לוגיקה ותורת הקבוצות למדעי המחשב ־ הרצאות

גדי אלכסנדרוביץ'

תוכן עניינים

1 מבוא

בקורס זה יילמדו שני הנושאים שעומדים בבסיס המתמטיקה המודרנית ־ תורת הקבוצות ולוגיקה מתמטית. נפתח בתיאור לא פורמלי שלהן.

לוגיקה מתמטית היא הענף במתמטיקה שעוסק בהגדרות והוכחות מתמטיות. עד לתקופת יוון העתיקה, הידע המתמטי בא לידי ביטוי בשיטות היוריסטיות לפתרון בעיות קונקרטיות. האופן שבו הוסק ידע מתמטי היה באמצעות ניסוי וטעיה והערכה. היוונים הקדמונים שינו מן הקצה אל הקצה את הגישה למתמטיקה: לגישתם, אמיתות מתמטיות היה צריך **להוכיח**, כלומר להסיק באופן הגיוני מתוך הנחות בסיס פשוטות ומובנות מאליהן ("אקסיומות"). בנוסף, העיסוק במתמטיקה הפך למטרה בפני עצמה ולא רק ככלי עזר לביצוע מטלות מעשיות.

שיאה של המתמטיקה היוונית הוא ספרו של אוקלידס "יסודות", שבו הוא ריכז וערך את הידע המתמטי של תקופתו. הספר כולל הגדרות, אקסיומות והוכחות של משפטים בגאומטריה (ובתורת המספרים האלמנטרית). כך למשל מושגי יסוד המופיעים בו הם "נקודה", "קו", "זווית", "חפיפה", והאקסיומות המופיעות בו הן:

1. דרך כל שתי נקודות אפשר להעביר קטע ישר אחד ויחיד.
2. כל קטע אפשר להמשיך ללא גבול כקו ישר.
3. בהינתן קטע ישר, ניתן להעביר מעגל שמרכזו בנקודת קצהו האחת ורדיוסו שווה לקטע הנתון.
4. כל הזווית הישרות חופפות זו לזו.
5. בהינתן ישר ונקודה מחוץ לישר, ניתן להעביר דרכה מקביל אחד ויחיד לישר הנתון (במקור אקסיומה זו נוסחה בצורה שונה).

מחמש אקסיומות אלו אוקלידס גוזר את משפטי הענף שנקרא על שמו ־ **גאומטריה אוקלידית**, ונלמד גם כיום בבתי הספר. "שיטת העבודה" של אוקלידס ־ הגדרות, אקסיומות ומשפטים ־ היא עד היום שיטת העבודה המקובלת במתמטיקה ואותה נבחן בקורס זה.

האקסיומה החמישית של אוקלידס נראתה מאז ומעולם "לא אלגנטית" עבור המתמטיקאים שניסו להוכיח כי היא נובעת מארבע האקסיומות האחרות. במשך כאלפיים שנים לא הייתה כל התקדמות במאמצים אלו, אף שפורסמו אלפי "הוכחות",

כולל כאלו של גדולי המתמטיקאים, שנתגלו כשגויות (עקב הנחות סמויות קשות לאיתור). במאה ה־19 הוכיחו לובצ'בסקי ובולאי (כל אחד בנפרד) כי האקסיומה החמישית אינה ניתנת להוכחה מבין היתר, שכן **קיימת גאומטריה בה היא אינה נכונה**. כלומר, קיים "עולם" אשר מקיים את ארבע האקסיומות הראשונות של אוקלידס אך לא את החמישית (תחת זאת, דרך נקודה שמחוץ לישר ניתן להעביר לו לפחות **שני** מקבילים). "עולם" זה נקרא **גאומטריה היפרבולית**. במרוצת השנים נתגלו גאומטריות נוספות שבהן אקסיומות המקבילים ואקסיומות נוספות אינן נכונות (ראויה במיוחד לציון גישתו של ברנהרד רימן לגאומטריה, שהראתה קיום של אינסוף גאומטריות שונות מהותית זו מזו, והכלים המתמטיים שפותחו כדי לטפל בסיטואציות אלו שימשו בסופו של דבר בפיתוח תורת היחסות הכללית).

גילויים אלו גרמו להתערערות של תפיסות יסודיות בעולם המתמטי. "אקסיומות" איבדו את המעמד של "עובדות בסיסיות שאין עליהן עוררין" והגישה הרווחת אליהן כיום היא כאל "הנחות יסוד לצורך פיתוח מערכת מתמטית ספציפית". בנוסף, הגאומטריה איבדה את מעמדה בתור התחום שעליו מתבססת שאר המתמטיקה, שכן אם ישנה יותר מגאומטריה אחת, כיצד ניתן לדעת על איזו מהן לבסס את המתמטיקה? לקראת סוף המאה ה־19 מעמד "המושג שעליו מתבסס המתמטיקה" עבר אל מושג ה**קבוצה**. באמצעות קבוצות ניתן היה לבנות את שאר האובייקטים המתמטיים המקובלים ־ מספרים, פונקציות, מרחבים וכדומה, וקבוצות הפכו להיות (ונותרו) המושג הנפוץ ביותר במתמטיקה. בנוסף, המתמטיקאי גאורג קנטור גילה תכונות מפתיעות של קבוצות אינסופיות ־ בפרט, את קיומם של אינסוף גדלים שונים של אינסוף.

לרוע המזל, בתחילת המאה ה־20 בתורת הקבוצות התגלו גם **פרדוקסים** ־ קבוצות שמעצם הגדרתן נבעה סתירה. הדבר אילץ את המתמטיקאים לנסח מחדש באופן זהיר את תורת הקבוצות; ניסוח חדש ומדויק זה נעשה באמצעות כלים שפותחו במאה ה־19 ובפרט בעבודתו של גוטלוב פרגה (אף שפרגה עצמו לקח קשה את גילוי הפרדוקסים בתורת הקבוצות שהצביעו על בעיות באופן שבו הוא ניסח את המתמטיקה). באותה התקופה נוסחה מחדש גם הגאומטריה האוקלידית על ידי הילברט, באופן שהתאים לסטנדרטים החדשים של דיוק מתמטי; בהשראת עבודה זו, הילברט הציע גם מערכת אקסיומטית למספרים הממשיים, ולאחר מכן הציב לעצמו יעד שאפתני אף יותר ־ למצוא מערכת אקסיומות **לכל המתמטיקה** שתהיה חפה מפרדוקסים, מבוססת על אקסיומות פשוטות ביותר ("סופיות") ושהוכחות בה יוכלו להימצא ולהיבדק באופן אוטומטי־מכני לחלוטין (מחשבים עוד לא היו קיימים אז). אם מערכת אקסיומות כזו הייתה מתגלה, היה זה ההישג המתמטי הגדול ביותר אי פעם, והחיפוש אחר מערכת כזו הלהיב את העולם המתמטי בשנות ה־20 ונתן לענף הלוגיקה דחיפה משמעותית קדימה. לרוע המזל, בשנת 1931 הוכיח לוגיקאי צעיר בשם קורט גדל כי מערכת כזו אינה יכולה להתקיים; לכל מערכת אקסיומות חפה מפרדוקסים וניתנת לבדיקה מכנית שעדיין מנסה למדל את כל המתמטיקה (ובפרט את המספרים הטבעיים) יהיו קיימים משפטים מתמטיים שאינם ניתנים להוכחה או להפרכה ממערכת זו. דוגמה בולטת לבעיה זו היא **השערת הרצף** שעוסקת בקיום קבוצות אינסופיות מסויימות, והוכח (על ידי שילוב עבודות בלתי תלויות של קורט גדל ופול כהן) כי לא ניתן להוכיח או להפריך אותה מהאקסיומות הסטנדרטיות של תורת הקבוצות.

סקירה היסטורית זו מצביעה על הנקודות שעליהן יינתן דגש בקורס:

1. הגדרות **מדויקות** והוכחות **פורמליות**: חשיבותן של אלו כאשר עוסקים במושגים יסודיים היא ברורה, שכן כל הנחה סמויה יכולה להוביל לתוצאות שגויות. בדרך כלל במתמטיקה הקפדנות אינה כה גדולה כשם שתהיה בקורס זה משום שהדבר יהפוך טקסטים מתמטיים לארוכים וקשים מדי לקריאה, אך כאן אנו עוסקים בנושאים פשוטים דיים כדי שנוכל להקפיד.

2. תורת הקבוצות **הנאיבית**: בקורס זה נלמד את ההגדרות והמושגים הבסיסיים בתורת הקבוצות שכן הם שימושיים ביותר בכל תחומי המתמטיקה. כמו כן נלמד מקצת מתורת קנטור על גדלים שונים של אינסוף ("עוצמות"). נציג פרדוקסים שמתעוררים בתורת הקבוצות עקב הגדרה חופשית מדי של "קבוצה", אך לא נתעמק באופן שבו בעיה זו מטופלת על ידי מערכת אקסיומות מגבילה לתורת הקבוצות. עם זאת, כל מה שנלמד ניתן לניסוח גם במסגרת תורת הקבוצות האקסיומטית כך שאיננו מוכיחים דברים שגוים בשום שלב.

3. לוגיקה מתמטית ־ **תחביר** אל מול **משמעות**. מצד אחד, נעסוק באופן שבו משפטים ואקסיומות בלוגיקה הם רצפי תווים שנבנים ונגזרים בהתאם לכללי תחביר מסויימים; מצד שני, נבין כיצד נותנים משמעות לרצפי התווים הללו והקשר בין התחביר והמשמעות (ששיאו בהוכחת טענות מסוג "ניתן להוכיח פורמלית טענה מתוך אקסיומות אם ורק אם הטענה נובעת מתוך האקסיומות").

2 תורת הקבוצות הנאיבית ־ מושגי יסוד

2.1 הגדרות בסיסיות

המושג הבסיסי בתורת הקבוצות הוא, כצפוי, **קבוצה**. קבוצה מורכבת מאפס או יותר **איברים**, אשר בגישתנו הנאיבית יכולים להיות כל דבר שהוא.

- קבוצה מסומנת לרוב באופן מפורש באמצעות סוגריים מסולסלים ובתוכם פירוט של איברי הקבוצה:
  - $\{1,2,5,7\}$ היא הקבוצה שמכילה את המספרים הטבעיים 1,2,5,7.
  - $\{16,\pi,\mathrm{Dog},$מגדל אייפל$\}$ היא קבוצה שמכילה את המספר הטבעי 16, המספר האי רציונלי פאי, המילה Dog והביטוי "מגדל אייפל". בפרט, איברי הקבוצה אינם חייבים להיות כולם מאותו "סוג".
  - $\mathbb{N}=\{0,1,2,3,\dots\}$ היא הקבוצה שכוללת את כל המספרים הטבעיים. מכיוון שיש אינסוף כאלו לא כותבים את כולם במפורש אלא מסתפקים בכתיבת האיברים הראשונים ושלוש נקודות שמשמעותן המדוייקת היא "ומכאן והלאה ממשיכים על פי אותו כלל" (ההנחה היא שהקורא מסוגל להבין מהו הכלל; קיימת הגדרה מדוייקת יותר למספרים הטבעיים).
  - לעתים קרובות קבוצה מתוארת באופן הבא: $A=\{$איבר$|$תנאי על האיבר$\}$. דוגמאות יינתנו בהמשך.
- איבר יכול להיכלל בקבוצה בדיוק פעם אחת. אם הוא מופיע יותר מפעם אחת, הוא נספר בדיוק פעם אחת. כלומר, $\{1,1,1\}=\{1\}$.
- קבוצות מסומנות לרוב באותיות לטיניות גדולות מראשית הא"ב: A,B,C. עם זאת, משתמשים בסימונים רבים ושונים בהתאם למשמעות שאנו מייחסים לקבוצה.
- אם איבר x שייך לקבוצה A מסמנים זאת על ידי $x\in A$. אם x אינו שייך לקבוצה A מסמנים זאת $x\notin A$.
  - הנחת יסוד: לכל x ולכל קבוצה A, או שמתקיים $x\in A$ או שמתקיים $x\notin A$ ולא ייתכן ששניהם מתקיימים בו זמנית.
  - הנחת יסוד: בהינתן שתי קבוצות A,B, אם לכל $x\in A$ מתקיים $x\in B$ ובנוסף לכך לכל $y\in B$ מתקיים $y\in A$ אז $A=B$ (בתורת הקבוצות האקסיומטית זוהי **אקסיומת ההיקפיות**).
  - הנחת יסוד: קיימת קבוצה A כך שלכל x מתקיים $x\notin A$. הקבוצה A הזו נקראת **הקבוצה הריקה** ומסומנת ב־$\emptyset$ ולפעמים ב־$\{\}$ (בתורת הקבוצות האקסיומטית, **אקסיומת הקבוצה הריקה** דורשת במפורש את קיום הקבוצה הזו). כדאי לחשוב על קבוצות כעל "קופסאות", ואז הקבוצה הריקה היא פשוט קופסה ריקה.
- אם לכל $x\in A$ מתקיים $x\in B$ אז מסמנים זאת על ידי $A\subseteq B$ ואומרים ש־"A מוכלת ב־B", או ש"A היא תת־קבוצה של B". אם בנוסף לכך קיים $y\in B$ כך ש־$y\notin A$ אז מסמנים זאת על ידי $A\subset B$ (ולעתים $A\subsetneq B$ כדי למנוע בלבול; לרוע המזל, יש ספרים שמשתמשים ב־$A\subset B$ במשמעות של $A\subseteq B$) ואומרים ש־"A מוכלת **ממש** ב־B".

נציג כעת דוגמאות נוספות לקבוצות:

1. $\mathbb{N}^{+}=\{1,2,3,\dots\}$ - קבוצת המספרים הטבעיים ללא אפס (יש המגדירים מראש שאפס איננו מספר טבעי; כפי שנראה בהמשך, עבורנו יהיה נוח להגדיר את 0 כמספר טבעי).
2. $\mathbb{Z}=\{\dots,-2,-1,0,1,2,\dots\}$ - המספרים השלמים. שימו לב כי תיארנו אותה עם שלוש נקודות "בשני הכיוונים".
3. $\mathbb{Q}=\left\{\frac{a}{b}|a,b\in\mathbb{Z}\text{ and }b\neq0\right\}$ - המספרים הרציונליים. שימו לב לסגנון הכתיבה: בצד שמאל כתוב איבר $\frac{a}{b}$ ובצד ימין כתובים התנאים עליו - a,b שניהם שלמים, ו־$b\neq0$.
4. $\mathbb{R}$ - קבוצת המספרים הממשיים שלא תוגדר במפורש (ההגדרות הסטנדרטיות מתבססות על **חתכי דדקינד** או על **סדרות קושי** והבנתן דורשת היכרות כלשהי עם חשבון אינפיניטסימלי).
5. $[0,1]=\{x\in\mathbb{R}|0\le x\le1\}$ - הקטע הסגור שמכיל את כל המספרים הממשיים בין 0 ל־1 כולל.
6. $(0,1)=\{x\in\mathbb{R}|0<x<1\}$ - הקטע הפתוח שמכיל את כל המספרים הממשיים בין 0 ל־1 לא כולל.
7. $A=\{\emptyset\}$ היא קבוצה בעלת איבר בודד, ואיבר זה הוא הקבוצה הריקה. נשים לב לכך ש־$A\neq\emptyset$ כי ל־$\emptyset$ אין איברים ול־A יש.
8. $A=\{A\}$ היא קבוצה שמכילה איבר בודד - את עצמה. הגדרה זו נראית מוזרה מאוד אבל לבינתיים נתיר אותה.

2.2 הפרדוקס של ראסל

נציג כעת במפורש בעיה שעשויה להיווצר משימוש חופשי מדי בהגדרות שנתנו. נגדיר את הקבוצה הבאה:
$X = \{A | A \notin A$ קבוצה וגם $A\}$
במילים - X היא קבוצת כל הקבוצות שאינן איבר של עצמן.
הגדרה זו מובילה לפרדוקס הבא: X אינה יכולה להיות איבר של עצמה, אבל גם אינה יכולה שלא להיות איבר של עצמה, שכן:

- אם $X \in X$ אז על פי הקריטריון שמגדיר שייכות ל־X מתקיים $X \notin X$ - סתירה להנחת היסוד שלנו שאיבר לא יכול להיות שייך ולא־שייך בו זמנית לקבוצה.

- אם $X \notin X$ אז בפרט X אינה מקיימת את הקריטריון של שייכות ל־X, כלומר X **אינה** מקיימת את התכונה $X \notin X$ ולכן $X \in X$ ושוב הגענו לסתירה.

המסקנה מהפרדוקס של ראסל היא שלא כל קבוצה שניתן להגדיר באופן מילולי אכן קיימת. בפועל, ה"סכנה" ליפול על הגדרות לא הגיוניות היא זניחה ברוב תחומי המתמטיקה. בנוסף לכך, אם A היא קבוצה "חוקית", אז כל קבוצה שמוגדרת בתור $\{x \in A |$ מקיים תכונה מסויימת $x\}$ גם היא קבוצה חוקית (בתורת הקבוצות האקסיומטית תכונה זו נקראת **אקסיומת ההחלפה**). הקבוצות שבהן נעסוק בקורס יוגדרו באופן זה או באמצעות מספר בניות "תקינות" שיוצגו בהמשך, כך שהפרדוקס של ראסל (ופרדוקסים דומים לו) לא ישפיעו על המשך דרכנו.

2.3 כמה סימונים לוגיים

על מנת לפשט כתיבה של ביטויים והוכחות מתמטיות בהמשך, נציג מספר סימונים שבהם נהוג להשתמש בלוגיקה.

- במקום "וגם" נהוג להשתמש בסימן $\wedge$. כך למשל $\mathbb{Q} = \left\{\frac{a}{b} | a \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge b \neq 0\right\}$.

- במקום "או" נהוג להשתמש בסימן $\vee$. אם C, D הם שני תנאים, אז $C \vee D$ פירושו "או ש־C מתקיים, או ש־D מתקיים, או ששניהם מתקיימים".

- אם C היא טענה, אז השלילה של C מסומנת ב־$\neg C$ או $\sim C$. השלילה של C נכונה אם C אינה נכונה, ולהפך.

- אם C, D הן טענות אז הטענה $C \Rightarrow D$ (קרי: "C **גורר** את D") היא קיצור של $\neg C \vee D$. כלומר, היא טענה שנכונה באחד משני המקרים הבאים:

  - אם C נכונה וגם D נכונה.
  - אם C לא נכונה.

- אם C, D הן טענות אז הטענה $C \iff D$ (קרי: "C **שקול** ל־D") היא קיצור של $(C \Rightarrow D) \wedge (D \Rightarrow C)$. כלומר, היא טענה שנכונה באחד משני המקרים הבאים:

  - אם C נכונה וגם D נכונה.
  - אם C לא נכונה וגם D לא נכונה.

- ההגדרה של $C \Rightarrow D$ עשויה לגרום לקשיים עם האינטואיציה. כך למשל הטענה "אם מגדל אייפל נמצא בלונדון, אז $\pi = 3$" היא **נכונה** לחלוטין שכן הרישא של הטענה ("מגדל אייפל נמצא בלונדון") שגוי. גם טענה כמו "אם מגדל אייפל נמצא בפריז אז $\pi < 5$" היא נכונה לחלוטין למרות שהטענה נשמעת מוזרה. האינטואיציה מצפה שאם מתקיים ש־$C \Rightarrow D$ אז יהיה קשר לוגי ברור בין C ו־D, אולם בהגדרה שנתנו קשר שכזה כלל לא נדרש.

- משפטים מתמטיים רבים מנוסחים בסגנון "אם A אז B" שמשמעותו $A \Rightarrow B$. או בסגנון "A רק אם B" שמשמעותו $A \Rightarrow B$.

- משפטים אחרים מנוסחים בסגנון "A אם ורק אם B" שמשמעותו $A \iff B$ (מקוצר לפעמים בתור "אסם", ובאנגלית iff).

- הוכחה של טענה מהצורה "A גורר B" מתחילה לרוב מ**ההנחה** ש־A נכונה, ואז שרשרת טענות שנובעות זו מזו, ובסופו של דבר הגעה ל־B.

- הוכחה של טענה מהצורה "A אם ורק אם B" דורשת הוכחה של **שני** כיוונים שונים: צריך להוכיח את "אם A אז B" **וגם** את "אם B אז A". לפעמים הוכחת שני הכיוונים זהה או דומה מאוד ולכן ניתן לקצר, אבל באופן כללי הוכחה שאיננה דו כיוונית היא שגויה.

- לעתים במקום להוכיח את "A גורר B" נוח יותר להוכיח את "$\neg B$ גורר $\neg A$" אשר שקול לוגית ל-"A גורר B". לעתים מבלבלים זאת עם **הוכחה בשלילה**, שבה כדי להוכיח טענה מניחים את שלילתה ומגיעים לסתירה, אך הוכחה בשלילה היא שיטה כללית יותר (הסתירה אינה חייבת להיות $\neg A$ דווקא).

- במקום לכתוב "קיים" נהוג לכתוב $\exists$ ובמקום לכתוב "לכל" נהוג לכתוב $\forall$.

  כך למשל הגדרת הגבול $\lim_{x\to x_0} f\left(x\right)=L$ בחדו"א נכתבת כ-

$$\forall\varepsilon>0\left(\exists\delta>0\left(\left|x-x_0\right|<\delta\Rightarrow\left|f\left(x\right)-L\right|<\varepsilon\right)\right)$$

2.4 טענות בסיסיות על קבוצות

נתחיל בהוכחה של מספר "משפטים" מועילים שגם יעזרו לנו לקבל תחושה לגבי אופי ההוכחות בקורס:

טענה 2.1 יהיו A,B קבוצות. אז $A=B$ אם ורק אם $A\subseteq B\wedge B\subseteq A$ (**אנטי-סימטריות** יחס ההכלה).

הוכחה: כיוון אחד: נניח ש-$A=B$. יהי $x\in A$. מכיוון ש-$A=B$ בפרט יש להן אותם איברים, ולכן $x\in B$ ולכן $A\subseteq B$. באותו האופן מוכיחים $B\subseteq A$.

כיוון שני: נניח ש-$A\subseteq B\wedge B\subseteq A$. אם $x\in A$ אז מכיוון ש-$A\subseteq B$ מתקיים $x\in B$. אם $y\in B$ אז מכיוון ש-$B\subseteq A$ מתקיים $y\in A$. מהנחת היסוד שלנו ("אקסיומת ההיקפיות") נובע ש-$A=B$. ■

טענה 2.2 לכל קבוצה A מתקיים $\emptyset\subseteq A$.

הוכחה: אנו רוצים להוכיח שאם $x\in\emptyset$ אז $x\in A$. מכיוון שאין $x\in\emptyset$, הרישא של הטענה אינה נכונה ולכן הטענה כולה נכונה.

במקרה כזה, שבו אנו מוכיחים טענה בסגנון $C\Rightarrow D$ והטענה נכונה שכן C **תמיד** אינה נכונה, אומרים ש-$C\Rightarrow D$ מתקיים "באופן ריק".

