שאפשר להוכיח ממנה סתירה. נניח שיש אוסף משפטים  $F$  – אפשר לקחת את האוסף השקול ב-*PNF* שנסמן אותו ב- $S$ . ל- $S$  או שיש מודל או שאפשר להוכיח ממנו סתירה. אם יש לו מודל הוא גם מודל עבור  $F$ , כי הראנו שמ- $S$  אפשר להוכיח את  $F$  (השקילות בין  $S$  ל- $F$  היא גם הוכחתית). זה אומר שכל מה שאפשר להוכיח ב- $S$  גם מתקיים במודל הזה, לכן זה גם מודל עבור  $F$ . לעומת זאת, נגיד שהצלחנו להוכיח סתירה מ- $S$ , אנחנו גם רוצים להוכיח סתירה מ- $F$ . כל משפט  $s \in S$  אפשר להוכיח מתוך  $f \in F$  כלשהו (ראינו שאפשר לעשות את זה כי  $f \leftrightarrow s$ ). זה אומר שגם מ- $F$  אפשר להוכיח סתירה. כל זה היה קריטי כדי שמשפט השלמות יהיה נכון באופן כללי, לא רק ב-*PNF*. נקודה נוספת היא שאמרנו שבגלל שהראנו שלא צריך פונקציות ושיוויון, אז במקום התעסקנו רק עם יחסים. מה שלא ראינו בקורס, מקוצר זמן, זה איך לקחת הוכחה בלי פונקציות ושיוויון, ולתרגם אותה חזרה להוכחה עם פונקציות ושיוויון. בתרגיל 12 הוכחנו את משפט השלמות. זה חוזר למה שדיברנו עליו בשיעור הראשון: יש אינסוף שדות, ואנחנו רוצים להוכיח משהו באינסוף שדות בעולם. בשביל זה כותבים טקסט סופי על דף של הוכחה, וזה משכנע אותנו שזה נכון. אנחנו גם יודעים שכל מה שנכון במקרה יש לו הוכחה. זה מפתיע שע"י בדיקה של משהו סופי כמו הוכחה מאפשרת להשתכנע שמהו נכון לגבי אינסוף עולמות שונים.

### 13.3 מה לא עשינו בקורס – לקראת לוגיקה 2

נעבור לדבר כעת על מה לא עשינו בקורס, מה לא נפתר. נסתכל על גדל בתחילת המאה ה-20, שמה שעניין אותו זה מה שעניין הרבה אנשים מהאסכולה הגרמנית של המתמטיקה, שניסתה להבין את יסודות המתמטיקה. גדל התעניין בשאלה הבאה:

מה אפשר להוכיח מתוך סט אקסיומות?

הוא ניסה להבין את משמעות ההוכחה. התשובה שלו:

כל מה שנכון.

מה זה אומר נכון: כל מה שמתקיים בכל מודל שמקיים את האקסיומות.

לכאורה זה נראה טוב, אבל זה עדיין לא אומר שעבור כל פסוק שהוא אפשר להוכיח או אותו או את שלילתו. מתמטיקאים היו רוצים למצוא סט אקסיומות טוב במיוחד, כלומר כזה שכל פסוק מתמטי שאומרים בסט האקסיומות הזה או שהוא נכון תמיד או שהוא תמיד לא נכון. כלומר, סט אקסיומות שממנו אפשר להוכיח לכל פסוק או אותו או את שלילתו.

המטרה היא למצוא סט של אקסיומות שבו אין פסוקים מעורפלים כאלה שלפעמים נכונים, למצוא סט של אקסיומות שהכל תמיד מתקיים או לא מתקיים בו. לזה קוראים סט אקסיומות שלם (לא בלבד עם המובן של שלמות שדיברנו עליו בהקשר של משפט השלמות, שאומרת שאפשר להוכיח כל דבר שנכון. זה מובן אחר של המילה שלמות).

זה מוביל אותנו למשפט שלומדים בלוגיקה 2:

משפט אי-השלמות של גדל: אין קבוצת אקסיומות שלמה (לפחות אם היא מספיק חזקה, כלומר לפחות אריתמטיקת פיאנו)

אפשר לעשות דברים כ"כ טריוויאליים שלא יינבע מזה שום דבר, אבל בדברים שלפחות יודעים לטפל במספרים טבעיים (לפחות חזקים כמו אריתמטיקת פיאנו) שום דבר הוא לא מספיק טוב, אף פעם לא מגיעים לסט אקסיומות שלם.

נלך קצת אחורה, ונדבר על איך גדל התחיל להבין את הסוגייה של מה אפשר להוכיח עד שהוא הגיע למשפט השלמות – הוא עבד באופן פורמלי על מושג ההוכחה, בדיוק כמו שעשינו בקורס. הוא חשב על הוכחה בתור אוסף של שורות, והוא עשה מתמטיקה של הוכחות: אם יש הנחות, שורות ומסקנה אז אפשר לבנות מסקנה אחרת. בלוגיקה שלו, האלמנטים שהוא עבד איתם היו הוכחות (במקום וקטורים או מספרים וכו' בתחומים אחרים של מתמטיקה). זה בדיוק מה שאנחנו עשינו במהלך הקורס, אצלינו קיבלנו הוכחה והוצאנו הוכחה. זה מה שעשינו כל הזמן, וזה מה שגדל למד לעשות.