ניתן להוכיח את הטענה גם בצורה שונה שפחות מפריעה לאינטואיציה: ברור כי אם $x\notin A$ אז $x\notin\emptyset$ שכן לכל x מתקיים ש-$x\notin\emptyset$, אולם ניסוח זה שקול לחלוטין לניסוח הקודם.

דרך נוספת לראות את ההוכחה: הטענה $\emptyset\subseteq A$ שגויה אם ורק אם קיים $x\in\emptyset$ כך ש-$x\notin A$, אולם מכיוון שלא קיים $x\in\emptyset$ לא ניתן להציג דוגמה נגדית שכזו. ■

משתי הטענות הללו ניתן להסיק:

מסקנה 2.3 קיימת קבוצה ריקה אחת ויחידה. כלומר, אם A,B שתיהן קבוצות ריקות אז $A=B$.

הוכחה: אם A ריקה אז היא תת־קבוצה של כל קבוצה אחרת ובפרט $A\subseteq B$. באותו אופן $B\subseteq A$ ולכן $A=B$. ■

זו דוגמה לשיטת פעולה מקובלת בטקסטים מתמטיים - אחרי הוכחת משפטים "כבדים" יחסית מביאים מסקנות מיידיות שנובעות מהם בקלות.

טענה 2.4 לכל קבוצה A מתקיים $A\subseteq A$ (**רפלקסיביות** יחס ההכלה).

הוכחה: טריוויאלי. ■

גם זו שיטת הוכחה מקובלת: כאשר הטענה כל כך קלה עד שהקורא יכול להשלים אותה בעצמו ללא כל קושי נוהגים להשמיט את ההוכחה (לעתים ההוכחה שיש להשלים היא לא מיידית כלל ודורשת עבודה מצד הקורא אך לא יותר מדי חשיבה יצירתית).

טענה 2.5 אם $A\subseteq B$ וגם $B\subseteq C$ אז $A\subseteq C$ (**טרנזיטיביות** יחס ההכלה).

אינטואיציה ניתן לקבל באמצעות **דיאגרמת ון** שבה כל קבוצה מצויירת כעיגול ומתקיימים בין העיגולים יחסי ההכלה המתאימים. כאן A היא עיגול שנמצא בתוך העיגול של B שנמצא בתוך העיגול של C ולכן גם אם יימחק העיגול של B עדיין העיגול של A יהיה בתוך העיגול של C. **זו אינה הוכחה.** **הוכחה:** יהי $x \in A$. מכיוון ש־$A \subseteq B$ אז $x \in A$ גורר $x \in B$. מכיוון ש־$B \subseteq C$ אז $x \in B$ גורר $x \in C$. ראינו כי אם $x \in A$ אז $x \in C$, כנדרש. ■

2.5 פעולות על קבוצות

בהינתן קבוצה (או מספר קבוצות), אנו רוצים לעתים קרובות ליצור מהם קבוצות חדשות באופן מסויים. נציג כאן את הבניות הנפוצות ביותר. כל הבניות שנציג מקיימות את התכונה שאם אנו מתחילים עם קבוצה "חוקית" אז גם התוצאה היא קבוצה "חוקית", ולכן בעיות דוגמת זו שהפרדוקס של ראסל הצביע עליהן לא יהיו רלוונטיות עבורנו.

בכל ההגדרות A, B הן קבוצות כלשהן. נשתמש בסימן $\triangleq$ כדי לומר "מוגדר כ־".

2.5.1 איחוד

הגדרה 2.6 איחוד: $A \cup B \triangleq \{x | x \in A \vee x \in B\}$ (האיחוד של שתי קבוצות כולל את כל האיברים שיש לפחות באחת מהן).

בתורת הקבוצות האקסיומטית משתמשים ב**אקסיומת האיחוד** כדי לבטא את ההנחה שאם A, B הן קבוצות אז הקבוצה $A \cup B$ קיימת.

נציג מספר תכונות בסיסיות של איחוד:

טענה 2.7 איחוד מקיים את התכונות הבאות:

1. $(A \cup B) \cup C = A \cup (B \cup C)$ (**אסוציאטיביות** האיחוד).
2. $A \cup B = B \cup A$ (**קומוטטיביות** האיחוד).
3. $A \subseteq B \iff A \cup B = B$
4. $A \cup \emptyset = A$ (הקבוצה הריקה היא **איבר אדיש** ביחס לאיחוד).

הוכחה: כדי לקבל אינטואיציה, נוח לצייר את דיאגרמת ון של כל המקרים
אסוציאטיביות:

$$\begin{aligned}
x \in (A \cup B) \cup C &\iff x \in A \cup B \vee x \in C \\
&\iff (x \in A \vee x \in B) \vee x \in C \\
&\iff x \in A \vee (x \in B \vee x \in C) \\
&\iff x \in A \vee (x \in B \cup C) \\
&\iff x \in A \cup (B \cup C)
\end{aligned}$$

בהוכחה זו אנו רואים כי אסוציאטיביות פעולת האיחוד נובעת בסופו של דבר מאסוציאטיביות האופרטור הלוגי $\vee$, שאותה לא הוכחנו (אך ניתן להוכיח באמצעות טבלת אמת ונראה זאת בהמשך הקורס).

קומוטטיביות מוכחת באופן דומה לאסוציאטיביות, תוך התבססות על קומוטטיביות $\vee$.

נעבור לתכונה 3. ראשית נניח כי $A \cup B = B$ ונוכיח כי $A \subseteq B$. יהי $a \in A$, אז בפרט $a \in A \cup B = B$, כלומר $a \in B$, כלומר $A \subseteq B$.

כעת נניח כי $A \subseteq B$ ונוכיח כי $A \cup B = B$:

בכיוון אחד, אם $x \in B$ אז בוודאי ש־$(x \in A \vee x \in B)$ ולכן $x \in A \cup B$ (זה נכון תמיד, ללא תלות בתכונה $A \subseteq B$).

בכיוון השני, אם $x \in A \cup B$ אז אחד משניים: או ש־$x \in B$, וזה מה שעלינו להראות, או ש־$x \in A$, ומכך ש־$A \subseteq B$ נובע ש־$x \in B$ ושוב קיבלנו את מה שרצינו להראות.

תכונה 4 נובעת כעת מתכונה 3 ומכך ש־$\emptyset \subseteq A$. ■

2.5.2 חיתוך

הגדרה 2.8 חיתוך: $A \cap B \triangleq \{x | x \in A \wedge x \in B\}$ (החיתוך של שתי קבוצות כולל את כל האיברים שנמצאים בשתיהן).

התכונות של חיתוך מזכירות את אלו של איחוד:

טענה 2.9 חיתוך מקיים את התכונות הבאות:

1. $(A \cap B) \cap C = A \cap (B \cap C)$ (**אסוציאטיביות** החיתוך).
2. $A \cap B = B \cap A$ (**קומוטטיביות** החיתוך).
3. $A \subseteq B \iff A \cap B = A$
4. $A \cap \emptyset = \emptyset$

הוכחה: הוכחת תכונות 1 ו־2 זהה לחלוטין להוכחה עבור איחוד, פרט לכך ש־$\wedge$ תופס את מקום $\vee$ (ואנו מתבססים על האסוציאטיביות והקומוטטיביות של $\wedge$).

עבור תכונה 3 נוכיח את כל אחד מהכיוונים בנפרד. בכיוון הראשון, אם $A \cap B = A$, אז אם $a \in A = A \cap B$ אז $a \in A \wedge a \in B$ ובפרט $a \in B$ ולכן $A \subseteq B$.

בכיוון השני, אם $A \subseteq B$ אז אם $a \in A$ נובע ש־$a \in B$ ולכן $(a \in A \wedge a \in B)$ ולכן $a \in A \cap B$ ולכן $A \subseteq A \cap B$. ההוכחה ש־$A \cap B \subseteq A$ טריוויאלית.

תכונה 4 נובעת כעת מתכונה 3 כי $\emptyset \subseteq A$ לכל A. ■

2.5.3 חיסור ומשלים

הגדרה 2.10 חיסור קבוצות: $A \backslash B \triangleq \{x | x \in A \wedge x \notin B\}$ (החיסור של B מ־A מסיר מ־A את האיברים ששייכים ל־$A \cap B$).

לעתים מסמנים חיסור גם כ־$A - B$ אך מכיוון שלסימון זה שימושים ומשמעויות נוספות נעדיף להשתמש בסימן $A \backslash B$.

לעתים קרובות משתמשים בקבוצות בתוך הקשר ספציפי שבו קיימת קבוצה X שמשמשת כ"עולם הייחוס" וכל שאר הקבוצות שמדברים עליהן הן תת־קבוצות של X. במקרים אלו קיים מושג של "משלים":

הגדרה 2.11 משלים: אם $A \subseteq X$ אז המשלים של A ביחס ל־X מוגדר כ־$\overline{A} \triangleq \{x \in X | x \notin A\} = X \backslash A$ (מסומן לפעמים גם כ־A^c).

שימו לב שמשלים הוא **תמיד** ביחס לקבוצה X שמכילה את A! הגדרה כמו $\{x \notin A\}$ ותו לא תוביל לפרדוקסים.

בטענות הבאות אנו מניחים קיום של קבוצה X שמכילה את A, B ומשלים נלקח ביחס אליה (תמיד ניתן להגדיר $X = A \cup B$ כך שאין בעיה בהנחה זו).

טענה 2.12 $A \backslash B = A \cap \overline{B}$

הוכחה: אם $x \in A \backslash B$ אז $x \in A \subseteq X$ ולכן $x \in X$ בפרט. כמו כן, $x \notin B$ ולכן בשילוב עם $x \in X$ נקבל ש־$x \in \overline{B}$, ומכאן ש־$A \backslash B \subseteq A \cap \overline{B}$.

בכיוון השני, אם $x \in A \cap \overline{B}$ אז בפרט גם $x \in A$ וגם $x \notin B$, ולכן $x \in A \backslash B$ ולכן $A \cap \overline{B} \subseteq A \backslash B$ כנדרש. ■

הטענה הבאה שימושית במיוחד:

טענה 2.13 (כללי דה־מורגן):

1. $\overline{A \cup B} = \overline{A} \cap \overline{B}$
2. $\overline{A \cap B} = \overline{A} \cup \overline{B}$

הוכחה: כמו אסוציאטיביות וקומוטטיביות של איחוד וחיתוך קבוצות, כך גם כללים אלו נובעים מכללים מקבילים עבור $\wedge$ ו־$\vee$. נוכיח את כלל 1 במפורש; ההוכחה של כלל 2 דומה.

אם $x \in \overline{A \cup B}$ אז $x \in X$ וגם $x \notin A \cup B$. מכאן ש־$x \notin A$ וגם $x \notin B$ (כי אם היה מתקיים $x \in A$ או $x \in B$ היה נובע מכך $x \in A \cup B$). מכך ש־$x \in X$ ו־$x \notin A$ נקבל $x \in \overline{A}$ ובדומה נקבל $x \in \overline{B}$ ולכן $x \in \overline{A} \cap \overline{B}$, ולכן $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

בכיוון השני אם $x \in \overline{A} \cap \overline{B}$ אז $x \notin A$ וגם $x \notin B$ וגם $x \in X$. משני הראשונים נובע ש־$x \notin A \cup B$ ולכן נקבל ש־$x \in \overline{A \cup B}$ ולכן $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$ כנדרש. ■

2.5.4 קבוצת החזקה

ראינו שבהינתן קבוצה A קיימות לה תת־קבוצות (בפרט $\emptyset$ היא תת־קבוצה של כל A). אם כן, יש הגיון בדיבור על **קבוצת** כל תת־הקבוצות של A:

הגדרה 2.14 קבוצת החזקה של A היא הקבוצה $\mathcal{P}\left(A\right)=\left\{ B|B\subseteq A\right\}$.

בתורת הקבוצות האקסיומטית, **אקסיומת קבוצת החזקה** מניחה שלכל קבוצה A, הקבוצה $\mathcal{P}\left(A\right)$ קיימת.

לעתים קרובות מסמנים את קבוצת החזקה גם בסימון 2^{A}. אף שסימון זה נראה מבלבל בתחילה יש מאחוריו הגיון שנראה בהמשך, ולאחר מכן אכן נשתמש בסימון זה.

דוגמאות:

- עבור הקבוצה הריקה $\emptyset$ מתקיים $\mathcal{P}\left(\emptyset\right)=\left\{ \emptyset\right\}$, כלומר $\mathcal{P}\left(\emptyset\right)$ היא קבוצה שכוללת איבר יחיד: $\emptyset$.
- בדומה, $\mathcal{P}\left(\mathcal{P}\left(\emptyset\right)\right)=\mathcal{P}\left(\left\{ \emptyset\right\} \right)=\left\{ \emptyset,\left\{ \emptyset\right\} \right\}$.
- $\mathcal{P}\left(\left\{ 1,2,3\right\} \right)=\left\{ \emptyset,\left\{ 1\right\} ,\left\{ 2\right\} ,\left\{ 3\right\} ,\left\{ 1,2\right\} ,\left\{ 1,3\right\} ,\left\{ 2,3\right\} ,\left\{ 1,2,3\right\} \right\}$.

2.5.5 זוגות סדורים ומכפלה קרטזית

עד כה עסקנו בקבוצות חסרות סדר: $\left\{ 2,1\right\} =\left\{ 1,2\right\}$. כמו כן, אותו איבר לא נספר פעמיים: $\left\{ 1\right\} =\left\{ 1,1\right\}$. עם זאת, במקרים רבים במתמטיקה כן חשוב לנו הסדר ואנו כן רוצים שאותו איבר יופיע מספר פעמים. כיצד ניתן לנסח זאת בפורמליזם שכולל קבוצות בלבד? התשובה היא שללא קושי רב.

הגדרה 2.15 זוג סדור $\left(a,b\right)$ הוא הקבוצה $\left(a,b\right)\triangleq\left\{ \left\{ a\right\} ,\left\{ a,b\right\} \right\}$.

בתורת הקבוצות האקסיומטית, **אקסיומת הזוג** מתארת את ההנחה שאם a,b איברים אז הקבוצה $\left\{ a,b\right\}$ קיימת (ובפרט אם $a=b$ אז הקבוצה $\left\{ a\right\}$ קיימת).

אין צורך אמיתי לזכור את האופן שבו הגדרנו את הזוג $\left(a,b\right)$; מספיק לשים לב לכך שההגדרה עובדת באופן שאנו מצפים ממנה לעבוד:

טענה 2.16 $\left(a,b\right)=\left(x,y\right)$ אם ורק אם $x=a$ וגם $b=y$.

הוכחה: כיוון אחד של ההוכחה טריוויאלי: אם $a=x$ וגם $b=y$ אז $\left(a,b\right)=\left\{ \left\{ a\right\} ,\left\{ a,b\right\} \right\} =\left\{ \left\{ x\right\} ,\left\{ x,y\right\} \right\} =\left(x,y\right)$. עיקר העבודה היא בכיוון השני.

נניח כי $\left(a,b\right)=\left(x,y\right)$, כלומר $\left\{ \left\{ a\right\} ,\left\{ a,b\right\} \right\} =\left\{ \left\{ x\right\} ,\left\{ x,y\right\} \right\}$. שתי קבוצות זהות אם יש להן בדיוק את אותם איברים, וכאן יש לנו שתי קבוצות עם שני איברים כל אחת ולכן קורה בדיוק אחד מבין שני מקרים אפשריים:

מקרה 1: במקרה זה, $\left\{ a\right\} =\left\{ x\right\}$ ו־$\left\{ a,b\right\} =\left\{ x,y\right\}$. מכיוון ש־$\left\{ a\right\} =\left\{ x\right\}$ אז בהכרח $a=x$. לכן את השוויון השני ניתן לכתוב כ־$\left\{ x,b\right\} =\left\{ x,y\right\}$. כעת, אם $b\ne y$ אז בהכרח $b\ne x$ או $y\ne x$ (או שניהם). נניח כי $b\ne x$, אז b הוא איבר שאינו שייך ל־$\left\{ x,y\right\}$ שכן הוא שונה משני איבריה ־ סתירה. לכן $b=y$.

מקרה 2: במקרה זה $\left\{ a\right\} =\left\{ x,y\right\}$ ו־$\left\{ a,b\right\} =\left\{ x\right\}$. מהשוויון הראשון עולה שבהכרח $a=x=y$ אחרת $\left\{ x,y\right\}$ היא קבוצה בת שני איברים ובפרט שונה מ־$\left\{ a\right\}$. לכן השוויון השני הוא למעשה $\left\{ a,b\right\} =\left\{ a\right\}$ ולכן מאותו שיקול $b=a=y$. קיבלנו $x=a$ ו־$b=y$ גם במקרה זה. ■

אם A,B הן קבוצות, שימושי מאוד לדבר על אוסף כל הזוגות הסדורים של איבר מ־A ואיבר מ־B:

הגדרה 2.17 המכפלה הקרטזית של A,B היא $A\times B\triangleq\left\{ \left(a,b\right)|a\in A\wedge b\in B\right\}$

הקיום של $A\times B$ נובע מ**אקסיומת ההחלפה** של תורת הקבוצות האקסיומטית, שאיננו מתארים כרגע במפורש.

ניתן להגדיר גם מכפלה בין מספר גדול משתיים של קבוצות, למשל $A\times\left(B\times C\right)$, אולם שימו לב שמכפלה זו איננה אסוציאטיבית כי איבר ב־$A\times\left(B\times C\right)$ הוא מהצורה $\left(a,\left(b,c\right)\right)$ בעוד שאיבר של $\left(A\times B\right)\times C$ הוא מהצורה $\left(\left(a,b\right),c\right)$. לכן ננקוט בסימון $\left(a_{1},a_{2},\dots,a_{n}\right)$ כדי לתאר את הזוג הסדור $\left(\left(a_{1},a_{2},\dots,a_{n-1}\right),a_{n}\right)$, ונגדיר $A_{1}\times\dots\times A_{n}\triangleq\left\{ \left(a_{1},\dots,a_{n}\right)|\forall i\left(a_{i}\in A_{i}\right)\right\}$.

בהמשך נראה כיצד ניתן להרחיב את מושג המכפלה הקרטזית כך שיוגדר לכל אוסף של קבוצות (לאו דווקא סופי) באמצעות **פונקציות** (שבתורן מוגדרות בעזרת מכפלות קרטזיות, כך שההגדרה הנוכחית לא הייתה לשווא).

טענה 2.18 התכונות הבאות של מכפלה קרטזית מתקיימות:

1. $A \times \emptyset = \emptyset \times A = \emptyset$ (הקבוצה הריקה מתנהגת כמו אפס ביחס לפעולת הכפל).
2. אם $A \times B = \emptyset$ אז $A = \emptyset$ או $B = \emptyset$ (אין **מחלקי אפס**).
3. אם $A \subseteq B$ אז לכל C, $A \times C \subseteq B \times C$ (**מונוטוניות**).
4. $(A \odot B) \times C = A \times C \odot B \times C$ עבור $\odot \in \{\cup, \cap, \setminus\}$ (**דיסטריביוטיביות**).

הוכחה: טענה 1 נובעת מההגדרה: מכיוון ש־$b \notin \emptyset$ לכל b, הרי שהתנאי $a \in A \wedge b \in B$ אינו יכול להתקיים אף פעם ולכן $A \times \emptyset$ ריקה, ובדומה גם $\emptyset \times A$.

טענה 2 נובעת מכך שאם $A \neq \emptyset$ אז קיים $a \in A$. בדומה, אם $B \neq \emptyset$ אז קיים $b \in B$, ולכן $(a, b) \in A \times B$ ולכן $A \times B \neq \emptyset$. הראינו ש־$\neg (A = \emptyset \vee B = \emptyset) \Leftarrow \neg (A \times B = \emptyset)$, וזה שקול לוגית למה שרצינו להראות.

עבור טענה 3, ניקח $(a, c) \in A \times C$, אז בפרט $a \in A, c \in C$ ומכיוון ש־$A \subseteq B$ נקבל $a \in B$ ולכן $(a, c) \in B \times C$ כנדרש.

נוכיח את טענה 4 עבור $\odot = \cup$; שאר ההוכחות דומות. במקרה זה:

$$\begin{aligned}
(x, y) \in (A \cup B) \times C &\iff (x \in A \cup B) \wedge (y \in C) \\
&\iff (x \in A \vee x \in B) \wedge (y \in C) \\
&\iff (x \in A \wedge y \in C) \vee (x \in B \wedge y \in C) \\
&\iff (x, y) \in A \times C \vee (x, y) \in B \times C \\
&\iff (x, y) \in A \times C \cup B \times C
\end{aligned}$$

כאן הסתמכנו על דיסטריביוטיביות $\vee$ מעל $\wedge$, שאותה ניתן להוכיח באמצעות טבלת אמת. ■

2.6 איחודים וחיתוכים כלליים

הגדרנו איחוד וחיתוך עבור זוג קבוצות. ניתן להשתמש בהגדרה זו כדי לקבל איחוד וחיתוך של מספר סופי של קבוצות, אולם אין קושי להכליל את ההגדרה אף יותר מכך.

נסמן ב־$\mathcal{F}$ קבוצה של קבוצות (לעתים קבוצה כזו נקראת **משפחה** כדי להדגיש שמדובר על אוסף של קבוצות ולא של איברים שרירותיים).

הגדרה 2.19 (איחוד וחיתוך כלליים):
לכל $\mathcal{F} \neq \emptyset$ נגדיר:

- $\bigcup \mathcal{F} \triangleq \bigcup_{A \in \mathcal{F}} A \triangleq \{a | \exists A \in F \, (a \in A)\}$
- $\bigcap \mathcal{F} \triangleq \bigcap_{A \in \mathcal{F}} A \triangleq \{a | \forall A \in F \, (a \in A)\}$

למרות הסימטריה בין שתי ההגדרות, יש בינן מספר הבדלים מהותיים: קיום הקבוצה $\bigcup \mathcal{F}$ אינו מובן מאליו; בתורת הקבוצות האקסיומטית נדרשת **אקסיומת האיחוד** כדי להניח שהיא אכן קיימת. לעומת זאת, אם $X \in \mathcal{F}$ אז $\bigcap \mathcal{F} \subseteq X$ ולכן ניתן להגדיר את $\bigcap \mathcal{F}$ כתת־קבוצה של X המקיימת תנאי כלשהו ואיך צורך באקסיומה מיוחדת עבורה.

עם זאת, אם היינו מרשים שיתקיים $\mathcal{F} = \emptyset$ אז $\bigcap \mathcal{F}$ היה סימון חסר משמעות; מכיוון שאם $\mathcal{F} = \emptyset$ אז התנאי $\forall A \in F \, (a \in A)$ מתקיים באופן ריק בלי תלות ב־a אז $\bigcap \mathcal{F}$ הייתה על פי הגדרה זו פשוט קבוצת "כל האיברים" (הקבוצה האוניברסלית) וראינו כבר בפרדוקס של ראסל כי קבוצה זו אינה יכולה להתקיים.

לעתים קרובות במקום הסימון $A \in \mathcal{F}$ משתמשים בסימונים אחרים. נציג כאן דוגמה.

הגדרה 2.20 תהא $A_1, A_2, A_3, \ldots$ סדרה של קבוצות.

- **הגבול העליון** של הסדרה מוגדר בתור $\limsup A_n \triangleq \bigcap_{k=0}^{\infty} \bigcup_{n=k}^{\infty} A_n$.
- **הגבול התחתון** של הסדרה מוגדר בתור $\liminf A_n \triangleq \bigcup_{k=0}^{\infty} \bigcap_{n=k}^{\infty} A_n$.

אינטואיטיבית, גבול עליון הוא "קבוצת כל האיברים ששייכים לאינסוף קבוצות בסדרה" וגבול תחתון הוא "קבוצת כל האיברים ששייכים לכל אברי הסדרה החל ממקום מסוים". דוגמה זו ממחישה את סגנון הכתיבה $\bigcup_{n=0}^{\infty}$ כאשר קיים מספור של אברי $\mathcal{F}$.

2.7 בניית המספרים הטבעיים

קבוצת המספרים הטבעיים $\mathbb{N} = \{0, 1, 2, \ldots\}$ היא אחת הקבוצות השימושיות ביותר עבורנו. בשל כך, נציג כעת דרך פורמלית לבנות את איבריה, שגם תסייע לנו בהבנת סימונים והגדרות בהמשך.

נניח כי לא ידוע לנו כלל על קיומם של מספרים, ועלינו לבנות את $\mathbb{N}$ רק מתוך "אבני הבניין" שפיתחנו עד כה במסגרת תורת הקבוצות. הקבוצה הפשוטה ביותר שראינו (והנחנו את קיומה) היא הקבוצה הריקה $\emptyset$. נגדיר אם כך $0 \triangleq \emptyset$.

את 1 נוכל להגדיר כעת בתור $\{\emptyset\}$, כלומר קבוצה שמכילה את הקבוצה הריקה. את 2 ניתן להגדיר בתור $\{\{\emptyset\}\}$, וכן הלאה; אך גישה זו מועילה פחות מהגישה שנציג.

נניח שהגדרנו עד כה את כל המספרים עד n בתור קבוצות (בהתחלה $n = 0$). אז נגדיר את $n+1$ להיות $n+1 \triangleq n \cup \{n\}$. כלומר, $n+1$ הוא הקבוצה שמכילה את כל אברי n ובנוסף לכך את n עצמו כאיבר חדש.

באופן זה נקבל:

- $0 = \emptyset$
- $1 = \emptyset \cup \{0\} = \{0\} = \{\emptyset\}$
- $2 = \{0\} \cup \{1\} = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$
- $3 = \{0, 1\} \cup \{2\} = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

ובאופן כללי נקבל $n = \{0, 1, 2, \ldots, n-1\}$. בשיטה זו, הקבוצה שמייצגת את n מכילה בדיוק n איברים, שהם בדיוק n המספרים הטבעיים שקודמים ל־n.

לבניה זו קיימת הכללה מרחיקת לכת שנציג בהמשך כאשר נדבר על סודרים.

3 יחסים

3.1 מבוא והגדרות כלליות

נתחיל מלהתבונן במספר דוגמאות ולהבין את המשותף לכולן:

1. $1 = 1$
2. $e < \pi$
3. $A \subseteq B$
4. בגרף G קיים מסלול בין הצמתים u ו־v
5. 3 מחלק את 15
6. $\cos(0) = 1$

בכל הדוגמאות הללו יש לנו שני איברים שנלקחים מאותו תחום (שני מספרים, שתי קבוצות, שני צמתים בגרף) ובכל דוגמה מתקיים קשר מסויים ביניהם. במתמטיקה משתמשים במילה **יחס** (Relation) כדי לתאר קשר שכזה. בדוגמה 1 היחס הוא "שווה"; בדוגמה 2 הוא "קטן מ־"; בדוגמה 3 הוא "מוכל"; בדוגמה 4 הוא "קיים מסלול בין"; בדוגמה 5 הוא "מחלק" ובדוגמה 6 הוא "ה־$\cos$ של... שווה ל...".

אף שמבחינה אינטואטיבית הרעיון ברור, לא לחלוטין ברור איך לפרמל אותו. למשל, את היחס $A \subseteq B$ מבטאים באמצעות הנוסחה "$x \in A \Leftarrow x \in B$" ואילו את היחס "$x$ מחלק את y" מבטאים באמצעות הנוסחה "$\exists z : xz = y$" שנראית שונה למדי, וכן הלאה. למרות שיש עניין בשאלה איך ניתן **לתאר** את היחס, אפשר לחמוק ממנה כעת באמצעות הגדרה רחבה:

הגדרה 3.1 **יחס** n־מקומי R על הקבוצות $A_1, \ldots, A_n$ הוא תת־קבוצה $R \subseteq A_1 \times \cdots \times A_n$.

בפרט, יחס דו־מקומי (בינארי) R על הקבוצות A, B הוא תת־קבוצה $R \subseteq A \times B$ ויחס חד־מקומי (אונרי) R על הקבוצה A הוא פשוט תת־קבוצה $R \subseteq A$.

כלומר, יחס R על A, B הוא פשוט זוגות (a, b) של איבר מ־A ואיבר מ־B. אוסף הזוגות הזה הוא שמתאר את היחס: אם $(a, b) \in R$ אז אומרים ש־a, b נמצאים ביחס R ולעתים קרובות מסמנים זאת aRb. אם $(a, b) \notin R$ אז אומרים ש־a, b אינם נמצאים ביחס R.

דוגמאות

1. $R \subseteq \mathbb{N} \times \mathbb{N}$ המוגדר על ידי $R = \{(a, a) \mid a \in \mathbb{N}\}$ ־ זהו יחס השוויון על המספרים הטבעיים. במקום לכתוב aRa נהוג לכתוב $a = a$.
2. $R \subseteq \mathbb{N} \times \mathbb{N}$ המוגדר על ידי $R = \left\{(1, 2), (4, 1), \left(10^{100}, 10^{101}\right)\right\}$ הוא יחס שכולל בדיוק שלושה זוגות, ואין שום חוקיות ברורה שעומדת מאחוריו. דוגמה זו באה להמחיש את העובדה שניתן לדבר על יחס גם בלי לתת "כלל" שמגדיר אותו.
3. $R \subseteq A \times B$ המוגדר על ידי $R = \emptyset$ הוא יחס חוקי לכל דבר, אם כי טריוויאלי; ביחס זה, aRb אינו נכון לאף a, b.
4. $R = A \times B$ גם הוא יחס חוקי לכל דבר, אם כי טריוויאלי: ביחס זה aRb נכון **לכל** a, b.
5. $R \subseteq \mathbb{R} \times \mathbb{R}$ המוגדר על ידי $R = \{(x, y) \mid \exists r > 0 : (x + r = y)\}$. זהו היחס $<$ ב"תחפושת" ־ מכאן אנו רואים שניתן להגדיר את אותו היחס במספר דרכים שונות.

יחסים דו־מקומיים ניתן להרכיב, באופן הבא:

הגדרה 3.2 אם $R \subseteq A \times B$ ו־$S \subseteq B \times C$ הם יחסים, אז נגדיר יחס $R \circ S \subseteq A \times C$ באופן הבא:

$$R \circ S \quad = \quad \{(a, c) \mid \exists b \in B : (a, b) \in R \wedge (b, c) \in S\}$$

טענה 3.3 הרכבת יחסים היא פעולה אסוציאטיבית. כלומר, אם $R_1 \subseteq A_1 \times A_2$, $R_2 \subseteq A_2 \times A_3$ ו־$R_3 \subseteq A_3 \times A_4$ אז $R_1 \circ (R_2 \circ R_3) = (R_1 \circ R_2) \circ R_3$.

הוכחה: נניח כי $(a_1, a_4) \in R_1 \circ (R_2 \circ R_3)$, אז קיים $a_2 \in A_2$ כך ש־$a_1 R_1 a_2$ וגם $a_2 (R_2 \circ R_3) a_4$. כלומר, קיים $a_3 \in A_3$ כך ש־$a_2 R_2 a_3$ וגם $a_3 R_3 a_4$.

כעת, מכך ש־$a_1 R_1 a_2$ וגם $a_2 R_2 a_3$ נסיק כי $a_1 (R_1 \circ R_2) a_3$; ומכך ש־$a_3 R_3 a_4$ נסיק ש־$(a_1, a_4) \in (R_1 \circ R_2) \circ R_3$. על כן $R_1 \circ (R_2 \circ R_3) \subseteq (R_1 \circ R_2) \circ R_3$. ההוכחה לכיוון השני דומה. ■

במקרה שבו היחס הוא בין קבוצה לעצמה, ניתן להרכיב יחס עם עצמו:

הגדרה 3.4 בהינתן יחס $R \subseteq A \times A$, נגדיר: $R^0 = \{(a, a) \mid a \in A\}$ ולכל $n > 0$ טבעי, $R^n = R \circ R^{n-1}$.

בנוסף נגדיר $R^+ \triangleq \bigcup_{n=1}^{\infty} R^n$. ל־$R^+$ קוראים **הסגור הטרנזיטיבי** של R. כמו כן נגדיר $R^* \triangleq \bigcup_{n=0}^{\infty} R^n$ ־ **הסגור הרפלקסיבי־טרנזיטיבי** של R.

3.2 יחסי שקילות

3.2.1 הגדרה ודוגמאות

במקרים רבים במתמטיקה ישנם שני אובייקטים שאינם זהים זה לזה, אך בתכונות המהותיות שלהן שרלוונטיות עבורנו כן קיימת זהות. במקרים אלו היינו רוצים להחשיב את האיברים כ"שקולים זה לזה". הדרך הפורמלית לעשות כן היא באמצעות יחסי שקילות. לצורך הגדרת יחסי שקילות נזהה את התכונות המהותיות של יחס השוויון, שהוא האב טיפוס שלנו בבואנו להגדיר יחסי שקילות.

1. כל איבר a מקיים תמיד $a=a$. זהו אולי הרעיון הבסיסי בשוויון - כל איבר שווה לעצמו.
2. אם יש לנו משוואה $a=b$, אז בוודאי שגם המשוואה $b=a$ נכונה - המושג של שוויון אינו מושפע מהסדר (בניגוד חריף ליחסים כמו $a<b$).
3. אם $a=b$ וגם $b=c$ אז נובע מכך ש־$a=c$.

שלוש התכונות הללו הן הבסיס להגדרה הכללית של יחס שקילות:

הגדרה 3.5 יחס דו־מקומי $R\subseteq A\times A$ הוא **יחס שקילות** על הקבוצה A אם הוא מקיים:

1. לכל $a\in A$ מתקיים aRa (**רפלקסיביות**).
2. $aRb \iff bRa$ (**סימטריה**).
3. אם aRb וגם bRc אז aRc (**טרנזיטיביות**).

דוגמאות

1. כצפוי, יחס השוויון הוא יחס שקילות. זהו יחס השקילות הקטן ביותר האפשרי, במובן זה שכל יחס שקילות אחר על אותה קבוצה מכיל אותו.
2. גם היחס $R=A\times A$ שבו כל זוג איברים הם שקולים הוא יחס שקילות. זהו יחס השקילות הגדול ביותר האפשרי על A.
3. אם A היא קבוצת המשולשים בגאומטריה אוקלידית, אז $R=\{(\Delta_1,\Delta_2)\,|\,\Delta_2$ בעל אותן זוויות כמו $\Delta_1\}$ הוא יחס השקילות של **דמיון משולשים**.
4. אם $G=(V,E)$ הוא גרף לא מכוון, אז $R\subseteq V\times V$ שמוגדר על ידי $\{(u,v)\mid$ קיים מסלול מ־u אל v ב־$G\}=V$ הוא יחס שקילות.
5. אם A היא קבוצת כל האנשים בעולם, אפשר להגדיר יחסי שקילות רבים ושונים: אנשים הם שקולים אם יש להם אותו צבע שיער, או אותו מין, או שהם חיים באותה מדינה, וכן הלאה.
6. עבור הקבוצה $M_n(\mathbb{R})$ של מטריצות מסדר $n\times n$ מעל $\mathbb{R}$, היחס $R=\left\{(A,B)\,|\,\exists P\in M_n(\mathbb{R}):P^{-1}AP=B\right\}$ הוא יחס שקילות של **דמיון מטריצות**.

נראה בהמשך דוגמאות מהותיות אף יותר, אך קודם נבין יותר לעומק את המבנה שיחס שקילות R משרה על הקבוצה A.

3.2.2 קבוצת המנה

הגדרה 3.6 תהא A קבוצה ו־$R\subseteq A\times A$ יחס שקילות על A. לכל $a\in A$ נגדיר את **מחלקת השקילות** של a ביחס ל־R:
$$[a]_R\triangleq\{b\in A|aRb\}$$

מחלקת השקילות של a היא פשוט אוסף האיברים ששקולים ל־a ביחס השקילות R. לרוב נשמיט את ה־R מהסימון $[a]_R$ כשיהיה ברור על איזה יחס שקילות מדובר.

לכל זוג איברים a,b הקשר בין $[a],[b]$ הוא פשוט במיוחד:

טענה 3.7 תהא A קבוצה ו־R יחס שקילות עליה ו־$a,b\in A$ כלשהם. אז:

- אם aRb אז $[a]=[b]$.
- אם לא aRb אז $[a]\cap[b]=\emptyset$

הוכחה: ראשית נניח כי aRb ונוכיח כי $[a]=[b]$. ראשית נוכיח כי aRb גורר $[b]\supseteq[a]$. יהי $c\in[b]$, אז על פי הגדרה bRc. כמו כן, aRb על פי הנחתנו ומטרנזיטיביות R נקבל aRc, כלומר $c\in[a]$, ולכן $[b]\supseteq[a]$, כנדרש. בכיוון השני, מכיוון ש־R סימטרי ו־aRb הרי ש־bRa ולכן ניתן לחזור על ההוכחה שראינו ולקבל $[b]\subseteq[a]$. מכאן ש־$[b]=[a]$, כנדרש.

עבור המקרה השני, נוכיח כי אם $[a]\cap[b]\neq\emptyset$ אז aRb. יהי $c\in[a]\cap[b]$, כלומר $c\in[a]\wedge c\in[b]$, כלומר $aRc\wedge bRc$. מסימטריית R נקבל cRb, ומטרנזיטיביות R נקבל כעת aRb. ∎

מכאן אנו למדים שניתן לתאר מחלקת שקילות בתור $[a]$ **לכל** איבר a של מחלקת השקילות הזו. כאשר אנו משתמשים ב־a לצורך זה, אז a נקרא **נציג** של מחלקת השקילות.

הגדרה 3.8 תהא X קבוצה. משפחה $\mathcal{F}$ של קבוצות היא **חלוקה** של X אם מתקיים:

1. $\bigcup_{A\in\mathcal{F}}A=X$
2. לכל $A\in\mathcal{F}$ מתקיים $A\neq\emptyset$
3. לכל זוג $A,B\in\mathcal{F}$ כך ש־$A\neq B$ מתקיים $A\cap B=\emptyset$

במילים, חלוקה של X היא משפחת קבוצות לא ריקות, זרות בזוגות, שאיחודן הוא בדיוק X. בחלוקה כל איבר של X שייך **בדיוק לאחת** מבין הקבוצות בחלוקה, ואין קבוצות "מיותרות" (ריקות).

כעת אנו מגיעים להגדרה המרכזית, שבזכותה יחסי שקילות הם כל כך חשובים:

הגדרה 3.9 תהא A קבוצה ו־R יחס שקילות על A. אז נגדיר את **קבוצת המנה** של A ביחס ל־R באופן הבא:

$$A/R \quad\triangleq\quad \{[a]\,|a\in A\}$$

.

כלומר, קבוצת המנה של A היא קבוצת **מחלקות השקילות** של אברי A ביחס ל־R.

טענה 3.10 אם A קבוצה ו־R יחס שקילות על A, אז A/R היא חלוקה של A.

הוכחה: מכיוון ש־R רפלקסיבי אז לכל $a\in A$ מתקיים aRa ולכן $a\in[a]$. מכאן ש־$a\in\bigcup_{b\in A}[b]$ שכן בפרט $[a]$ משתתף באיחוד (תכונה 1). כמו כן, זה מראה כי כל אברי A/R הם לא ריקים שכן אם $[a]$ הוא איבר כלשהו של A/R, הוא מכיל את a (תכונה 2). עבור תכונה 3 יהיו $[a],[b]$ שתי מחלקות שקילות ב־A/R (לא בהכרח שונות). אם aRb אז $[a]=[b]$, ואם לא aRb אז $[a]\cap[b]=\emptyset$, כנדרש. ∎

נחזור אל מקצת הדוגמאות שראינו ונבין כיצד קבוצת המנה באה לידי ביטוי במקרים אלו:

1. עבור יחס השוויון, $[a]=\{a\}$, ולכן נקבל $A/R=\{\{a\}\,|a\in A\}$ לכל A. זוהי החלוקה ה"עדינה ביותר" האפשרית של A.
2. עבור היחס $R=A\times A$ קיימת בדיוק מחלקת שקילות אחת, כלומר $A/R=A$. זוהי החלוקה ה"גסה ביותר" האפשרית של A.
3. עבור יחס השקילות שהגדרנו על גרף $G=(V,E)$ בו זוג צמתים היו שקולים אם היה מסלול ביניהם, הרי ש־V/R היא קבוצת **רכיבי הקשירות** של G.
4. עבור מטריצות ויחס הדמיון, מחלקות השקילות שנקבל הן **מחלקות הצמידות** של המטריצות; כשהמטריצות הן מעל שדה סגור אלגברית ניתן לתאר כל מחלקה על ידי נציג **קנוני** שהוא מטריצה **בצורת ז'ורדן**.

נשים כעת לב לכך ש**כל** חלוקה משרה יחס שקילות:

טענה 3.11 תהא $\mathcal{F}$ חלוקה של A. נגדיר יחס $R\subseteq A\times A$ באופן הבא: $R=\{(a,b)\,|\exists B\in\mathcal{F}:(a\in B\wedge b\in B)\}$. אז R הוא יחס שקילות.

הוכחה: רפלקסיביות: יהיה $a \in A$ כלשהו. אז מכיוון ש-$\mathcal{F}$ היא חלוקה של A, קיימת $B \in \mathcal{F}$ כך ש-$a \in B$ ולכן aRa.

סימטריה: יהיו $a, b \in A$ כך ש-aRb, כלומר קיים $B \in \mathcal{F}$ כך ש-$a \in B \wedge b \in B$, אז כמובן ש-$b \in B \wedge a \in B$ ולכן bRA (נובע מכך ש-$\wedge$ קומוטטיבי).

טרנזיטיביות: יהיו $a, b, c \in A$ כך ש-aRb ו-bRc. אז קיימות קבוצות $B_1, B_2 \in \mathcal{F}$ כך ש-$a \in B_1, c \in B_2$ וכמו כן $b \in B_1 \wedge b \in B_2$, כלומר $b \in B_1 \cap B_2$ ובפרט $B_1 \cap B_2 \neq \emptyset$. מכיוון ש-$\mathcal{F}$ היא חלוקה, נובע מכך ש-$B_1 = B_2$ ולכן $a, c \in B_1$ ומכאן ש-aRc. ■

3.2.3 דוגמאות נוספות

בניית המספרים השלמים והרציונליים: נגדיר על $\mathbb{N} \times \mathbb{N}$ את יחס השקילות הבא: $R = \{((a,b),(x,y)) \mid a + y = b + x\}$, ונסמן $\mathbb{Z} \triangleq \mathbb{N} \times \mathbb{N} / R$.

האינטואיציה שלנו היא לחשוב על הזוג (a, b) בתור המספר השלם $a - b$, ולכן שני זוגות (a, b) ו-(x, y) מייצגים את אותו מספר אם $a - b = x - y$, כלומר $a + y = b + x$.

את מחלקות השקילות אפשר לתאר באופן הבא בעזרת נציגים קנוניים:

$\mathbb{Z} = \bigcup_{a \in \mathbb{N}} [(a,0)] \cup \bigcup_{a \in \mathbb{N}} [(0,a)]$

הרכיב השמאלי מתאר לנו את הטבעיים, והרכיב הימני את השליליים (יחד עם אפס). כדי לראות שאכן כל (a, b) שקול לנציג מאחת מהקבוצות, נפריד לשני מקרים:

- אם $a \geq b$ אז $(a,b) R (a - b, 0)$
- אם $a < b$ אז $(a,b) R (0, b - a)$

בניית הרציונליים מתבצעת באופן דומה באמצעות זוגות של שלמים. האינטואיציה כעת היא שזוג (a, b) עם $b \neq 0$ ייצג את $\frac{a}{b}$, ולכן אם $\frac{a}{b} = \frac{x}{y}$ מתקיים $ay = bx$.

פורמלית, נגדיר על $\mathbb{Z} \times (\mathbb{Z} \backslash \{0\})$ את יחס השקילות $R = \{((a,b),(x,y)) \mid ay = bx\}$, ונסמן $\mathbb{Q} \triangleq \mathbb{Z} \times (\mathbb{Z} \backslash \{0\}) / R$.

כדי לתאר את $\mathbb{Q}$ באמצעות נציגים קנוניים, יש להשתמש במושג מתורת המספרים האלמנטרית: $a, b \in \mathbb{Z}$ הם **זרים** אם לא קיים להם מחלק משותף הגדול מ-1. נסמן זאת $\gcd(a,b) = 1$.

כעת: $\mathbb{Q} = \bigcup \{[(a,b)] \mid \gcd(a,b) = 1 \wedge a, b \neq 0\} \cup [(0,1)]$.

הבניה לא שלמה שכן לא הגדרנו את פעולות החשבון על $\mathbb{Q}$, אך זה כבר עניין לקורס בתורת החוגים.

בניית $\mathbb{Z}_n$: נשים לב כי החלוקה למספרים זוגיים ואי-זוגיים של $\mathbb{Z}$ משרה, כפי שראינו עבור כל חלוקה, יחס שקילות. האם קיים לו תיאור פשוט? היחס המתבקש הוא $R = \{(a,b) \mid a \bmod 2 = b \bmod 2\}$ כאשר mod היא הפעולה של חלוקה ולקיחת השארית, אך קיים תיאור פשוט יותר: $R = \{(a,b) \mid 2 | a - b\}$, כאשר $x|y$ פירושו "x מחלק את y", כלומר קיים $z \in \mathbb{Z}$ כך ש-$xz = y$.