ברגע שהוא הבין את הקונספט הזה שהוכחה היא אובייקט שאפשר לעבוד עליו, הוא הרגיש לא בנח עם שני המובנים השונים של המילה "הוכחה". ראינו את המובנים האלה גם בקורס שלנו: יש הוכחה שאנחנו כותבים על הלוח, שהיא לכל דבר ועניין הוכחה של מתמטיקאים, ויש הוכחה בתוכנית, שהיא מחרוזת. גדל אמר שהוא את ההוכחה של הלוח רוצה לכתוב בשפת המחרוזות.

זו רוב העבודה שלו שנתקלים בה בלוגיקה 2: גדל הסתכל על אקסיומות פיאנו. אם להקביל את העבודה שלו לעבודה של מתכנת, רוב העבודה שלו לכתוב את פונקציית ה- $is\_valid$ . הוא כתב את  $is\_valid(x, y, z)$ , שאומרת האם  $x$  היא הוכחה ל- $y$  מתוך הנחות  $z$  ואקסיומות פיאנו. רוב קורס לוגיקה 2 זה עבודה של לקחת את הפונקציה  $is\_valid$  ולתרגם אותה לאסמבלר שפועל עם  $plus, times, s$  וכו'.

גדל ראה שאפשר לתרגם את ה- $is\_valid$  הזה לנוסחא אחת ארוכה, שהיא בעצם בדיוק התוכנית  $is\_valid$  רק מתורגמת לאקסיומות מסדר ראשון. מה הכוונה: אם אצלינו מופיע  $x$  בהוכחה, ה- $x$  הזה הוא מחרוזת. אמנם רשמנו הוכחה כאובייקט ולא כמחרוזת, אבל יכולנו לתרגם את זה מחרוזת אחת ארוכה (לדוגמא לשרשר את השורות ולשים ביניהן פסיק). לגדל עוד לא היו מחרוזות (אנחנו מדברים על התקופה שלפני טיורינג ולפני המצאת המחשב), אז הוא קידד מחרוזות ע"י מספר מתאים. כיוון שאפשר לכתוב את  $is\_valid$  כמחרוזת אחת ארוכה, זה אומר שאפשר להתאים להוכחה שלה מספר שלם.

ברגע שהוא עשה את זה, זה נתן לו מספיק כח ללכת לשלב הבא – לא רק מה הוכחות עושות במתמטיקה, אלא איך הן מדברות על עצמם. בפרט, אפשר להסתכל על:

$$consistent(z) = \sim \exists x [is\_valid(x, (plus(0,0) = 1 \& \sim plus(0,0) = 1), z)]$$

המחרוזת הזאת אומרת: מתי אוסף פסוקים הוא עקבי – אם לא קיים משהו שמוכיח סתירה ממנו.

אפשר היה לקחת בתור  $z$  את אריתמטיקת פיאנו, ולשאול את עצמינו האם אריתמטיקת פיאנו קונסיסטנטית, כלומר האם מתוך אקסיומות פיאנו אפשר להוכיח סתירה בתור אקסיומות פיאנו. מכל מה שלמדנו בקורס אנחנו כבר יודעים שזה לא נכון – לפיאנו יש מודל, הטבעיים, ואנחנו יודעים שאם יש מודל אז אי אפשר להוכיח סתירה.

אבל בא עכשיו גדל ואומר – נשים לב שהמשפט הזה "האם משהו קונסיסטנטי" זה משפט באריתמטיקת פיאנו. אז אמנם אנחנו יודעים שפיאנו קונסיסטנטי, אבל האם אנחנו גם יכולים להוכיח את העקביות הזאת מתוך אריתמטיקת פיאנו?

זה משפט אי השלמות השני של גדל – הוא אומר שאי אפשר להוכיח מתוך אקסיומות פיאנו את העקביות של אקסיומות פיאנו. לזה הוא הגיע ע"י זה שהוא הצליח להבין שאפשר לדבר על נוסחאות לא רק באופן פורמלי כמתמטיקאים, אלא בתוך הנוסחאות עצמן לדבר על נוסחאות. ברגע שיש לך מספיק עושר כדי לדבר על נוסחאות זה אומר שאתה יכול לדבר על עצמך, ואז אתה לא יכול להיות שלם.

$consistent(PA)$  זה בדיוק הדבר הזה שאי אפשר להוכיח אותו או את שלילתו מתוך  $PA$ . אנחנו יודעים שזה עקבי, אבל אנחנו גם יודעים שאי אפשר להוכיח את זה.