ניתן לבצע בניה זו גם באופן כללי: בהינתן $n \in \mathbb{N}$ כלשהו, נגדיר יחס שקילות $\equiv_n$ על $\mathbb{Z}$ באופן הבא: $a \equiv_n b$ אם ורק אם $n | a - b$. נוכיח כי זה אכן יחס שקילות:

1. רפלקסיביות: לכל $a \in \mathbb{Z}$ מתקיים $a - a = 0 = 0 \cdot n$ ולכן $n | a - a$ ולכן $a \equiv_n a$.
2. סימטריה: אם עבור $a, b \in \mathbb{Z}$ מתקיים $a \equiv_n b$, פירוש הדבר ש-$a - b = z \cdot n$, ולכן $b - a = (-z) \cdot n$ ולכן $b \equiv_n a$.
3. טרנזיטיביות: אם עבור $a, b, c \in \mathbb{Z}$ מתקיים $a \equiv_n b$ וגם $b \equiv_n c$ אז קיימים z_1, z_2 כך ש-$a - b = z_1 n$ ו-$b - c = z_2 n$. מכאן ש-

$$\begin{aligned} a - c &= (a - b) + (b - c) \\ &= z_1 n + z_2 n = (z_1 + z_2) n \end{aligned}$$

ולכן $a \equiv_n c$

נסמן $\mathbb{Z}_n = \mathbb{Z} / R$. נשים לב לכך ש-$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$. כדי לראות זאת, יהי $a \in \mathbb{Z}$ כלשהו ו-$r = a \bmod n$, כלומר קיים $q \in \mathbb{Z}$ כך ש-$a = q \cdot n + r$, כלומר $a - r = q \cdot n$, כלומר $a \equiv_n r$. מכיוון ש-r הוא השארית בחלוקה ב-n, הוא תמיד בתחום $\{0, 1, \ldots, n-1\}$.

הבניה לא שלמה שכן לא הגדרנו את פעולות החשבון על $\mathbb{Z}_n$, אך גם זה כבר עניין לקורס בתורת החוגים.

בניות טופולוגיות: בטופולוגיה נהוג לבנות **מרחבי מנה** על ידי "הדבקה" של חלקים מהמרחב יחד. באופן פורמלי הדבר מתבצע על ידי הגדרת יחס שקילות שמזהה את הנקודות שהודבקו יחד.

נציג כאן דוגמה פשוטה בלבד: נתבונן בקטע $A=[0,1]$ ו"נדביק" את שני קצותיו יחד על ידי הגדרת יחס שקילות $R=\{(a,a)\,|a\in[0,1]\}\cup\{(0,1)\}$. על קבוצת המנה שמתקבלת A/R ניתן לחשוב כעל מעגל.

ניתן לקבל מעגל גם כתוצאה של בניה מחוכמת יותר. נגדיר יחס שקילות על כל $\mathbb{R}$: $R\subseteq\mathbb{R}\times\mathbb{R}$ כך ש־$R=\{(a,b)\,|a-b\in\mathbb{Z}\}$. לא קשה לראות כי a,b שקולים אם ורק אם החלק השברי שלהם (כל מה שמימין לנקודה העשרונית) שווה. גם במקרה זה ניתן לחשוב על $\mathbb{R}/R$ (שמסומן לעתים $\mathbb{R}/\mathbb{Z}$) כמעגל; באופן ציורי, ניתן לחשוב על הבניה כאילו היא לוקחת את הישר האינסופי $\mathbb{R}$ ומלפפת אותו במעגל היחידה אינסוף פעמים (עוד דרך לחשוב על הבניה: $\mathbb{R}$ יוצר "ספירלה" בצורת בורג שלאחר מכן משוטחת)

3.3 פונקציות

3.3.1 הגדרה ודוגמאות

אינטואיטיבית, ניתן לחשוב על פונקציה כמעין "מכונה" או "כלל" שמתרגמים **קלט** ל**פלט**, כלומר מבצעים תהליך שממיר ערך x לערך אחר y. הדרך הטבעית לתאר פונקציה היא על ידי תיאור הכלל או התהליך הזה, אבל כמו במקרה הכללי של יחסים, גם כאן אנחנו מעדיפים גישה כללית יותר שמתמקדת בתכונות הבסיסיות שצריכות להתקיים ולא בדרך ההגדרה של הפונקציה.

הגדרה 3.12 פונקציה $f:A\to B$ היא יחס דו־מקומי $f\subseteq A\times B$ המקיים:

- (קיום) לכל $x\in A$ קיים $y\in B$ כך ש־$(x,y)\in f$.
- (יחידות) לכל $x\in A$ ו־$y_1,y_2\in B$, אם $(x,y_1)\in f$ וגם $(x,y_2)\in f$ אז $y_1=y_2$.

במילים: **לכל** $x\in A$ קיים $y\in B$ **יחיד** כך ש־$(x,y)\in f$.

הקבוצה A נקראת **התחום** של הפונקציה והקבוצה B נקראת **הטווח** של הפונקציה.

אם f היא פונקציה נהוג להשתמש בסימון $f(x)=y$ במקום $(x,y)\in f$.

התחום והטווח של פונקציה הם חלק אינטגרלי מהגדרתה; שתי פונקציות שמכילות בדיוק אותם זוגות אך התחום או הטווח שלהן מוגדרים באופן שונה הן פונקציות שונות (ליתר דיוק, התחום שלהן חייב להיות זהה או שבלתי אפשרי שהן יכילו את אותם זוגות; אך הטווחים יכולים להיות שונים).

נציג מספר דוגמאות לפונקציות פשוטות:

- $f:\mathbb{R}\to\mathbb{R}$ המוגדרת על ידי $f(x)=x$ - פונקציית הזהות על $\mathbb{R}$.
- $f:\mathbb{R}\to\mathbb{R}$ המוגדרת על ידי $f(x)=x^2$ - העלאה בריבוע. נשים לב לכך שגם $g:\mathbb{R}\to[0,\infty)$ המוגדרת על ידי $g(x)=x^2$ היא פונקציית "העלאה בריבוע של מספר ממשי" אך היא איננה זהה ל־f מכיוון שהטווח שלהן שונה, וזאת למרות ש־f אינה "משתמשת" בטווח הנוסף שיש לה כי איננה מחזירה מספר שלילי (בכל מובן אחר f ו־g זהות).
- $f:[0,\infty)\to[0,\infty)$ המוגדרת על ידי $f(x)=\sqrt{x}$ - הפונקציה המחזירה לכל מספר שלם אי שלילי את השורש החיובי שלו. במקרה זה תחום הפונקציה אינו יכול לכלול מספרים שליליים שכן השורש שלהם איננו מספר ממשי.
- $f:A\to 2^A$ המוגדרת על ידי $f(a)=\{a\}$ - הפונקציה שמעבירה כל איבר ב־A לקבוצה שמכילה רק אותו.
- $f:2^A\times 2^A\to 2^A$ המוגדרת על ידי $f((B,C))=B\cup C$ - פונקציה זו מקבלת זוג סדור של שתי תת־קבוצות של A ומחזירה את איחודן.
- $f:\mathbb{R}^3\to\mathbb{R}^4$ המוגדרת על ידי $f((x,y,z))=\left(x^2+z^2,13,y^3,x-y+17\right)$ - פונקציה זו ממחישה כי ניתן לתאר פונקציות מרובות משתנים (ועם פלט מרובה משתנים) גם בעזרת הניסוח ה"מצומצם" שלנו שהסתפק בקבוצה אחת לתחום וקבוצה אחת לטווח. לרוב במקום $f((x,y,z))$ כותבים לצורך פשטות $f(x,y,z)$.

כעת ניתן מספר דוגמאות לנסיונות להגדיר פונקציה באמצעות כלל, שבגלל בעיה בהגדרה אינן מובילות לפונקציה. יש שני דברים עיקריים שיכולים להשתבש: או שהכלל המוצע לא יהיה בעל משמעות עבור כל אברי A, או שיהיו איברים ב־A עבורם הכלל מחזיר יותר מפלט אפשרי אחד. עבור "פונקציות" שהוגדרו באמצעות כלל בעייתי שכזה אומרים שהן אינן **מוגדרות היטב**.

1. הפונקציה $f:\mathbb{R}\to\mathbb{R}$ המוגדרת באמצעות הכלל $f(x)=\frac{1}{x}$ אינה מוגדרת ב־$x=0$ שכן אין משמעות לחלוקה באפס.

2. הפונקציה $f:(0,\infty)\to\mathbb{R}$ המוגדרת באמצעות הכלל $f(x)=\pm\sqrt{x}$ מחזירה יותר מערך אחד לכל x בתחום (גם $\sqrt{x}$ וגם $-\sqrt{x}$)

3. הפונקציה $f:\mathbb{Z}_n\to\mathbb{Z}$ המוגדרת באמצעות הכלל $f([a])=a$ מחזירה יותר מערך אחד לכל מחלקת שקילות, כתלות בנציג שאנו בוחרים למחלקת השקילות. למשל, $f([0])=0$ ו־$f([n])=n$ על פי הגדרה זו, אך $[0]=[n]$.

את בעיות 1 ו־2 ניתן לתקן על ידי שינויים לא מהותיים בהגדרות. את המקרה שבו פונקציה $f:A\to B$ אינה מוגדרת על ערכים מסויימים של A ניתן לתקן בשתי דרכים שונות: או להקטין את התחום של f לתת־קבוצה של A שעליה f מוגדרת, או להרחיב את הטווח B על ידי הוספת סימן מיוחד שמשמעותו תהיה "לא מוגדר" - למשל, $\perp$ - ולהגדיר $f(x)=\perp$ לכל ערך $x\in A$ שעליו f לא הוגדרה. מכיוון שלרוב אין צורך בדקויות אלו, במרבית המקרים שבהם נתונה פונקציה אשר אינה מוגדרת על כל התחום שלה לרוב מסתפקים בציון הערכים עבורם היא אינה מוגדרת. פונקציות כאלו נקראות פונקציות **לא מלאות**.

בעיה מספר 2 ניתנת לפתרון על ידי שינוי הטווח - במקום $f:A\to B$ ניתן להגדיר $\hat{f}:A\to 2^B$, כך שאם $f(x)=y$ אז $\hat{f}(x)=\{y\}$, ואם ל־f יש יותר מפלט אחד על x, אז $\hat{f}(x)$ תחזיר את קבוצת הפלטים הזו. ניתן גם לטפל באופן זה בפונקציות שאינן מוגדרות על קלטים מסויימים באמצעות ההגדרה $f(x)=\emptyset$. כך למשל הפונקציה בבעיה מס' 2 ניתנת לתיאור כ־$\hat{f}(x)=\{\sqrt{x},-\sqrt{x}\}$. לרוב בפועל לא משתמשים פורמלית בהגדרה זו ומסתפקים בדיבור לא פורמלי על פונקציה שיכולה להחזיר מספר פלטים. פונקציות כאלו נקראות **פונקציות רב־ערכיות**.

3.3.2 פונקציות חד־חד ערכיות, פונקציות על ופונקציות הפיכות

נפתח בהצגה נוספת של שתי התכונות שעל יחס לקיים כדי שייחשב לפונקציה:

- (קיום) לכל $x\in A$ קיים $y\in B$ כך ש־$(x,y)\in f$.
- (יחידות) לכל $x\in A$ ו־$y_1,y_2\in B$, אם $(x,y_1)\in f$ וגם $(x,y_2)\in f$ אז $y_1=y_2$.

נציג כעת שתי תכונות שפונקציה יכולה לקיים שהן דואליות לשתי התכונות שלעיל, בהחלפת תפקידי A ו־B:

הגדרה 3.13 תהא $f:A\to B$ פונקציה.

- f היא **על** אם לכל $y\in B$ קיים $x\in A$ כך ש־$(x,y)\in f$, כלומר $f(x)=y$.
- f היא חד־חד־ערכית (חח"ע) אם לכל $y\in B$ ו־$x_1,x_2\in A$, אם $(x_1,y)\in f$ וגם $(x_2,y)\in f$ אז $x_1=x_2$, כלומר $f(x_1)=f(x_2)$ גורר ש־$x_1=x_2$.

כדי להבין את חשיבותה של ההגדרה, נשים לב שעבור הפונקציה f, שהיא בפרט יחס, ניתן להגדיר את **היחס ההפוך** $f^{-1}\triangleq\{(y,x)\,|\,(x,y)\in f\}$.

טענה 3.14 f^{-1} היא פונקציה אם ורק אם f היא חח"ע ועל.

הוכחה: טריוואלי; תכונת ה"קיום" של f^{-1} היא בדיוק תכונת ה"על" של f, ותכונת ה"יחידות" של f^{-1} היא בדיוק תכונת ה"חח"ע" של f. ■

הגדרה 3.15 אם f היא חח"ע ועל אז נאמר ש־f היא **הפיכה** (באופן שקול, f היא הפיכה אם f^{-1} היא פונקציה).

מכיוון שפונקציות הן מקרה פרטי של יחסים, ההגדרה של **הרכבה** תקפה גם לגביהן:

הגדרה 3.16 ההרכבה $f\circ g$ תסומן לרוב כ־gf והסימון $gf(x)$ ייצג את האיבר $g(f(x))$.

שימו לב להבדלי הסימון בהם נקטנו: הסימון $f\circ g$ מתאר את הרכבת **היחסים** f,g, אך מכיוון שאנו רגילים לחשוב על פונקציות כאילו הן פועלות מימין לשמאל, העדפנו את הסימון gf (ללא $\circ$) כדי לתאר את הפונקציה שבה קודם כל f פועלת ואחר כך g פועלת.

בהגדרה שלעיל מסתתרת ההנחה ש־$f\circ g$ היא אכן פונקציה:

טענה 3.17 אם $f:A\to B$ ו־$g:B\to C$ הן פונקציות, אז **ההרכבה** שלהן $f\circ g$ היא פונקציה מ־A אל C.

הוכחה: קיום: אם $a \in A$ הוא איבר כלשהו, אז $c = g\left(f\left(a\right)\right)$ מקיים $gf\left(a\right) = c$.
יחידות: אם $g\left(f\left(a\right)\right) = c_1$ וגם $g\left(f\left(a\right)\right) = c_2$, אז מכיוון ש־$f$ היא פונקציה, $f\left(a\right)$ הוא אותו איבר בשני השוויונות, ומכיוון ש־g היא פונקציה אז $c_1 = c_2$. ■

הגדרה 3.18 **פונקצית הזהות** על קבוצה A היא פונקציה $\mathrm{Id}_A : A \to A$ המקיימת $\mathrm{Id}_A\left(x\right) = x$ לכל $x \in A$.

טענה 3.19 תהא $f : A \to B$ פונקציה.

- אם f חד־חד ערכית, אז קיימת $g : B \to A$ כך ש־$gf = \mathrm{Id}_A$.
- אם f על אז קיימת $g : B \to A$ כך ש־$fg = \mathrm{Id}_B$.
- אם f הפיכה אז $f^{-1}f = \mathrm{Id}_A$ ו־$ff^{-1} = \mathrm{Id}_B$.

הוכחה: נניח כי f חח"ע. יהי $a \in A$ כלשהו (אם $A = \emptyset$ אז f טריוויאלית ממילא). נגדיר

$$g\left(y\right) = \begin{cases} x & \exists x \in A : f\left(x\right) = y \\ a & \neg\exists x \in A : f\left(x\right) = y \end{cases}$$

במילים, אם קיים x ש־f מעבירה ל־y, אז x זה יהיה פלט g; אחרת, הפלט יהיה a שרירותי. נשים לב לכך ש־g מוגדרת היטב שכן חד־חד ערכיות f מבטיחה שאם קיים x שמועבר ל־y, הוא יחיד.
נניח כי f על. יהי $y \in B$ כלשהו. קיים x (אחד לפחות) כך ש־$f\left(x\right) = y$. נגדיר $g\left(y\right) = x$. כעת מתקיים $fg\left(y\right) = f\left(g\left(y\right)\right) = f\left(x\right) = y$, כנדרש.
השוויונות $f^{-1}f = \mathrm{Id}_A$ ו־$ff^{-1} = \mathrm{Id}_B$ נובעים ישירות מההגדרה של f^{-1}. ■

מסקנה 3.20 יהיו A, B קבוצות. קיימת פונקציה $f : A \to B$ שהיא חח"ע אם ורק אם קיימת פונקציה $g : B \to A$ שהיא על.

הוכחה: אם $f : A \to B$ חח"ע קיימת $g : B \to A$ כך ש־$gf = \mathrm{Id}_A$, כלומר לכל $a \in A$ מתקיים $g\left(\left(f\left(a\right)\right)\right) = a$ ומכאן ש־g על.
אם $g : B \to A$ על אז קיימת $f : A \to B$ כך ש־$gf = \mathrm{Id}_A$, כלומר אם $f\left(a_1\right) = f\left(a_2\right)$ אז $a_1 = g\left(f\left(a_1\right)\right) = g\left(f\left(a_2\right)\right) = a_2$ ומכאן ש־f חח"ע. ■

דוגמאות:

- הפונקציה $f : \mathbb{R} \to \mathbb{R}$ המוגדרת על ידי $f\left(x\right) = x^2$ איננה חח"ע (כי $f\left(1\right) = f\left(-1\right) = 1$) ואיננה על (כי ל־$-1$ אין מקור). העובדה שהיא איננה חח"ע באה לידי ביטוי בגרף הפונקציה בכך שקיים קו מאוזן החותך את הפונקציה בשני מקומות; העובדה שהיא איננה על באה לידי ביטוי בכך שקיים קו מאוזן שאינו חותך אותה כלל.
- הפונקציה $f : \mathbb{R} \to \mathbb{R}$ המוגדרת על ידי $f\left(x\right) = x^3$ היא כן חח"ע ועל, ולכן הפיכה; ההופכית שלה מסומנת כ־$f^{-1}\left(x\right) = \sqrt[3]{x}$.
- הפונקציה $f : \mathbb{N} \to \mathbb{N}$ המוגדרת על ידי $f\left(x\right) = x + 1$ היא חח"ע אך איננה על, כי אין מקור ל־0.
- הפונקציה $f : \mathbb{N} \to \mathbb{N}$ המוגדרת על ידי $f\left(x\right) = \left\lfloor \frac{x}{2} \right\rfloor$ היא על (המקור של y הוא $2y$) אך איננה חח"ע כי למשל $f\left(0\right) = f\left(1\right) = 0$ ($\lfloor a \rfloor$ הוא **הערך השלם התחתון** של a; המספר השלם הגדול ביותר שקטן או שווה ל־a).

לעתים קרובות אנחנו עוסקים ביותר משתי קבוצות שבינן יש פונקציות שהן חח"ע, על והפיכות; לכן המשפט הבא מועיל:

טענה 3.21 יהיו A, B, C קבוצות ו־$f : A \to B$ ו־$g : B \to C$ פונקציות. נגדיר $h : A \to C$ על ידי $h = gf$.

1. אם f, g הן חח"ע, כך גם h.

2. אם f,g הן על, כך גם h.

3. אם f,g הן הפיכות, כך גם h.

הוכחה: נניח כי $h(x_1)=h(x_2)$, כלומר $g(f(x_1))=g(f(x_2))$. מחח"ע g נובע ש־$f(x_1)=f(x_2)$ ומחח"ע f נובע ש־$x_1=x_2$.

נניח כי $c\in C$ הוא איבר כלשהו. מכיוון ש־g על קיים $b\in B$ כך ש־$g(b)=c$. מכיוון ש־f על קיים $a\in A$ כך ש־$f(a)=b$. על כן $h(a)=g(f(a))=g(b)=c$ ולכן h על.

הטענה על f,g הפיכות נובעת משתי קודמותיה. ■

קיום פונקציה חח"ע ועל $f:A\to B$ מעידה על כך ששתי הקבוצות A,B הן במובן מסויים "אותו הדבר". אפשר לחשוב על f כפונקציה ש"משנה את השם" של אברי A, ובאופן זה מתקבלים בדיוק אברי B, כך שניתן לחשוב על A,B כעל "אותה קבוצה עם שמות אחרים לאיברים". זוהי תכונה כה חשובה עד כי ניתן לה שם:

הגדרה 3.22 אומרים שקבוצות A,B הן **שקולות** ומסמנים $A\sim B$ אם קיימת פונקציה $f:A\to B$ שהיא חח"ע ועל.

טענה 3.23 שקילות של קבוצות היא יחס שקילות.

הוכחה: לכל קבוצה A, $A\sim A$ עם הפונקציה $f:A\to A$, $f(a)=a$ שהיא בבירור חח"ע ועל.

אם $A\cong B$ אז קיימת פונקציה חח"ע ועל $f:A\to B$, ולכן קיימת הפונקציה $f^{-1}:B\to A$. f^{-1} היא חח"ע שכן אם $f^{-1}(b_1)=f^{-1}(b_2)$ אז $b_1=ff^{-1}(b_1)=ff^{-1}(b_2)=b_2$; ו־$f^{-1}$ היא על שכן אם $a\in A$ הוא איבר כלשהו, אז $f^{-1}f(a)=a$, ולכן $f(a)$ הוא מקור של a. לכן $B\sim A$.

אם $A\sim B$ ו־$B\sim C$ אז קיימות פונקציות חח"ע ועל $f:A\to B$ ו־$g:B\to C$. נגדיר פונקציה $h:A\to C$ על ידי $h=gf$. כפי שראינו קודם, מכיוון ש־g,f הפיכות כך גם h. ■

3.3.3 קבוצות של פונקציות ומכפלות קרטזיות, גרסה כללית

לקבוצת **כל** הפונקציות $f:A\to B$ חשיבות רבה עד כדי כך שהיא זוכה לסימון מיוחד:

הגדרה 3.24 $B^A\triangleq\{f:A\to B\}$.

קיומה של B^A מובטח מכיוון ש־$B^A\subseteq\mathcal{P}(\mathcal{P}(A\times B))$, שכן כל פונקציה $f:A\to B$ היא יחס (תת־קבוצה של $A\times B$, כלומר איבר של $\mathcal{P}(A\times B)$).

סימון זה מבהיר את המשמעות של הסימון $2^A\triangleq\mathcal{P}(A)$: ניתן לחשוב על כל תת־קבוצה של A בתור פונקציה $f:A\to\{0,1\}$ כך ש־$f(a)=1$ אם ורק אם a שייך לתת־הקבוצה המוגדרת באמצעות f (וכפי שראינו, ניתן לחשוב על 2 כעל הקבוצה $\{0,1\}$). מעתה ואילך נשתמש בסימון 2^A לתיאור קבוצת החזקה.

ראינו בפרק 2.5.5 את האופן שבו הוגדרה מכפלה קרטזית של שתי קבוצות, $A\times B$. באמצעות הגדרה זו הגדרנו פונקציות. כעת הפונקציות יוכלו להחזיר את החוב ונגדיר באמצעותן מכפלות קרטזיות כלליות.

תהא Λ קבוצה כלשהי, שנחשוב על איבריה בתור **אינדקסים** (למשל, קבוצת המספרים הטבעיים, אך Λ יכולה להיות כל קבוצה שהיא). נניח כי קיימת התאמה חח"ע ועל בין Λ לאוסף קבוצות $\{A_l\}_{l\in\Lambda}$ (הקבוצה שמותאמת ל־$l\in\Lambda$ מסומנת ב־A_l).

הגדרה 3.25 **המכפלה הקרטזית** $\prod_{l\in\Lambda}A_l$ מוגדרת בתור $\prod_{l\in\Lambda}A_l\triangleq\left\{f:\Lambda\to\bigcup_{l\in\Lambda}A_l|\forall l\in\Lambda:f(l)\in A_l\right\}$

כל איבר במכפלה הקרטזית הוא פונקציה f, שערכה על $l\in\Lambda$ הוא האיבר שנמצא בקואורדינטה ה־l־ית ש־f מתארת. נמחיש זאת במספר דוגמאות:

- עבור $\Lambda=\{1,2\}$ וקבוצות A_1,A_2 נקבל קבוצה איזומורפית למכפלה הקרטזית הרגילה: $\prod_{i\in\{1,2\}}A_i$ כך שכל איבר בה הוא פונקציה f כך ש־$f(1)\in A_1$ ו־$f(2)\in A_2$. בפרט, אם A,B הן קבוצות כלשהן אז $A\times B$ ניתן לתיאור במונחי המכפלה הקרטזית $\prod_{i\in\{1,2\}}A_i$ כך ש־$A_1=A,A_2=B$ והאיבר $(a,b)\in A\times B$ עובר לפונקציה $f(i)=\begin{cases}a & i=1\\ b & i=2\end{cases}$.

- עבור n טבעי וקבוצה A, נגדיר $A^n \triangleq \prod_{i=1}^{n} A$ (דהיינו $A_i = A$ לכל $1 \leq i \leq n$). את אברי A^n לרוב מסמנים בפשטות $(a_1, \ldots, a_n)$. לאיבר כזה קוראים לעתים "n־יה". נשים לב שניתן להגדיר גם את A^n בתור אוסף הפונקציות מהקבוצה $n = \{0, 1, \ldots, n-1\}$ אל A, ואז מתקבלת קבוצה איזומורפית ל־$\prod_{i=1}^{n} A$.

- עבור $\Lambda = \mathbb{N}$ וקבוצה A, המכפלה $\prod_{i \in \mathbb{N}} A$ היא אוסף **הסדרות האינסופיות** עם איברים מתוך A. לעתים מסמנים מכפלה זו ב־A^ω, כאשר $\omega = \{0, 1, 2, \ldots\}$, ואז סימון זה תואם את ההגדרה של A^ω כאוסף הפונקציות מ־ω אל A.

3.3.4 הגדרה אינדוקטיבית של קבוצות

בהמשך יהיה נוח לחשוב על $f : X^n \to X$ כעל פונקציה ב־n משתנים ($n \geq 1$), שכל אחד מהם מקבל ערך של איבר ב־X. לפונקציה כזו נקרא "פונקציה n־ארית".

תהא $f : X^n \to X$ פונקציה n־ארית מקבוצה לעצמה ו־$A \subseteq X$ תת־קבוצה של X.

הגדרה 3.26 A **סגורה** תחת f אם $f(A) \subseteq A$. כלומר, לכל $a \in A$ מתקיים $f(a) \in A$.

מייד נרחיב הגדרה זו לסגירות תחת קבוצות של פונקציות. נשתמש בסימון $F \subseteq \bigcup_{n \geq 1} X^{X^n}$ כדי לתאר קבוצה של פונקציות מ־n־יות של אברי X (לא בהכרח אותו n לכל הפונקציות בקבוצה) ל־X.

הגדרה 3.27 A סגורה תחת F אם $\bigcup_{f \in F} f(A) \subseteq A$, כלומר לכל $a \in A$ ו־$f \in F$ מתקיים $f(a) \in A$.

נראה מספר דוגמאות ולאחר מכן שימוש חשוב של ההגדרה בבנייה של קבוצות.

- $\emptyset, X$ שתיהן סגורות תחת כל פונקציה f באופן טריוויאלי.

- אם $X = \mathbb{R}$ ו־$A = \mathbb{N}$, אז A סגורה תחת הפונקציה $f(x) = x + 1$ ואינה סגורה תחת הפונקציה $f(x) = x - 1$ (למשל, כי $0 \in A$ אבל $f(0) = -1 \notin A$).

הגדרה 3.28 תהא X קבוצה, $B \subseteq X$ תת־קבוצה של X, ו־$F \subseteq \bigcup_{n \geq 1} X^{X^n}$ קבוצת פונקציות.

הקבוצה הנוצרת מתוך הבסיס B על ידי פונקציות היצירה F היא הקבוצה $X_{B,F} \triangleq \bigcap_{l \in \Lambda} A_l$, כאשר $\{A_l\}_{l \in \Lambda}$ הוא אוסף הקבוצות $A_l \subseteq X$ המקיימות:

1. $B \subseteq A_l$.
2. A_l סגורה תחת F.

ההגדרה חוקית שכן החיתוך $\bigcap_{l \in \Lambda} A_l$ נלקח על פני קבוצה לא ריקה של איברים, שכן X משתתפת בחיתוך.

כדי להבין את משמעות ההגדרה, נבין את התכונות ש־$X_{B,F}$ מקיימת:

משפט 3.29 תהא $X_{B,F} \subseteq X$ הקבוצה הנוצרת מתוך הבסיס B על ידי פונקציות היצירה F. אז $X_{B,F}$ מקיימת:

1. $B \subseteq X_{B,F}$.
2. $X_{B,F}$ סגורה תחת F.
3. $X_{B,F}$ מינימלית ביחס לשתי התכונות הקודמות, כלומר אם $C \subseteq X$ היא קבוצה שמקיימת את תכונות 1,2 אז $X_{B,F} \subseteq C$.

הוכחה: תכונה 1 נובעת מכך ש־$B \subseteq A_l$ לכל $l \in \Lambda$ בחיתוך שמגדיר את $X_{B,F}$: אם $b \in B$ אז $b \in A_l$ לכל $l \in \Lambda$ (תכונה 1 בהגדרה), ולכן $b \in \bigcap_{l \in \Lambda} A_l = X_{B,F}$.

תכונה 2 מוכחת באופן דומה: אם $f \in F$ ו־$a \in X_{B,F}$, אז $a \in A_l$ לכל $l \in \Lambda$, ולכן $f(a) \in A_l$ (תכונה 2 בהגדרה) ולכן $f(a) \in \bigcap_{l \in \Lambda} A_l = X_{B,F}$.

תכונה 3 נובעת מכך ש־אם C מקיימת את תכונות 1,2 אז בפרט C משתתפת בחיתוך שמגדיר את A, ולכן $X_{B,F} \subseteq C$.

■

את המינימליות של $X_{B,F}$ ניתן להבין בדרך נוספת: לא קיימים ב־$X_{B,F}$ איברים שאינם **הכרחיים** כדי ש־$X_{B,F}$ תקיים את תכונות 1 ו־2.

מסקנה 3.30 קיימת קבוצה יחידה שמקיימת את תכונות 3־1 של המשפט הקודם.

הוכחה: נניח כי קיימות שתי קבוצות A_1, A_2 המקיימות תכונות אלו. אז מכיוון שכל אחת מהן מקיימת את שתי התכונות הראשונות, מתכונה 3 עולה ש־$A_1 \subseteq A_2$ ו־$A_2 \subseteq A_1$ ולכן $A_1 = A_2$. ■

דוגמאות: בכל הדוגמאות $X = \mathbb{R}$. הפונקציה $+$ היא הפונקציה $+(a,b) = a + b$, ובדומה נגדיר גם את הפונקציות $-$ ו־$/$.

- עבור $F = \{+\}$ ו־$B = \{0,1\}$ נקבל ש־$X_{B,F}$ היא $\mathbb{N} = \{0,1,2,3,\dots\}$.
- עבור $F = \{+\}$ ו־$B = \{0\}$ נקבל ש־$X_{B,F}$ היא $\{0\}$.
- עבור $F = \{+,-\}$ ו־$B = \{1\}$ נקבל ש־$X_{B,F}$ היא $\mathbb{Z} = \{0,1,-1,2,-2,\dots\}$.
- עבור $F = \{+,-,/\}$ ו־$B = \{1\}$ נקבל ש־$X_{B,F}$ היא $\mathbb{Q} = \left\{\frac{a}{b} | a,b \in \mathbb{Z}\right\}$. כאן אנו מגדירים שרירותית $/(a,0) = a$ כדי לקבל פונקציה שמוגדרת לכל זוג ב־A^2.

טהרנים שמעוניינים לפשט את ההגדרה של הקבוצה הנוצרת ככל האפשר יכולים לעשות זאת על ידי ביטול קבוצת הבסיס B, והרחבת הגדרת F כך שתכיל גם פונקציות 0־אריות, אם מקבלים את הקונבנציה ש־$f : X^0 \to X$ הוא פשוט איבר כלשהו של X (ולכן B ניתנת להחלפה בקבוצה של פונקציות $f : X^0 \to X$). לא ננקוט בגישה זו כאן שכן הפרדה קונספטואלית בין ה"בסיס" B ו"כללי היצירה" F מסייעת להבנת האופן שבו הקבוצות נבנות.

אחד היתרונות של הגדרה אינדוקטיבית של קבוצות היא הקלות שבה ניתן להוכיח טענות עליהן: די להוכיח שהטענה מתקיימת לאברי הבסיס B, ושהיא משתמרת בהפעלת הפונקציה F. הסיבה לכך מתחוורת כאשר מנסים להגדיר פורמלית **טענה**: הדרך הפשוטה ביותר היא להגדיר אותה בתור תת־קבוצה $P \subseteq X$ של כל האיברים ב־X שהטענה מתקיימת עבורם. אם הטענה מתקיימת עבור כל אברי B ומשתמרת בהפעלת הפונקציה F, הרי ש־$B \subseteq P$ ו־P סגורה ל־F ועל כן כפי שראינו $A \subseteq P$, ומכאן שכל אברי $X_{B,F}$ מקיימים את התכונה P. נסכם זאת:

מסקנה 3.31 (אינדוקציית מבנה) אם $X_{B,F}$ היא הקבוצה הנוצרת מהבסיס B וכללי היצירה F, ו־P היא תכונה כלשהי, כך ש:

1. כל אברי B מקיימים את P.
2. אם $f(x_1,\dots,x_n) \in F$ ו־$a_1,\dots,a_n \in X$ הם איברים המקיימים את P אז $f(a_1,\dots,a_n)$ מקיים את P.

אז כל אברי $X_{B,F}$ מקיימים את P.

עבור $B = \{0\}$ וכלל היצירה $f(x) = x + 1$ מקבלים את האינדוקציה המתמטית ה"רגילה".

לרוב נוח לחשוב על אברי $X_{B,F}$ בתור תוצרים של "תהליך" שבו מתחילים מאיברים ב־B ובונים מהם איברים מורכבים יותר על ידי הפעלות של פונקציות מ־F:

הגדרה 3.32 סדרת יצירה עבור איבר $a \in X_{B,F}$ היא סדרה **סופית** $a_1,\dots,a_n \in X_{B,F}$ כך ש:

1. $a = a_n$.
2. לכל $1 \le i \le n$, או ש־$a_i \in B$ או ש־a_i התקבל מאיברים קודמים בסדרה על ידי הפעלת פונקציה מ־F. פורמלית: קיימים $a_{k_1},\dots,a_{k_m}$ כך ש־$k_j < i$ לכל $1 \le j \le m$ וקיימת $f \in F$ כך ש־$a_i = f(a_{k_1},\dots,a_{k_m})$.

טענה 3.33 $a \in X_{B,F}$ אם ורק אם קיימת סדרת יצירה עבור a.

הוכחה: ראשית נוכיח שכל a שיש לו סדרת יצירה שייך ל־$X_{B,F}$, באינדוקציה על **אורך סדרת היצירה**. עבור סדרה מאורך 1, a_1, בהכרח $a_1 \in B \subseteq X_{B,F}$ (כי לא ייתכן ש־a_1 התקבל מאיברים קודמים). עבור סדרה מאורך n, $a_1,\dots,a_n$, הנחת האינדוקציה היא ש־$a_1,\dots,a_{n-1}$ שייכים כולם ל־$X_{B,F}$. כעת, אחד משניים: או ש־$a_n \in B \subseteq X_{B,F}$, או ש־$a_n = f(a_{k_1},\dots,a_{k_m})$ כך ש־$a_{k_1},\dots,a_{k_m}$ שייכים כולם ל־$X_{B,F}$ ו־$f \in F$ ומסגירות $X_{B,F}$ נקבל ש־$a = a_n \in X_{B,F}$.

כעת נוכיח שלכל $a \in X_{B,F}$ קיימת סדרת יצירה, באינדוקציית מבנה על $X_{B,F}$.

בסיס: אם $a \in B$ אז $a_1 = a$ היא סדרת יצירה עבור a.

צעד: אם $a=f\left(a_1,\dots,a_n\right)$ עבור $f\in F$ ו־$a_i\in X_{B,F}$ אשר לכל אחד מהם קיימת סדרת יצירה, אז פשוט נשרשר את כל סדרות היצירה של a_i אלו לאלו ונוסיף את a בסוף. קיבלנו סדרת יצירה עבור a שהיא עדיין סופית (כי היא שרשור של מספר סופי של סדרות סופיות). ■

שימו לב כי ל־$a\in X_{B,F}$ יכולות להיות סדרות יצירה רבות ושונות, ולא רק סדרת יצירה אחת. זאת מכיוון שאפשר "לערבב" את הסדר שבו מופיעים חלק מהאיברים בכל סדרת יצירה, וכמו כן בגלל ש־a עשוי להתקבל כפלט של f עבור קלטים שונים.

4 עוצמות

4.1 מדידת גדלים של קבוצות

מהו גודל של קבוצה? אינטואיטיבית, גודל הוא **מספר** האיברים שבקבוצה. הקבוצה $A=\{0,1e,\pi,i\}$ כוללת חמישה איברים ולכן טבעי לומר שגודלה הוא 5. עם זאת, זוהי איננה הגדרה פורמלית; אם נגדיר "גודל קבוצה הוא מספר האיברים שבה" נצטרך להסביר מהו "מספר האיברים" שגם אותו טרם הגדרנו. אם כן, עלינו למצוא דרך לתאר גודל של קבוצות באמצעות המושגים שבנינו עד כה. כאן נחלץ מושג ה**פונקציה** לעזרתנו: אנחנו יכולים להשתמש בפונקציה כדי **למספר** את אברי הקבוצה. למשל, נתבונן בפונקציה:

$f\left(0\right)=0,f\left(1\right)=1,f\left(e\right)=2,f\left(\pi\right)=3,f\left(i\right)=4$

פונקציה זו ממספרת את אברי A מ־0 ועד 4, ובכך מהווה אינדיקציה לכך שיש ב־A בדיוק חמישה איברים. נשים לב לכך שזו רחוקה מלהיות הפונקציה היחידה שמתאימה למטרה זו; כך למשל גם הפונקציה

$g\left(0\right)=3,g\left(1\right)=0,g\left(e\right)=4,g\left(\pi\right)=2,g\left(i\right)=1$

מראה את אותו הדבר בדיוק, אף שכעת המספור "מעורבב" ביחס למספור ש־f הציעה.

התכונות החשובות שמשותפות הן ל־f והן ל־g הן ששתיהן חד־חד־ערכיות ושתיהן על מהקבוצה A אל הקבוצה $B=\{0,1,2,3,4\}$. כדי להמחיש את חשיבות תכונות אלו נתבונן בשתי דוגמאות נגדיות:

- הפונקציה $h:\{0,1\}\to\{0\}$ המוגדרת על ידי $h\left(0\right)=h\left(1\right)=0$ היא על הקבוצה $\{0\}$ אך איננה חד־חד ערכית. מכאן האינטואיציה שאם יש פונקציה $h:A\to B$ שהיא **על** B אז גודלה של A הוא לפחות כגודל B, אבל יכול להיות גם גדול יותר.
- הפונקציה $h:\{0\}\to\{0,1\}$ המוגדרת על ידי $h\left(0\right)=0$ היא חח"ע אך איננה על, ומכאן האינטואיציה שאם יש פונקציה $h:A\to B$ שהיא חח"ע אז גודלה של A הוא לכל היותר כגודל B.

מכאן אנו מגיעים להגדרה המרכזית שלנו. מכיוון שהמושג שאנו מתארים יהיה תקף גם לקבוצות אינסופיות, לא נשתמש במילה "גודל" אלא במילה "עוצמה", שהיא פחות טעונה במשמעויות אינטואיטיביות.

הגדרה 4.1 בהינתן שתי קבוצות A,B, נאמר שהן **שוות עוצמה** ונסמן זאת $|A|=|B|$ אם קיימת פונקציה חח"ע ועל $f:A\to B$. במילים אחרות, קבוצות הן שוות עוצמה אם ורק אם הן שקולות.

נתבונן בכמה דוגמאות קונקרטיות של שוויון עוצמה בין קבוצות (נציג את הפונקציה החח"ע ועל המתאימה בין הקבוצות אך לא נוכיח כי היא אכן חח"ע ועל):

- נסמן $\mathbb{S}=\{0,1,4,9,16,\dots\}=\left\{n^2|n\in\mathbb{N}\right\}$ קבוצת הריבועים של מספרים טבעיים. אז $\mathbb{N}\sim\mathbb{S}$ עם הפונקציה $f\left(n\right)=n^2$.
  אבחנה מפתיעה זו ניתנה כבר על ידי גלילאו. תוצאה זו נראית מוזרה ממבט ראשון שכן לא רק ש־$\mathbb{S}$ היא קבוצה חלקית ל־$\mathbb{N}$, אלא גם שה"חורים" בין שני איברים סמוכים של A הולכים וגדלים: בין 4 ו־9 "חסרים" 4 מספרים טבעיים, בין 9 ו־16 "חסרים" 6 , בין 16 ל־25 "חסרים" 8 וכדומה.
- $\mathbb{R}\sim(0,1)$. נבנה את ההתאמה החח"ע והעל בין שתי הקבוצות כהרכבה של מספר התאמות חח"ע ועל בין "קבוצות ביניים":
  - נגדיר $f_1:(0,1)\to(-1,1)$ על ידי $f_1\left(x\right)=2x-1$. פונקציה זו ראשית "מותחת" את הקטע $(0,1)$ והופכת אותו ל־$(0,2)$ ולאחר מכן מזיזה אותו יחידה אחת שמאלה והופכת אותו ל־$(-1,1)$.
  - נגדיר $f_2:(-1,1)\to\left(-\frac{\pi}{2},\frac{\pi}{2}\right)$ על ידי $f_2\left(x\right)=\frac{\pi}{2}x$. גם כאן האפקט הוא של "מתיחה" של הקטע על ידי הכפלה במספר קבוע.

- נגדיר $f_1 : \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \to \mathbb{R}$ על ידי $f_3(x) = \tan x$. הבחירה בטנגנס כאן היא מכיוון שזוהי פונקציה מוכרת ופשוטה שמבצעת את האפקט המבוקש ("מריחת" קטע סופי על פני כל הממשיים).
- כעת נגדיר $f : (0,1) \to \mathbb{R}$ על ידי ההרכבה $f = f_3 f_2 f_1 = \tan\left(\frac{\pi}{2}(2x-1)\right)$. ניתן לבדוק כי f_i חח"ע ועל לכל $1 \le i \le 3$ ולכן כך גם f.

- $\mathbb{N} \sim \mathbb{N} \cup \{-1\}$ ("המלון של הילברט", מקרה 1) עם הפונקציה $f : \mathbb{N} \cup \{-1\} \to \mathbb{N}$ המוגדרת על ידי $f(x) = x + 1$.
- $\mathbb{N} \sim \mathbb{N} \times \{0,1\}$ ("המלון של הילברט", מקרה 2) עם הפונקציה $f : \mathbb{N} \times \{0,1\} \to \mathbb{N}$ המוגדרת על ידי $f((n,x)) = 2n + x$.

הגדרה 4.2 נסמן $|A| \le |B|$ אם ורק אם קיימת פונקציה חח"ע $f : A \to B$.

ראינו במסקנה 3.20 שקיימת $f : A \to B$ חח"ע אם ורק אם קיימת $g : B \to A$ על. לכן מתבקש להשתמש בסימון $|A| \ge |B|$ אם קיימת פונקציה $f : A \to B$ שהיא על.

משפט 4.3 (קנטור־שרדר־ברנשטיין) אם $|A| \le |B|$ וגם $|B| \le |A|$ אז $|A| = |B|$.

הוכחה: תינתן בהמשך. ■

נזכור כי בפרק 2.7 הגדרנו את כל המספרים הטבעיים באופן האינדוקטיבי הבא: $0 \triangleq \emptyset$ ו־$n + 1 \triangleq n \cup \{n\}$. זה מצדיק את השימוש בסימון הבא: $\{0, 1, 2, \ldots, n\}$.

הגדרה 4.4 נסמן $|A| = n$ אם $|A| = |n|$, כלומר $A \sim n$. אם $|A| = n$ עבור n טבעי כלשהו, אז נאמר ש־A היא **קבוצה סופית**.

קיימות דרכים אחרות להגדיר קבוצות סופיות, אך ההגדרה שלעיל היא טבעית ונוחה למדי.

הגדרה זו מצדיקה את האופן שבו אנו כותבים כל קבוצה סופית A בתור $A = \{a_1, a_2, \ldots, a_n\}$; ניתן לחשוב על a_i בתור $f(i)$ כאשר $f : n \to A$ היא חח"ע ועל.

טענה 4.5 אם A, B קבוצות סופיות, אז מתקיים:

1. $|A \cup B| = |A| + |B| - |A \cap B|$
2. $|A \times B| = |A| \cdot |B|$
3. $\left|A^B\right| = |A|^{|B|}$ (ובפרט $\left|2^A\right| = 2^{|A|}$, כלומר $|\mathcal{P}(A)| = 2^{|A|}$).

הוכחה פורמלית לטענות אלו צריכה להתבסס על הגדרה פורמלית לפעולות החשבון של המספרים הטבעיים (ולא נתנו הגדרה כזו) ולכן נפסח עליה (נעיר כי דרך אחת **להגדיר** את פעולות החשבון של הטבעיים היא באמצעות נוסחאות אלו).

מטענה זו נובעת האבחנה הפשוטה הבאה:

מסקנה 4.6 אם A, B סופיות כך גם $A \cup B$ ו־$A \cap B$.

הוכחה: מכיוון ש־$|A \cup B| = |A| + |B| - |A \cap B|$ הרי ש־$|A \cup B| + |A \cap B| = |A| + |B|$. אגף ימין הוא סופי כסכום שני מספרים טבעיים ולכן גם המחוברים באגף שמאל כאלו. ■

4.2 קבוצות אינסופיות

אם קבוצה איננה סופית הרי שהיא **אינסופית**. אנו מכירים קבוצה אחת כזו לפחות:

טענה 4.7 $\mathbb{N}$ היא קבוצה אינסופית. בפרט, לכל $n \in \mathbb{N}$, לא קיימת פונקציה על $f : n \to \mathbb{N}$.

הוכחה: יהא $n \in \mathbb{N}$ מספר טבעי כלשהו ופונקציה $f : n \to \mathbb{N}$ כלשהי. נגדיר $a = \max\{f(0), \ldots, f(n-1)\} + 1$, אז $a \in \mathbb{N}$ הוא איבר ב־$\mathbb{N}$ שאין לו מקור ב־n, כי הוא גדול ב־1 מכל תמונה של איבר ב־n, ולכן f אינה על. מכיוון ש־f הייתה פונקציה כלשהי, נסיק שלא קיימת פונקציה על מ־n אל $\mathbb{N}$ (ובפרט לא קיימת פונקציה חח"ע ועל). ■

נשים לב כי קיומה של קבוצה אינסופית אינו נובע משאר אקסיומות תורת הקבוצות! אנו נזקקים לאקסיומה מפורשת שמניחה קיום של קבוצה אינסופית.

במובן מסוים $\mathbb{N}$ היא הקבוצה האינסופית מהגודל "הקטן ביותר", כפי שמראה האפיון הבא להיות קבוצה אינסופית:

משפט 4.8 A היא אינסופית אם ורק אם קיימת פונקציה $f : \mathbb{N} \to A$ שהיא חח"ע.

הוכחה: נניח כי קיימת $f : \mathbb{N} \to A$ שהיא חח"ע, אז יש פונקציה $g : A \to \mathbb{N}$ שהיא על. אם קיימת פונקציה $h : n \to A$ שהיא חח"ע ועל עבור n טבעי כלשהו, אז ההרכבה $gh : n \to \mathbb{N}$ היא על $\mathbb{N}$ וכבר ראינו כי לא קיימת פונקציה מ־n על $\mathbb{N}$.

בכיוון השני, נגדיר את הפונקציה באופן אינדוקטיבי על ידי סדרת קבוצות $A_0, A_1, \ldots$ כך ש־$A_0 = A$, $f(n) \in A_n$ ו־$A_{n+1} = A_n \setminus \{f(n)\}$. נניח בשלילה שמתישהו $A_n = \emptyset$ ל־n כלשהו ולכן הבניה "נתקעת", אז $A = \{f(0), \ldots, f(n-1)\}$ וקיבלנו ש־$f : n \to A$ היא חח"ע ועל ולכן A סופית. מכאן שלא מתקיים $A_n = \emptyset$ לאף איבר בבניה וקיבלנו $f : \mathbb{N} \to A$ שהיא חח"ע. ■

נציין כי בהוכחת הכיוון השני במשפט לעיל השתמשנו באופן מובלע ב**אקסיומת הבחירה**. לא נציג את האקסיומה והשלכותיה במלואן בקורס, אך נעיר כי גם את אקסיומת הבחירה יש להניח במפורש כחלק מהאקסיומות של תורת הקבוצות (אחרת המשפט לעיל לא יהיה נכון כלל).

בעזרת אפיון זה קל להוכיח דרכים נוספות להראות כי קבוצה היא אינסופית:

משפט 4.9 תהא A קבוצה אינסופית.

1. אם $A \subseteq B$ אז B אינסופית.
2. אם קיימת פונקציה $f : A \to B$ חח"ע אז B אינסופית.
3. אם קיימת פונקציה $f : B \to A$ על אז B אינסופית.
4. 2^A אינסופית.
5. לכל B, $A \cup B$ אינסופית.
6. לכל $B \neq \emptyset$, $A \times B$ אינסופית.
7. לכל $B \neq \emptyset$, A^B אינסופית.

הוכחה: מכיוון ש־A אינסופית יש פונקציה $g : \mathbb{N} \to A$ שהיא חח"ע.

1 נובע כעת מכך ש־$g : \mathbb{N} \to B$ היא חח"ע (אותה פונקציה בדיוק).

2 נובע מכך ש־$fg : \mathbb{N} \to B$ היא חח"ע כהרכבת הפונקציות החח"ע g ו־f.

3 נובע מכך שאם קיימת $f : B \to A$ על אז קיימת $h : A \to B$ חח"ע, ומ־2.

4. נובע מכך שקיימת פונקציה חח"ע $f : A \to 2^A$ הנתונה על ידי $f(x) = \{x\}$ ומ־2.

5. נובע מכך שקיימת פונקציה חח"ע $f : A \to A \cup B$ הנתונה על ידי $f(x) = x$ ומ־2.

6 נובע מכך שקיימת פונקציה חח"ע $f : A \to A \times B$ הנתונה על ידי $f(x) = (x, b)$ עבור $b \in B$ מסויים, ומ־2.

7 נובע מכך שקיימת פונקציה חח"ע $f : A \to A^B$ הנתונה על ידי $f(x) = \{(b, x) \mid b \in B\}$ ומ־2 (אם $B \neq \emptyset$ אז הקבוצות $\{(b, x) \mid b \in B\}$ שונות אלו מאלו). ■

4.3 קבוצות בנות מניה

ראינו כבר את החשיבות של $\mathbb{N}$ בתור הדוגמה הבסיסית שלנו לקבוצה אינסופית "קטנה ביותר". זה מצדיק את השימוש בסימונים מיוחדים:

הגדרה 4.10 אם $|A| = |\mathbb{N}|$ נאמר ש־A היא קבוצה שעוצמתה **אלף־אפס** ונסמן זאת $|A| = \aleph_0$. אם A סופית או מעוצמה $\aleph_0$ נאמר גם ש־A היא **בת־מניה**.

ישנם כאלו שמשתמשים ב"בת מניה" כדי לתאר רק קבוצות אינסופיות מעוצמה $\aleph_0$; כדי למנוע בלבול נאמר במפורש על מקרים כאלו "בת־מניה אינסופית".

הסימון $\aleph_0$ מרמז כי יש גם $\aleph_1, \aleph_2$ וכדומה, ואכן ישנם כאלו, אך הדיון בהם מצריך דיון **בסודרים** שלא יוצגו בקורס זה.

אם קבוצה היא בת מניה אינסופית, אז ניתן להציג אותה בתור **סדרה** של איברים: $A = \{a_0, a_1, a_2, \dots\}$. בכיוון ההפוך, אם ניתן להציג שיטה **למספור** אברי קבוצה כלשהי, אז הקבוצה היא בת מניה:

טענה 4.11 אם קיימת סדרה שבה מופיעים כל אברי A, אז A בת מניה.

הוכחה: נגדיר פונקציה $f : A \to \mathbb{N}$ שמתאימה לכל איבר A את האינדקס של המקום הראשון בסדרה שבו הוא מופיע (זהו מספר טבעי). זוהי בבירור פונקציה חח"ע ולכן $|A| \le |\mathbb{N}|$. אם A סופית, סיימנו; אחרת, $|\mathbb{N}| \le |A|$ וממשפט קנטור־שרדר־ברנשטיין נקבל $|A| = |\mathbb{N}| = \aleph_0$. ■

בזכות טענה זו קל להוכיח שקבוצות הן בנות מניה מבלי להזדקק להצגה של פונקציה חח"ע ועל מפורשת בין A והטבעיים - פשוט מציגים דרך שיטתית כלשהי למנות, או לסדר, או לייצר באופן סדרתי, את אברי A. שימו לב שאין מניעה אפילו שאותו איבר של A יופיע מספר פעמים במניה.

טענה 4.12 $|\mathbb{Z}| = \aleph_0$

הוכחה: באמצעות המספור $0, 1, -1, 2, -2, \dots$. בשלב ה־k של המספור נספרים k ו־$-k$. ■

טענה 4.13 (קנטור) $|\mathbb{Q}| = \aleph_0$

הוכחה: אינטואיטיבית, הרעיון של קנטור הוא כדלהלן: כתבו טבלה אינסופית שבה בשורה ה־a והעמודה ה־b נמצא המספר $\frac{a}{b}$. כעת עברו סדרתית על הטבלה על גבי **האלכסונים המשניים** שלה. כלומר, התחילו מ־$(1,1)$; אחר כך עברו על האלכסון $(1,2), (2,1)$; לאחר מכן על $(3,1), (2,2), (1,3)$ וכן הלאה.

באופן פורמלי אנו מבצעים את האלגוריתם הבא:

1. הוסף את 0 למניה.
2. לכל $n = 1, 2, \dots$:
   (א) לכל $a = 1, \dots n-1$:
      i. הוסף למניה את $\frac{a}{b}$ ואת $-\frac{a}{b}$ כאשר $b = n - a$.

יהא $\frac{a}{b}$ מספר רציונלי כלשהו עם $a, b > 0$, אז בבירור הוא יופיע במניה בשלב שבו $n = a + b$. לכן כל מספר רציונלי מופיע במניה (ולמעשה, כל מספר יופיע אינסוף פעמים בה). ■

תוצאה זו של קנטור היא מפתיעה למדי בשל ההבדלים המהותיים בין הטבעיים והרציונליים; בין כל זוג טבעיים קיימים אינסוף רציונליים.

את שיטת ההוכחה ניתן להכליל לתוצאה חזקה אף יותר:

משפט 4.14 תהא $A_0, A_1, A_2, \dots$ סדרה של קבוצות כך ש־$|A_n| = \aleph_0$. אז $|\bigcup_{n=0}^{\infty} A_n| = \aleph_0$ (איחוד בן מניה של קבוצות בנות מניה הוא בן מניה).

הוכחה: גם כאן נשתמש במניה באמצעות לולאה מקוננת:

1. לכל $n = 0, 1, 2, \dots$:
   (א) לכל $k = 0, 1, 2, \dots, n$:
      i. הוסף למניה את a_k^n כאשר a_k^n הוא האיבר ה־k במניה של A_n.

■

נשים לב שהטענה נכונה גם עבור איחודים סופיים של קבוצות, $A_1, \dots, A_k$; פשוט נגדיר $A_n = A_k$ לכל $n > k$ ונשתמש במשפט. בדומה, אם אחת מהקבוצות A_n היא סופית אפשר פשוט להגדיר $a_k^n = a_1^n$ לכל $k > |A_n|$ ולכן די לדרוש ש־$|A_n| \le \aleph_0$.

משפט 4.15 אם $|A| = |B| = \aleph_0$ אז $|A \times B| = \aleph_0$

הוכחה: ניתן למנות את אברי A: $A = \{a_0, a_1, a_2, \dots\}$. כעת, $A \times B = \bigcup_{n=0}^{\infty} \{(a_n, b) \,|b \in B\}$, והקבוצות $\{(a_n, b) \,|b \in B\}$ הן בנות מניה שכן קיימת התאמה חח"ע ועל בין כל אחת מהן ל־B ($(a_n, b) \mapsto b$). כעת נשתמש בטענה הקודמת. ■

4.4 האלכסון של קנטור

עד כה ראינו קבוצות רבות שהן בנות מניה, והדבר עשוי לתת את התחושה כי **כל** קבוצה היא בת מניה. אחת מתגליותיו הגדולות של קנטור הייתה כי לא כך הדבר.

משפט 4.16 (**האלכסון של קנטור**) $|\mathbb{R}| \neq \aleph_0$

הוכחה: נניח כי $|\mathbb{R}| = \aleph_0$ ולכן קיימת לה מניה. עבור מניה זו, נבנה מספר ממשי אשר **אינו** מופיע בתוך המניה; מכיוון שנציג שיטה שעושה זאת עבור **כל** מניה של $\mathbb{R}$, המסקנה תהיה שמניה של $\mathbb{R}$ אינה קיימת.

הרעיון הוא לבנות את המספר שאינו מופיע במניה על ידי כך שנבטיח שהוא יהיה שונה "קצת" מכל מספר במניה ־ מספיק יהיה לקלקל ספרה אחת בכל אחד מהמספרים במניה. הסיבה שבגללה נוכל לעשות זאת היא שבמספר ממשי יש **אינסוף** ספרות שיש לנו חופש פעולה לקבוע.

ראשית, נזכור כי ראינו כי $|\mathbb{R}| = |(0,1)|$ ולכן די להוכיח כי $|(0,1)| \neq \aleph_0$. כל מספר ממשי בין 0 ל־1 ניתן לכתיבה בתור $0.a_1a_2a_3\dots$ כאשר $a_i \in \{0,1,2,\dots,9\}$ היא ספרה. קיימים מספרים שניתן להציג בשתי דרכים שונות, כך למשל $0.8999\dots = 0.9000\dots$. תופעה זו מתרחשת רק במספרים שנגמרים בסדרה אינסופיות של 9 או 0 ולא תהיה רלוונטית עבור ההוכחה.

נניח כי קיים מספור של המספרים הממשיים בין 0 ו־1, אז נכתוב טבלה שבה השורות הן המספרים והעמודות הן הספרות:

$$\begin{aligned} r^1 &= 0.a_1^1a_2^1a_3^1a_4^1\dots \\ r^2 &= 0.a_1^2a_2^2a_3^2a_4^2\dots \\ r^3 &= 0.a_1^3a_2^3a_3^3a_4^3\dots \\ &\vdots \end{aligned}$$

וכעת נבנה מספר ממשי $b = 0.b_1b_2b_3\dots$ השונה מכל המספרים $r^1, r^2, \dots$ על ידי כך שנגדיר אותו בתור מעין היפוך של **האלכסון** של הטבלה: $b_n = \begin{cases} 3 & a_n^n = 4 \\ 4 & a_n^n \neq 4 \end{cases}$

נניח בשלילה כי $b = r^n$ עבור n כלשהו; אז נשים לב לכך ש־$b_n \neq a_n^n$, כלומר b נבדל מ־r^n בספרה במקום ה־n. זה מראה כי $b \neq r^n$ שכן הדרך היחידה שבה ייתכן $b = r^n$ למרות ההבדל בספרה היא אם הספרה היא 0 באחד המספרים ו־9 בשניה. ■

תוצאה זו מצביעה על הבדל מהותי ביותר בין המספרים הרציונליים והממשיים. הבדל זה מפתיע למדי בהתחשב בתכונת **הצפיפות** של הרציונליים: בין כל שני מספרים ממשיים קיים מספר רציונלי.

הסיבה שבגללה לא ניתן להוכיח שהרציונליים אינם בני מניה באותה הדרך היא שהפיתוח העשרוני של הרציונליים הוא **מחזורי** (החל ממקום מסויים). בשל כך, לא ניתן להסתפק בבניה של b כפי שהוצגה כאן, שכן הכרחי להבטיח ש־b שיתקבל יהיה בעל פיתוח עשרוני מחזורי (החל ממקום מסויים). מכיוון שלא ניתן לעשות זאת, ההוכחה נכשלת.

מכיוון ש־$|\mathbb{R}| \neq \aleph_0$ קיימים סימונים מיוחדים לעוצמה זו:

הגדרה 4.17 $|\mathbb{R}|$ נקראת **עוצמת הרצף** והיא מסומנת לעתים כ־$|\mathbb{R}| = \mathfrak{c}$, או כ־$2^{\aleph_0}$ (הסיבה לסימון האחרון תתברר בהמשך).

קנטור הוכיח משפט כללי יותר מאשר רק $|\mathbb{R}| \neq \aleph_0$ (אך תוצאה זו ראויה להצגה נפרדת בשל הוכחתה הציורית והאינטואיטיבית יחסית), שמראה כי ישנן **אינסוף** עוצמות שונות:

משפט 4.18 (קנטור) לכל קבוצה A, $|2^A| > |A|$, כלומר עוצמת קבוצת החזקה של A גדולה מעוצמת A.

הוכחה: קל לראות ש־$\left|2^A\right| \le |A|$ על ידי הפונקציה החח"ע $f(x) = \{x\}$. עיקר ההוכחה היא כי $|A| \ne \left|2^A\right|$.
נניח בשלילה כי קיימת פונקציה חח"ע ועל $f: A \to 2^A$, ונגדיר קבוצה $D = \{a \in A | a \notin f(a)\}$.
על פי הגדרתה, $D \subseteq A$ ולכן $D \in 2^A$; מכיוון ש־f על, קיים $x \in A$ כך ש־$f(x) = D$.
כעת, אם $x \in D$ אז $x \in f(x)$ ולכן על פי הגדרת D, $x \notin f(x)$ כלומר $x \notin D$, סתירה; ואילו אם $x \notin D$ אז $x \notin f(x)$ ולכן על פי הגדרת D, $x \in D$, ושוב הגענו לסתירה. ■

הדמיון של הוכחה זו לפרדוקס של ראסל אינו מקרי; ראסל גילה את הפרדוקס בזמן שעסק בהוכחה זו של קנטור. למעשה, עוד לפני ראסל גילה קנטור פרדוקס שנובע מייד ממשפטו:

משפט 4.19 (**פרדוקס קנטור**) "קבוצת כל הקבוצות" אינה קיימת.

הוכחה: נניח שקיימת קבוצה X כך שכל קבוצה שייכת ל־X. אז בפרט כל איבר של 2^X שייך ל־X, דהיינו $2^X \subseteq X$, כלומר $\left|2^X\right| \le |X|$, בסתירה לכך ש־$|X| < \left|2^X\right|$. ■

המסקנה מפרדוקס זה, בדומה לפרדוקס ראסל, היא שלא כל אוסף של קבוצות הוא בעצמו קבוצה. את אוסף כל הקבוצות מכנים אם כן **מחלקה** ולא מניחים שהוא מקיים תכונות של קבוצות ובפרט לא ניתן לדבר על עוצמת מחלקת כל הקבוצות.
משפט קנטור מצדיק את השימוש בסימון $2^{|A|}$ כדי לתאר עוצמות; זוהי עוצמתה של קבוצת החזקה של A. בפרט, אם $|A| = \aleph_0$ אז $2^{\aleph_0}$ מסמנת את עוצמת קבוצת החזקה של A (אנו מתבססים כאן על ההנחה שלא הוכחנו כי אם $A \sim B$ אז $2^A \sim 2^B$).
משפט קנטור מראה בפרט כי $\aleph_0 \ne \left|2^{\mathbb{N}}\right| = 2^{|\mathbb{N}|} = 2^{\aleph_0}$. כעת נשלים את התמונה ונראה מהי עוצמת הרצף המדויקת. מכיוון שאנו עוסקים ב־$\mathbb{R}$, באופן טבעי למדי ההוכחה תתבסס על תוצאות סטנדרטיות באנליזה מתמטית.

משפט 4.20 $|\mathbb{R}| = 2^{\aleph_0}$

הוכחה: ראשית, נראה כי $|\mathbb{R}| \le \left|2^{\mathbb{Q}}\right| = 2^{\aleph_0}$. נגדיר פונקציה $f: \mathbb{R} \to 2^{\mathbb{Q}}$ על ידי $f(r) = \{q \in \mathbb{Q} \mid q \le r\}$ (לכל ממשי אנו מתאימים את קבוצת הרציונליים הקטנים ממנו או שווים לו). כדי לראות כי f חח"ע, יהיו $r, s \in \mathbb{R}$ שונים זה מזה ונניח בלי הגבלת הכלליות כי $r < s$, אז מצפיפות הרציונליים קיים q כך ש־$r < q < s$, כלומר $q \in f(s)$ אבל $q \notin f(r)$, מה שמוכיח כי $f(r) \ne f(s)$.
כעת נראה כי $|\mathbb{R}| \ge \left|\{0,2\}^{\mathbb{N}}\right| = 2^{\aleph_0}$ על ידי פונקציה חח"ע $\{0,2\}^{\mathbb{N}} \to \mathbb{R}$. לכל סדרה $\bar{a} = a_1, a_2, \ldots$ (אנו מתחילים את האינדקס מ־1 מטעמי נוחות הסימון בלבד) נגדיר $g(\bar{a}) = \sum_{n=1}^{\infty} \frac{a_n}{3^n}$. טור זה מתכנס תמיד (למשל, ממבחן השורש של קושי) ולכן הפונקציה מוגדרת היטב. נראה כעת כי אם $\bar{a} \ne \bar{b}$ אז $g(\bar{a}) \ne g(\bar{b})$. יהי k האינדקס הראשון בו $\bar{a}, \bar{b}$ נבדלות ונניח בלי הגבלת הכלליות כי $a_n = 2, b_n = 0$. אז:

$$\begin{aligned} g(\bar{a}) - g(\bar{b}) &= \sum_{n=1}^{\infty} \frac{(a_n - b_n)}{3^n} \\ &= \frac{2}{3^k} + \sum_{n=k+1}^{\infty} \frac{a_n - b_n}{3^n} \end{aligned}$$

כעת, $\left|\sum_{n=k+1}^{\infty} \frac{a_n - b_n}{3^n}\right| \le \sum_{n=k+1}^{\infty} \frac{2}{3^n} = \frac{2}{3^{k+1}} \sum_{n=0}^{\infty} \frac{1}{3^n} = \frac{2}{3^{k+1}} \frac{3}{2} = \frac{1}{3^k}$ ולכן $\left|g(\bar{a}) - g(\bar{b})\right| \ge \frac{2}{3^k} - \frac{1}{3^k} = \frac{1}{3^k}$, כלומר $g(\bar{a}) \ne g(\bar{b})$ ■

לתמונה של הפונקציה g שהגדרנו במהלך ההוכחה יש חשיבות בפני עצמה במתמטיקה: קבוצה זו נקראת **קבוצת קנטור** והיא מקיימת מספר תכונות מפתיעות שאת רובן לא נוכל להציג כאן. הדרך המקובלת לחשוב עליה היא זו: נגדיר $C_0 = [0,1]$, וכעת נגדיר באופן אינדוקטיבי את C_{n+1} בתור אוסף הקטעים המתקבל מ־C_n על ידי כך שמסירים מכל קטע ב־C_n את השליש האמצעי שלו. כך למשל $C_1 = \left[0, \frac{1}{3}\right] \cup \left[\frac{2}{3}, 1\right]$ ו־$C_2 = \left[0, \frac{1}{9}\right] \cup \left[\frac{2}{9}, \frac{1}{3}\right] \cup \left[\frac{2}{3}, \frac{7}{9}\right] \cup \left[\frac{8}{9}, 1\right]$ וכן הלאה. כעת נגדיר את קבוצת קנטור באמצעות $C \triangleq \bigcap_{n=0}^{\infty} C_n$. תכונה מעניינת אחת של קבוצת קנטור שנוכל להצביע עליה מייד היא כי למרות שמתקיים $|C| = 2^{\aleph_0}$ כפי שראינו, הרי שסכום הקטעים ש"הוצאנו" מ־C במהלך בנייתה הוא 1; שכן בשלב הראשון הוצאנו קטע אחד מאורך $\frac{1}{3}$; בשלב השני שני קטעים מאורך $\frac{1}{9}$; בשלישי, ארבעה קטעים מאורך $\frac{1}{27}$ וכן הלאה, מה שמניב את הסכום $\sum_{n=0}^{\infty} \frac{2^n}{3^{n+1}} = \frac{1}{3} \sum_{n=0}^{\infty} \left(\frac{2}{3}\right)^n = \frac{1}{3} \frac{1}{1-2/3} = \frac{1}{3} \cdot \frac{1}{1/3} = 1$. במילים אחרות, החסרנו מ־C את כל **האורך** מבלי לשנות את **הכמות** של איברים ב־C!
לעובדה ש־$|\mathbb{R}| \ne \aleph_0$ יש השלכות מתמטיות לא טריוויאליות. נציג כאן אחת מהן, שהוצגה על ידי קנטור עצמו במאמר שבו תיאר את שיטת האלכסון. לצורך כך נזדקק להגדרה:

הגדרה 4.21 **שורש** של פולינום $p(x)$ הוא איבר a כך ש־$p(a)=0$. **מספר טרנצנדנטי** הוא מספר ממשי $a\in\mathbb{R}$ שאינו שורש של אף פולינום במקדמים רציונליים, כלומר לכל $p(x)\in\mathbb{Q}[x]$ מתקיים $p(a)\neq 0$.

משפט 4.22 (קנטור) קיימים אינסוף מספרים טרצנדנטיים.

הוכחה: לפולינום ממעלה n מעל $\mathbb{Q}$ קיימים לכל היותר n שורשים (ניתן להוכיח טענה זו באינדוקציה על מעלת הפולינום תוך הסתמכות על כך שאם a שורש של פולינום אז $x-a$ מחלק את הפולינום). כמו כן, כל פולינום ממעלה n במקדמים רציונליים נקבע על ידי סדרה מאורך $n+1$ של מספרים רציונליים. מכאן שיש רק מספר בן מניה של שורשים של פולינומים ממעלה $n+1$. מכיוון שאיחוד בן מניה של קבוצות בנות מניה הוא בן מניה, הרי שקבוצת כל השורשים של פולינומים מעל $\mathbb{Q}$ היא בת מניה, ולכן קיימים אינסוף ($2^{\aleph_0}$) מספרים ממשיים שאינם שורשים של אף פולינום במקדמים רציונליים. ■

טבעי למדי להניח שהעוצמה של $\mathbb{R}$ היא העוצמה "הבאה בתור" אחרי עוצמת $\mathbb{Q}$, שהרי ככלות הכל קבוצות אלו דומות מאוד באופיין ו־$\mathbb{R}$ נבנה מתוך $\mathbb{Q}$ בצורה טבעית. העובדה ש־$|\mathbb{R}|=2^{\aleph_0}$ רק מחזקת תחושה זו, שכן משפט קנטור הראה שבאופן כללי, עבור קבוצה A, העוצמה הבאה בגודלה אחרי $|A|$ שקל למצוא היא $2^{|A|}$. אינטואיציה זו הובילה את קנטור להשערה הבאה:

השערה: (השערת הרצף) לא קיימת קבוצה $A\subseteq\mathbb{R}$ כך ש־$\aleph_0<|A|<2^{\aleph_0}$. השערה זו (והכללתה: לכל A אינסופית לא קיימת B כך ש־$|A|<|B|<2^{|A|}$) הייתה בעיה פתוחה מרכזית במתמטיקה של סוף המאה ה־19 ותחילת המאה ה־20. לא עלה בידי קנטור לפתור אותה, והיא ניצבה במקום הראשון ברשימת 23 הבעיות שהציג דויד הילברט בהרצאתו בקונגרס המתמטי של 1900. רק בשנות ה־60 של המאה ה־20, כתוצאה מעבודות בלתי תלויות של קורט גדל ופול כהן, הוכח כי השערה זו **אינה תלויה באקסיומות של תורת הקבוצות** (מערכת האקסיומות ZFC, שאיננו מתארים כאן במפורש), בדומה לאופן שבו אקסיומת המקבילים לא הייתה תלויה בשאר אקסיומות הגאומטריה.

לסיום, נשלים חוב שהותרנו קודם: משפט קנטור־שרדר־ברנשטיין.

משפט 4.23 (קנטור־שרדר־ברנשטיין) אם $|B|\leq|A|$ וגם $|A|\leq|B|$ אז $|A|=|B|$.

הוכחה: נניח כי קיימות פונקציות חח"ע $f:A\to B$ ו־$g:B\to A$ ונבנה פונקציה $h:A\to B$ שהיא חח"ע ועל באופן הבא:

ראשית נגדיר $D_0=A\backslash g(B)$, ובאופן אינדוקטיבי $D_{n+1}=g(f(D_n))$.

כעת נגדיר $D=\bigcup_{n=0}^{\infty}D_n$, וכעת נגדיר את h:

$$h(a)=\begin{cases}f(a) & a\in D\\ g^{-1}(a) & a\in A\backslash D\end{cases}$$

h בבירור מוגדרת לכל A.

נראה כי h על B: יהא $b\in B$. אם $g(b)=a\in A\backslash D$, אז $h(a)=g^{-1}(a)=b$ וסיימנו.

נניח אם כן כי $g(b)\in D$, כלומר $g(b)\in D_n$ עבור n כלשהו. לא ייתכן ש־$n=0$ כי $D_0=A\backslash g(B)$; לכן $n\geq 1$.

כעת, מכיוון ש־$g(b)\in D_n=g(f(D_n))$ אז $g(b)=g(b')$ עבור $b'\in f(D_n)$, ומכיוון ש־g חח"ע $b=b'$, כלומר $b\in f(D_n)$ ובפרט יש $a\in D_n\subseteq D$ כך ש־$f(a)=b$, כלומר $h(a)=b$.

נראה כעת כי h חח"ע. עבור $a_1,a_2\in D$ ברור כי $h(a_1)=h(a_2)$ גוררת $a_1=a_2$ כי f חח"ע. בדומה, אם $a_1,a_2\in A\backslash D$ אז $h(a_1)=h(a_2)$ גורר ש־$g^{-1}(a_1)=g^{-1}(a_2)$ ובגלל ש־g פונקציה, $a_1=a_2$.

נותר לטפל במקרה בו (ללא הגבלת הכלליות) $a_1\in D$ ו־$a_2\in A\backslash D$, ומתקיים $h(a_1)=h(a_2)$, כלומר $f(a_1)=g^{-1}(a_2)$. על ידי הפעלת g על שני האגפים נקבל ש־$a_2=g(f(a_1))$; מכיוון ש־$a_1\in D$ אז $a_1\in D_n$ עבור n כלשהו ולכן $a_2\in g(f(D_n))=D_{n+1}\subseteq D$, בסתירה לכך ש־$a_2\in A\backslash D$. ■

5 תחשיב הפסוקים

5.1 התחביר של תחשיב הפסוקים

נשתמש במילים "נוסחה" ו"פסוק" כדי לתאר את אותו הדבר (בהמשך, כאשר נעסוק בתחשיב היחסים, יהיה הבדל בין נוסחאות ופסוקים).

כל נוסחה בתחשיב הפסוקים היא סדרה סופית של אותיות שנלקחות מתוך הקבוצה הבאה:

$$\{\wedge,\vee,\neg,\rightarrow,\mathbf{T},\mathbf{F},(,)\}\cup\{p_i|i\in\mathbb{N}\}$$

אברי הקבוצה השמאלית הם **סימנים לוגיים**, בעוד שאינסוף אברי הקבוצה הימנית הם **משתנים**. הסימנים $\vee,\wedge,\neg,\rightarrow$ נקראים **קשרים לוגיים**.

למרות שכל סדרה סופית של אותיות נחשבת לנוסחה, לא לכולן ניתן לייחס משמעות. למשל, לא ברור כיצד להתייחס לנוסחה כמו $p_5 \rightarrow\rightarrow \mathbf{FFF} \vee\vee$. על כן, אנו מגדירים תת־קבוצה של נוסחאות, **הנוסחאות הבנויות היטב** (Well-formed formulas) שתסומן WFF ותוגדר באינדוקציה:

הגדרה 5.1 נגדיר בסיס ופונקציות סגור:
בסיס: $B = \{\mathbf{T}, \mathbf{F}\} \cup \{p_i | i \in \mathbb{N}\}$ (הסימנים המודגשים עבור T, F מיועדים למנוע בלבול עם השימושים האחרים שלנו באותיות אלו). אברי הבסיס מכונים **פסוקים אטומיים**.
סגור: $F = \{F_\vee, F_\wedge, F_\rightarrow, F_\neg\}$, כאשר הפונקציות הללו מוגדרות לכל זוג נוסחאות α, β באופן הבא:

- $F_\vee(\alpha, \beta) = (\alpha \vee \beta)$
- $F_\wedge(\alpha, \beta) = (\alpha \wedge \beta)$
- $F_\rightarrow(\alpha, \beta) = (\alpha \rightarrow \beta)$
- $F_\neg(\alpha) = \neg\alpha$

וכעת נגדיר $\text{WFF} \triangleq X_{B,F}$

שימו לב: הסוגריים באגף ימין הן **חלק מהנוסחה**, בעוד שהסוגריים באגף שמאל הן מה שמקיף את הפרמטרים של הפונקציות F השונות.
כעת נגדיר $\text{WFF} \triangleq X_{B,F}$.
נתבונן במספר דוגמאות לנוסחאות בנויות היטב ושאינן בנויות היטב:

- p_1 היא נוסחה בנויה היטב ודוגמה לפסוק אטומי.
- $\mathbf{F}$ היא נוסחה בנויה היטב, וגם היא דוגמה לפסוק אטומי.
- (p_3) אינה נוסחה בנויה היטב.
- $(\neg\mathbf{T} \vee p_5)$ היא נוסחה בנויה היטב.

בפועל נכתוב לרוב נוסחאות תוך השמטת זוגות סוגריים לא חיוניים. למשל, במקום לכתוב $((p_1 \vee p_2) \vee p_3)$ נכתוב פשוט $p_1 \vee p_2 \vee p_3$. עם זאת, חשוב להדגיש כי זהו **קיצור לא פורמלי**, וכי $p_1 \vee p_2 \vee p_3$ איננה נוסחה חוקית ואיננה שייכת ל־WFF; אנו מניחים כי בהינתן נוסחה ממין זה ניתן להבין איך להוסיף לה סוגריים כדי שתתקבל נוסחה החוקית המתאימה ב־WFF (לפעמים יש יותר מנוסחה אפשרית אחת; במקרה זה חלק מההנחה שלנו היא שאין הבדל מהותי ביניהן).
כמו כן, בהמשך יהיה נוח לעתים לעבוד עם קבוצה מצומצמת יותר של נוסחאות (שכפי שנראה, אינה נופלת בכוח ההבעה שלה מכל WFF):

הגדרה 5.2 נגדיר $\text{WFF}_{\{\neg,\rightarrow\}} = X_{B,F}$ עבור הבסיס $B = \{p_i | i \in \mathbb{N}\}$ ופונקציות הסגור $F = \{F_\neg, F_\rightarrow\}$.

החשיבות של אופן הבניה של WFF, ובפרט של השימוש שלנו בסוגריים במהלכו, היא שלכל פסוק תהיה **קריאה יחידה**, כלומר תהיה דרך אחת בלבד לפרק אותו למרכיבים; הדבר יהיה קריטי כאשר נגדיר את **ערך האמת** של פסוק, שכן שני אופני קריאה שונים אפשריים לאותו פסוק עשויים לגרום לכך שיהיו לו שני ערכי אמת שונים.

משפט 5.3 (משפט הקריאה היחידה) בהינתן $\varphi \in \text{WFF}$, מתקיים בדיוק אחד משלושת הבאים:

1. φ הוא פסוק אטומי, כלומר φ היא משתנה או T או F.
2. $\varphi = \neg\alpha$ כאשר $\alpha \in \text{WFF}$.
3. $\varphi = (\alpha \odot \beta)$ כאשר $\odot \in \{\vee, \wedge, \rightarrow\}$ ו־$\alpha, \beta \in \text{WFF}$.

יתר על כן, אם φ הוא מהצורה $(\alpha \odot \beta)$ אז α, β הם **יחידים**, כלומר לא קיימים $\gamma, \delta \in \text{WFF}$ כך ש־$\gamma \neq \alpha$, $\delta \neq \beta$ ו־$\varphi = (\gamma \odot \delta)$.

על מנת להוכיח את המשפט נזדקק לכמה אבחנות בסיסיות על המבנה של פסוקים ־ בפרט, על מבנה סדרות הסוגריים שלהם. לצורך כך נזדקק להגדרה:

הגדרה 5.4 לכל סדרה, $a_0, a_1, \ldots, a_n$, **רישא** של הסדרה היא תת־סדרה הכוללת את כל האיברים מתחילת הסדרה ועד מקום כלשהו בה, $a_0, a_1, \ldots, a_k$; **וסיפא** של הסדרה היא תת־סדרה הכוללת את כל האיברים ממקום כלשהו בסדרה ועד סופה, $a_k, a_{k+1}, \ldots, a_n$ (כאן k אינו קבוע אלא יכול להיות כל אינדקס של איבר בסדרה).

כזכור, פסוקים הם סדרות של תווים ולכן ניתן לדבר על רישא וסיפא של פסוק. הרישות של הפסוק $(\alpha \vee \beta)$ הן המחרוזות $(\alpha \vee \beta)$, $(\alpha \vee \beta$, $(\alpha \vee$, $(\alpha$, $($ (וגם המחרוזת הריקה).

נזדקק גם לסימון הבא:

הגדרה 5.5 בהינתן פסוק α, $\#_([\alpha]$ הוא מספר המופעים של סוגר שמאלי ב־α, ו־$\#_) [\alpha]$ הוא מספר המופעים של סוגר ימני ב־α.

טענה 5.6 יהי $\alpha \in \mathrm{WFF}$ כלשהו.

1. $\#_([\alpha] = \#_) [\alpha]$ (α הוא **מאוזן סוגריים**)
2. לכל רישא β של α מתקיים $\#_([\beta] \geq \#_) [\beta]$ ולכל סיפא γ של α מתקיים $\#_([\gamma] \leq \#_) [\gamma]$
3. לכל פירוק $\alpha = \beta \odot \gamma$ כך ש־$\odot \in \{\vee, \wedge, \rightarrow\}$ מתקיים ש־$\#_([\beta] > \#_) [\beta]$ ו־$\#_([\gamma] < \#_) [\gamma]$.

הוכחה: נוכיח באינדוקציית מבנה על WFF. ברור כי כל פסוק אטומי מקיים את תכונות 1 ו־2 שכן הוא אינו כולל סוגריים כלל (ולכן $\#_([\alpha] = \#_) [\alpha] = 0$ עבורו ועבור כל רישא או סיפא שלו) ומכיוון שלא קיים לפסוק אטומי פירוק מהצורה $\beta \odot \gamma$ תכונה 3 מתקיימת עבורו באופן ריק.

נוכיח כעת שאם $\alpha \in \mathrm{WFF}$ מקיים את תנאי המשפט, כך גם $F_\neg [\alpha] = \neg\alpha$.

נשים לב לכך ש־$\neg\alpha$ זהה ל־α פרט להוספת תו שאינו סוגריים לפי α, ולכן מתקיים $\#_([\neg\alpha] = \#_([\alpha] = \#_) [\alpha] = \#_) [\neg\alpha]$.

בדומה, כל רישא לא ריקה של $\neg\alpha$ היא מהצורה $\neg\beta$ כאשר β היא רישא של α, וכל סיפא של $\neg\alpha$ שאיננה כל $\neg\alpha$ היא מהצורה β כאשר β היא סיפא של α ולכן תכונה 2 גם היא מתקיימת (לא נכתוב במפורש את השוויונות).

בדומה, כל פירוק של $\neg\alpha$ על ידי קשר $\odot$ הוא מהצורה $\neg\alpha = \neg\beta \odot \gamma$, כאשר $\alpha = \beta \odot \gamma$, ולכן גם תכונה 3 מתקיימת עבור $\neg\alpha$.

נוכיח לסיום כי אם $\alpha, \beta \in \mathrm{WFF}$ ומקיימים את תנאי המשפט, כך גם $F_\odot (\alpha, \beta) = (\alpha \odot \beta)$.

ראשית נשים לב לכך ש־$\#_([(\alpha \odot \beta)] = 1 + \#_([\alpha] + \#_([\beta] = 1 + \#_) [\alpha] + \#_) [\beta] = \#_) [(\alpha \odot \beta)]$ ולכן תכונה 1 מתקיימת.

כעת, כל רישא ממש של $(\alpha \odot \beta)$ היא מהצורה $(\gamma$ כאשר γ היא רישא של $\alpha \odot \beta$. נפריד בין שני מקרים:

אם γ היא רישא של α, אז על פי הנחת האינדוקציה נקבל ש־

$$\#_([(\gamma] \quad = \quad 1 + \#_([\gamma] \geq 1 + \#_) [\gamma] = 1 + \#_) [(\gamma] \geq \#_) [(\gamma]$$

.

אם γ כוללת את כל $\alpha\odot$, אז היא מהצורה $\alpha \odot \delta$ כאשר δ היא רישא של β, ולכן על פי הנחת האינדוקציה נקבל:

$$\#_([(\gamma] \quad = \quad \#_([(\alpha \odot \delta] = 1 + \#_([\alpha] + \#_([\delta] \geq 1 + \#_) [\alpha] + \#_) [\delta] = 1 + \#_) [(\alpha \odot \delta] \geq \#_) [(\gamma]$$

באותו האופן מוכיחים את תכונה 2 גם עבור הסיפא (שימו לב לסימטריה בין המקרים שיש כאן).

נותר להוכיח את תכונה 3. נתבונן אם כן בפירוק של $(\alpha \odot \beta)$: $(\alpha \odot \beta) = x \odot y$. כאן צריך להבדיל בין שלושה מקרים:

אם $x = (\alpha$ ו־$y = \beta)$ אז מתכונה 1 נקבל ש־

$$\#_([x] \quad = \quad \#_([(\alpha] = 1 + \#_([\alpha] = 1 + \#_) [\alpha] > \#_) [\alpha] = \#_) [(\alpha] = \#_) [x]$$

ובאופן דומה גם נקבל ש־$\#_((y) > \#_) (y)$.

במקרה השני, $x\odot$ הוא רישא של α). נכתוב $x = (\alpha'$ ונקבל:

$$\#_{(}[x] \;=\; 1+\#_{(}[\alpha'] \geq 1+\#_{)}[\alpha'] > \#_{)}[\alpha'] = \#_{)}[(\alpha'] = \#_{)}[x]$$

במקרה זה, $y = \alpha' \odot \beta)$ כאשר α' היא סיפא של α. כעת נקבל:

$$\#_{)}[y] \;=\; \#_{)}[\alpha' \odot \beta)] = \#_{)}[\alpha'] + \#_{)}[\beta] + 1 \geq \#_{(}[\alpha'] + \#_{(}[\beta] + 1 > \#_{(}[\alpha'] + \#_{(}[\beta] = \#_{(}[\alpha' \odot \beta)] = \#_{(}[y]$$

באותו האופן מטפלים גם במקרה השלישי. ■

בעזרת טענות עזר אלו נוכל כעת להוכיח את משפט הקריאה היחידה:

הוכחה: (למשפט הקריאה היחידה) יהי $\varphi \in \mathrm{WFF}$ כלשהו. ראשית נשים לב לכך שלא ייתכן ש־φ ישתייך ליותר מאחד מסוגי הפסוקים שבמשפט הקריאה היחידה: זאת מכיוון שכל סוג של פסוק מתחיל בתו אחר (פסוק אטומי מתחיל במשתנה או ב־$\mathbf{F}$ או ב־$\mathbf{T}$; $\neg\alpha$ מתחיל ב־$\neg$; ו־$(\alpha \odot \beta)$ מתחיל ב־().

ההוכחה לכך שכל $\varphi \in \mathrm{WFF}$ שייך לאחד משלושת הסוגים היא באינדוקציית מבנה קלה על WFF: כל איבר בסיס שייך לסוג הראשון; כל פלט של $F_\neg$ שייך לסוג השני; וכל פלט של $F_\odot$ שייך לסוג השלישי.

נותר להראות את יחידות הפירוק ביחס לקשר $\odot$. ראשית נשים לב לכך שמכיוון ש־$\alpha \in \mathrm{WFF}$, אז $\#_{(}[\alpha] = \#_{)}[\alpha]$.

יהא כעת $(\gamma \odot \delta)$ פירוק אחר של φ, כלומר $\gamma \neq \alpha$. נבדיל בין שני מקרים אפשריים:

אם γ הוא רישא ממש של α, אז קיים ל־α הפירוק $\alpha = \gamma \odot \gamma'$. מכיוון ש־$\alpha \in \mathrm{WFF}$, סעיף 3 בטענה 5.6 מראה ש־$\#_{(}[\gamma] > \#_{)}[\gamma]$ ולכן בפרט $\gamma \notin \mathrm{WFF}$ (אחרת היינו מקבלים סתירה לסעיף 1 של 5.6).

אם γ אינו רישא ממש של α אז δ הוא סיפא ממש של β. מכיוון ש־$\beta \in \mathrm{WFF}$, סעיף 3 בטענה 5.6 מראה ש־$\#_{)}[\delta] > \#_{(}[\delta]$ ולכן בפרט $\delta \notin \mathrm{WFF}$. ■

נשים לב שההוכחה גם מצביעה לנו על האופן ה"נכון" שבו יש לפרק פסוק φ שמתחיל בסוגריים: יש למצוא את הקשר $\odot$ היחיד כך ש־$\varphi = (\alpha \odot \beta)$ ו־α, β שניהם מאוזני סוגריים (בפועל די לסרוק את φ מתחילתו, מבלי לספור את הסוגר הפותח, ולסמן את $\odot$ שבא מייד לאחר שמספר הסוגריים הימניים משתווה לראשונה למספר הסוגריים השמאליים שנקראו).

5.2 הסמנטיקה של תחשיב הפסוקים

סמנטיקה היא ה**משמעות** שאנו מייחסים לפסוקים. בתחשיב הפסוקים, המשתנים מקבלים ערכי "אמת" או "שקר", המסומנים ב־$\mathbf{T}, \mathbf{F}$, ובהתאם לערכים שהמשתנים קיבלו גם הפסוקים עצמם מקבלים ערכי "אמת" או "שקר".

הגדרה 5.7 השמה למשתנים היא פונקציה $Z : \{p_i | i \in \mathbb{N}\} \to \{\mathbf{T}, \mathbf{F}\}$. הערכים בטווח של Z נקראים **ערכי אמת** (שימו לב - גם $\mathbf{T}$ וגם $\mathbf{F}$ נקראים שניהם "ערכי אמת").

משהגדרנו השמה למשתנים, נרצה להרחיב אותה לפונקציה $\overline{Z}$ שלכל פסוק מחזירה את ערך האמת שהוא "מחשב". לצורך כך ראשית כל יש להבין את האופן שבו הקשרים הלוגיים מחשבים ערכי אמת מתוך ערכי האמת ש"מוצבים" בהם.

על כל קשר לוגי ניתן לחשוב בתור פונקציה במשתנה אחד או יותר המקבלת ערכי אמת ומחזירה ערך אמת. את הפונקציה ניתן לתאר במפורש בעזרת **טבלת אמת**: טבלה שבה כל שורה מתארת במפורש את הקלטים והפלט של הקשר.

טבלאות האמת של האופרטורים הבינאריים המוכרים לנו הן:

X	Y	$X \vee Y$	$X \wedge Y$	$X \to Y$
$\mathbf{F}$	$\mathbf{F}$	$\mathbf{F}$	$\mathbf{F}$	$\mathbf{T}$
$\mathbf{T}$	$\mathbf{F}$	$\mathbf{T}$	$\mathbf{F}$	$\mathbf{F}$
$\mathbf{F}$	$\mathbf{T}$	$\mathbf{T}$	$\mathbf{F}$	$\mathbf{T}$
$\mathbf{T}$	$\mathbf{T}$	$\mathbf{T}$	$\mathbf{T}$	$\mathbf{T}$

עבור הקשר $\neg$ טבלת האמת פשוטה במיוחד שכן זהו קשר אונרי:

X	$\neg X$
$\mathbf{F}$	$\mathbf{T}$
$\mathbf{T}$	$\mathbf{F}$

ניתן להגדיר גם טבלאות אמת עבור קשרים על שלושה או יותר משתנים, אך בפועל אין בכך תועלת רבה.

נשים לב כי טבלת האמת של קשר בינארי היא בעלת 4 שורות (שכן יש 2^2 הצבות אפשריות לזוג המשתנים של האופרטור). מכיוון שכל בחירה של ערכי אמת עבור 4 שורות אלו מניבה קשר לוגי אחר, קיימים $2^4 = 16$ קשרים לוגיים בינאריים בסך הכל.

הגדרה 5.8 בהינתן $Z : \{p_i | i \in \mathbb{N}\} \to \{\mathbf{T}, \mathbf{F}\}$, הפונקציה $\overline{Z} : \mathrm{WFF} \to \{\mathbf{T}, \mathbf{F}\}$ מוגדרת באופן הרקורסיבי הבא:

1. אם $\varphi = \mathbf{T}$ אז $\overline{Z}(\varphi) = \mathbf{T}$ ואם $\varphi = \mathbf{F}$ אז $\overline{Z}(\varphi) = \mathbf{F}$.
2. אם $\varphi = p_i$ אז $\overline{Z}(\varphi) = Z(p_i)$.
3. אם $\varphi = \neg\alpha$ $\overline{Z}(\varphi) = \neg\overline{Z}(\alpha)$.
4. אם $\varphi = (\alpha \odot \beta)$ $\overline{Z}(\varphi) = \overline{Z}(\alpha) \odot \overline{Z}(\beta)$.

טענה 5.9 לכל $Z : \{p_i | i \in \mathbb{N}\} \to \{\mathbf{T}, \mathbf{F}\}$ הפונקציה $\overline{Z} : \mathrm{WFF} \to \{\mathbf{T}, \mathbf{F}\}$ מוגדרת היטב.

הוכחה: ההוכחה היא באינדוקציית מבנה על WFF. עבור פסוק אטומי ברור ש־$\overline{Z}$ מוגדרת היטב (כלומר, מקבלת ערך וערך זה הוא יחיד). גם עבור $\varphi = \neg\alpha$ ברור כי $\overline{Z}(\varphi) = \neg\overline{Z}(\alpha)$ מגדיר ערך יחיד (שכן $\overline{Z}(\alpha)$ קיים ויחיד). עבור $\varphi = (\alpha \odot \beta)$ הערך $\overline{Z}(\varphi) = \overline{Z}(\alpha) \odot \overline{Z}(\beta)$ מוגדר, אך לא מובן מאליו שהוא יחיד; עם זאת, ממשפט הקריאה היחידה עולה שהפירוק $\varphi = (\alpha \odot \beta)$ הוא יחיד ולכן $\overline{Z}(\varphi)$ היא חד ערכית גם במקרה זה. ■

5.3 מערכות שלמות של קשרים

כפי שראינו, כל השמה של ערכי אמת למשתנים מניבה ערך אמת עבור הפסוק המכיל אותם. ניתן אם כן לחשוב על כל פסוק φ כעל **פונקציה** במספר משתנים לוגיים, כפי שעשינו עם האופרטורים הלוגיים שלנו. ההבדל הוא שערך האמת של הפסוק נקבע על בסיס העץ שמייצג אותו, ולא על פי טבלת אמת. השאלה הטבעית שנשאלת היא האם לכל פונקציה על מספר סופי כלשהו של משתנים לוגיים קיים פסוק שמממש אותה. הדבר תלוי בקשרים שמהם הפסוק יכול להיות בנוי.

הגדרה 5.10 קבוצה X של קשרים לוגיים היא **שלמה** אם לכל פונקציה $f : \{\mathbf{T}, \mathbf{F}\}^n \to \{\mathbf{T}, \mathbf{F}\}$ (לכל $n \geq 1$) קיים פסוק $\varphi \in \mathrm{WFF}$ המורכב מהקשרים ב־X כך ש־$\overline{Z}(\varphi) = f(Z(p_1), \ldots, Z(p_n))$ לכל השמה Z.

אין זה מובן מאליו שמערכת קשרים **סופית** שלמה קיימת בכלל, מכיוון שהקשרים שנמצאים במערכת סופית מטפלים רק במספר סופי של משתנים בו זמנית (בפרט, שני משתנים במקרה של קשרים בינאריים) בעוד שהפונקציה f תלויה בכל n המשתנים "בבת אחת". עם זאת, קיימת מערכת קשרים קטנה שקל להראות כי היא שלמה:

משפט 5.11 מערכת הקשרים $\{\neg, \vee, \wedge\}$ היא שלמה.

הוכחה: נראה כיצד ניתן לרשום פסוק φ הנמצא בצורה קנונית הנקראת DNF עבור פונקציה $f : \{\mathbf{T}, \mathbf{F}\}^n \to \{\mathbf{T}, \mathbf{F}\}$ שרירותית שמחזירה ערך $\mathbf{T}$ לקלט אחד לפחות.

תהא $V = (V_1, V_2, \ldots, V_n)$ סדרה של ערכי אמת ($V_i \in \{\mathbf{T}, \mathbf{F}\}$) כך ש־$f(V_1, \ldots, V_n) = \mathbf{T}$. נגדיר תת־פסוק $\varphi_V = (l_1 \wedge \cdots \wedge l_n)$ באופן הבא: $l_i = \begin{cases} p_i & V_i = \mathbf{T} \\ \neg p_i & V_i = \mathbf{F} \end{cases}$

כעת נגדיר $\varphi = \bigvee \varphi_V$ כאשר ה־$\bigvee$ נלקח על כל הסדרות V שמתאימות לשורות $\mathbf{T}$ בטבלת האמת של f.

נותר לטפל במקרה שבו f היא הפונקציה שמחזירה $\mathbf{F}$ לכל קלט. הפסוק $\varphi = p_1 \wedge (\neg p_1)$ מתאים לפונקציה זו. נשים לב שפסוק זה אינו בצורת DNF; לא ניתן לייצג את הפונקציה שמחזירה $\mathbf{F}$ לכל קלט באמצעות DNF. ■

משידוע לנו על מערכת קשרים שלמה אחת, ניתן להוכיח באמצעותה שלמות של מערכות קשרים אחרות; כל שנדרש הוא להראות כיצד ניתן להחליף קשר של מערכת אחרת בפסוק המורכב מקשרי המערכת האחרת.

טענה 5.12 מערכת הקשרים $\{\neg, \to\}$ היא שלמה.

הוכחה: יש להראות כי ניתן להחליף את $\vee$ ו־$\wedge$ בפסוקים המורכבים מ־$\neg, \to$.
את $X \vee Y$ ניתן להחליף ב־$\neg X \to Y$.
את $X \wedge Y$ ניתן להחליף ב־$\neg(X \to \neg Y)$.
הצבה ישירה של כל הערכים מראה כי פסוקים אלו אכן מתאימים לקשרים שהם באים להחליף. ■

קיימת גם מערכת קשרים המכילה קשר בינארי יחיד:

טענה 5.13 נגדיר את הקשר הבינארי $\uparrow$ (NAND, כלומר Not-And) בתור $X \uparrow Y = \neg(X \wedge Y)$. אז $\{\uparrow\}$ היא מערכת קשרים שלמה.

הוכחה: די להראות כיצד ניתן לקבל את $\neg$ ואת $\to$ מתוך $\uparrow$.
את $\neg X$ ניתן להחליף ב־$X \uparrow X$.
את $X \to Y$ ניתן להחליף ב־$X \uparrow (Y \uparrow Y)$.
בדיקה ישירה מראה כי פסוקים אלו אכן מתאימים לקשרים שהם באים להחליף.
(פורמלית $\uparrow$ כלל אינו קשר חוקי ב־WFF, אך ניתן להוסיף את $F_\uparrow$ לקבוצת פונקציות היצירה של WFF מבלי לשנות דבר באופן מהותי). ■

טענה 5.14 מערכת הקשרים $\{\mathbf{F}, \to\}$ היא שלמה (אנו חושבים על $\mathbf{F}$ כקשר "אפס־מקומי" שפשוט מחזיר $\mathbf{F}$ בלי תלות בקלט).

הוכחה: די להראות כיצד ניתן לקבל את $\neg$ מתוך $\mathbf{F}, \to$.
את $\neg X$ ניתן להחליף ב־$X \to \mathbf{F}$.
בדיקה ישירה מראה כי פסוק זה אכן מתאים לקשר שהוא בא להחליף. ■

5.4 סמנטיקה ־ נביעה לוגית

נפתח בהגדרה:

הגדרה 5.15 פסוק φ הוא **טאוטולוגיה** אם לכל השמה Z מתקיים $\overline{Z}(\varphi) = \mathbf{T}$. אם φ הוא טאוטולוגיה נהוג לסמן זאת $\models \varphi$.

כלומר, טאוטולוגיה היא פסוק שנכון תמיד, ללא תלות בערכי האמת שמקבלים משתניו.
נראה מספר דוגמאות, גם כדי לתרגל את האופן שבו ניתן להראות שפסוקים הם טאוטולוגיות וגם כי הטאוטולוגיות הללו יסייעו לנו בהמשך.

טענה 5.16 הפסוקים הבאים הם טאוטולוגיות:

1. $X \vee \neg X$.
2. $X \to (Y \to X)$
3. $(X \to (Y \to W)) \to ((X \to Y) \to (X \to W))$
4. $(\neg X \to \neg Y) \to (Y \to X)$.

הוכחה: את 1 ניתן לראות בקלות על ידי בחינת כל ההשמות האפשריות. אמנם, על פי הגדרתנו להשמה יש אינסוף השמות אפשריות, אבל יש רק שני ערכים שונים שהן יכולות לתת למשתנה X ולכן די לבדוק את הצמצום של ההשמות על המשתנה X. קל לראות שבין אם מציבים $\mathbf{T}$ ובין אם מציבים $\mathbf{F}$ הפסוק מקבל את הערך $\mathbf{T}$.
באופן דומה ניתן לבדוק את 4, ובאופן דומה ניתן לבדוק גם את 2, רק שכעת יש לבדוק 4 השמות שונות.
מכיוון ש־3 מערב שלושה משתנים שונים, ננקוט בגישה קצת פחות מתישה. הפסוק הוא מהצורה $\alpha \to \beta$, ולכן האופן היחיד שבו הוא עשוי לקבל ערך $\mathbf{F}$ הוא כאשר α מקבל ערך $\mathbf{T}$ ו־β מקבל ערך $\mathbf{F}$.
כדי ש־β יקבל ערך $\mathbf{F}$, בהכרח $X \to Y$ צריך לקבל ערך $\mathbf{T}$ ו־$X \to W$ צריך לקבל ערך $\mathbf{F}$. אם X מקבל ערך $\mathbf{F}$ זה לא יקרה, כי $X \to W$ יקבל את הערך $\mathbf{T}$. מכאן שבהכרח $Z(X) = \mathbf{T}$, ו
כעת נציב את הערכים הללו ב־$\alpha = X \to (Y \to W)$. נקבל $\mathbf{T} \to (\mathbf{T} \to \mathbf{F}) = \mathbf{F}$, כלומר α לא קיבל ערך $\mathbf{T}$ ולכן הפסוק כולו כן קיבל ערך $\mathbf{T}$. ■

המושג הדואלי לטאוטולוגיה הוא סתירה:

הגדרה 5.17 פסוק φ הוא **סתירה** אם לכל השמה Z מתקיים $\overline{Z}(\varphi)=\mathbf{F}$

קיימים כמובן פסוקים שאינם סתירות ואינם טאוטולוגיות, למשל $\varphi = X \vee Y$. מה שברור הוא ש־φ הוא טאוטולוגיה אם ורק אם $\neg\varphi$ הוא סתירה, ובאופן דומה φ הוא סתירה אם ורק אם $\neg\varphi$ הוא טאוטולוגיה.

הגדרה 5.18 פסוק φ שאיננו סתירה נקרא **ספיק**. על השמה שנותנת ערך $\mathbf{T}$ לפסוק φ אומרים שהיא **מספקת** את φ. קבוצת פסוקים Φ היא **ספיקה** אם קיימת השמה שמספקת את כל הפסוקים ב־Φ. להשמה Z שמספקת את Φ קוראים גם **מודל** ל־Φ ומסמנים זאת $Z \models \Phi$.

כלומר, פסוק ספיק הוא פסוק שקיימת לפחות השמה אחת למשתניו שמחזירה ערך $\mathbf{T}$. כל טאוטולוגיה היא ספיקה, אך קיימים פסוקים ספיקים שאינם טאוטולוגיות.

הגדרה 5.19 תהא Φ קבוצה (לא בהכרח סופית) של פסוקים. נאמר שפסוק φ **נובע לוגית** מ־Φ ונסמן זאת $\Phi \models \varphi$ אם כל מודל של Φ הוא גם מודל של φ.

אם $\Phi=\emptyset$ הרי שכל השמה מספקת את Φ באופן ריק, ולכן $\emptyset \models \varphi$ אם ורק אם φ טאוטולוגיה. במקרה זה פשוט משמיטים את $\emptyset$, מה שמסביר את משמעות הסימון $\models \varphi$ לטאוטולוגיות.

אם ψ היא סתירה, אז $\psi \models \varphi$ לכל φ (אפילו אם φ היא עצמה סתירה). אינטואיטיבית, פירוש הדבר הוא ש"מסתירה נובע כל דבר".

טענה 5.20 ("דדוקציה סמנטית") אם Φ היא קבוצת פסוקים ו־α, β הם פסוקים כלשהם, אז $\Phi \cup \{\alpha\} \models \beta$ אם ורק אם $\Phi \models \alpha \to \beta$.

הוכחה: נניח ש־$\Phi \cup \{\alpha\} \models \beta$. עלינו להראות שאם השמה Z מספקת את Φ אז היא מספקת את $\alpha \to \beta$. תהא Z השמה שמספקת את Φ. נניח בשלילה כי $\overline{Z}(\alpha \to \beta)=\mathbf{F}$, אז על פי הגדרה $\overline{Z}(\alpha)=\mathbf{T}$ ו־$\overline{Z}(\beta)=\mathbf{F}$ ובפרט Z מספקת את $\Phi \cup \{\alpha\}$. מצד שני, מכיוון ש־$\Phi \cup \{\alpha\} \models \beta$ הרי ש־$\overline{Z}(\beta)=\mathbf{T}$ - סתירה. על כן לכל השמה Z המקיימת $Z \models \Phi$ מתקיים $Z \models \alpha \to \beta$ ומכאן ש־$\Phi \models \alpha \to \beta$.

בכיוון השני, אם $\Phi \models \alpha \to \beta$, תהא Z השמה כלשהי שמספקת את Φ כך ש־$\overline{Z}(\alpha)=\mathbf{T}$. מכיוון ש־$Z$ מספקת את Φ אז מ־$\Phi \models \alpha \to \beta$ נובע ש־$\overline{Z}(\alpha \to \beta)=\mathbf{T}$ ולכן $\overline{Z}(\beta)=\mathbf{T}$ בהכרח, אחרת היינו מקבלים $\overline{Z}(\alpha \to \beta)=\mathbf{F}$. מכאן ש־$\Phi \cup \{\alpha\} \models \beta$. ■

בפרט, כאשר $\Phi=\emptyset$ אנו מקבלים את המסקנה הבאה:

מסקנה 5.21 יהיו α, β פסוקים. אז $\alpha \models \beta$ אם ורק אם $\models \alpha \to \beta$.

טענה 5.22 ("סילוק הנחות מיותרות") אם $\Phi \models \alpha$ וגם $\Phi \cup \{\alpha\} \models \beta$ אז $\Phi \models \beta$.

הוכחה: יהא $Z \models \Phi$ מודל כלשהו ל־Φ. מכיוון ש־$\Phi \models \alpha$ הרי ש־$Z \models \alpha$ ולכן $Z \models \Phi \cup \{\alpha\}$ ומכיוון ש־$\Phi \cup \{\alpha\} \models \beta$ אז $Z \models \beta$. ■

הגדרה 5.23 שני פסוקים α, β הם **שקולים לוגית** אם $\alpha \models \beta$ וגם $\beta \models \alpha$, כלומר הם מקבלים את אותו ערך אמת בכל השמה. נסמן זאת לעתים בתור $\alpha \equiv \beta$.

קל לראות כי שקילות לוגית היא אכן יחס שקילות, ופשוט למדי להוכיח גם שאם Φ היא קבוצת פסוקים ו־Φ' היא אוסף נציגים של מחלקות השקילות של יחס השקילות הלוגית על Φ, אז $\Phi \models \varphi$ אם ורק אם $\Phi' \models \varphi$, כך שניתן לפשט את Φ תמיד על ידי שמירת נציג אחד מכל מחלקת שקילות. לא נרחיב על כך כעת.

נתרגל את מושג הנביעה הלוגית עם הוכחה של מספר טענות פשוטות:

טענה 5.24 (תכונות של נביעה לוגית) תהא Φ קבוצת פסוקים.

1. אם $\Phi_1 \subseteq \Phi_2$ ו־$\Phi_1 \models \alpha$ אז $\Phi_2 \models \alpha$ ("מונוטוניות").
2. אם $\Phi \cup \{\alpha\} \models \beta$ וגם $\Phi \cup \{\neg\alpha\} \models \beta$ אז $\Phi \models \beta$.
3. אם $\Phi \cup \{\neg\alpha\} \models \alpha$ אז $\Phi \models \alpha$.

4. אם $\Phi\cup\{\neg\alpha\}\models\beta$ וגם $\Phi\cup\{\neg\alpha\}\models\neg\beta$ אז $\Phi\models\alpha$ ("הוכחה בשלילה").

5. $\Phi\cup\{\alpha,\alpha\to\beta\}\models\beta$ ("מודוס פוננס").

הוכחה: עבור טענה 1, אם Z היא השמה אשר מספקת את Φ_2 אז היא מספקת בפרט כל נוסחה של Φ_2 ששייכת גם ל־Φ_1 ומכיוון ש־$\Phi_1\subseteq\Phi_2$, היא מספקת את כל Φ_1 ומכיוון ש־$\Phi_1\models\alpha$, היא מספקת את α ולכן $\Phi_2\models\alpha$, כנדרש.

עבור טענה 2, תהא Z השמה שמספקת את כל פסוקי Φ. נניח ש־$\overline{Z}(\alpha)=\mathbf{T}$, אז Z מספקת את $\Phi\cup\{\alpha\}$ ולכן חייבת לספק את β כי $\Phi\cup\{\alpha\}\models\beta$. אם לעומת זאת $\overline{Z}(\alpha)=\mathbf{F}$ אז Z מספקת את $\Phi\cup\{\neg\alpha\}$ ולכן מספקת את β. קיבלנו שלכל Z שמספקת את כל פסוקי Φ, Z מספקת את β ולכן $\Phi\models\beta$.

טענה 3 היא מקרה פרטי של טענה 2, מכיוון ש־$\Phi\cup\{\alpha\}\models\alpha$ בבירור מתקיים (כי $\alpha\models\alpha$ וניתן להפעיל על כך את טענה 1).

עבור טענה 4, תהא Z השמה שמספקת את כל פסוקי Φ. נניח בשלילה ש־$\overline{Z}(\alpha)=\mathbf{F}$, אז על פי הגדרה $\overline{Z}(\neg\alpha)=\mathbf{T}$. מכאן ש־$Z$ מספקת את $\Phi\cup\{\neg\alpha\}$ ולכן, מכיוון ש־$\Phi\cup\{\neg\alpha\}\models\beta$ אז Z מספקת את β; מצד שני, מכיוון ש־$\Phi\cup\{\neg\alpha\}\models\neg\beta$ אז Z מספקת גם את $\neg\beta$ והגענו לסתירה כי השמה אינה יכולה לספק בו זמנית את β ואת $\neg\beta$. מכאן ש־$\overline{Z}(\alpha)=\mathbf{T}$ ולכן $\Phi\models\alpha$.

בטענה 5 די להוכיח $\{\alpha,\alpha\to\beta\}\models\beta$ ולהשתמש בטענה 1. על פי טענה 5.20, $\{\alpha,\alpha\to\beta\}\models\beta$ אם ורק אם $\alpha\to\beta\models\alpha\to\beta$ והנכונות של כך מובנת מאליה.

5.5 צורות נורמליות

■

נפתח בהוכחה של מספר שקילויות לוגיות שניעזר בהן בהמשך:

טענה 5.25 יהיו $\alpha_1,\dots,\alpha_n$ ו־α פסוקים. מתקיימות השקילויות הלוגיות הבאות:

1. (שלילה כפולה) $\neg(\neg\alpha)\equiv\alpha$.
2. (כלל דה־מורגן) $\neg\left(\bigvee_{i=1}^{n}\alpha_i\right)\equiv\bigwedge_{i=1}^{n}(\neg\alpha_i)$.
3. (כלל דה־מורגן) $\neg\left(\bigwedge_{i=1}^{n}\alpha_i\right)\equiv\bigvee_{i=1}^{n}(\neg\alpha_i)$.

הוכחה: נכונות כל הטענות נובעת מיידית מבדיקת טבלת האמת שלהן (את כללי דה־מורגן ניתן להוכיח באינדוקציה). ■

כשימוש ראשון לכללים אלו, נוכיח כי כל לכל פסוק קיים פסוק שקול שבו כל השלילות סמוכות למשתנים עצמם:

הגדרה 5.26 פסוקים בצורת NNF (Negation normal form) הם פסוקי WFF המוגדרים על ידי קבוצת הבסיס $B=\{p_i|i\in\mathbb{N}\}\cup\{\neg p_i|i\in\mathbb{N}\}\cup\{\mathbf{T},\mathbf{F}\}$ ופעולות הסגור $F=\{F_\vee,F_\wedge\}$.

לכל פסוק $\varphi\in\mathrm{WFF}$ ניתן לעבור לפסוק שקול φ' בצורת NNF באופן הבא: כל מופע של $(\alpha\to\beta)$ מוחלף ב־$(\neg\alpha\vee\beta)$; לאחר מכן כללי דה־מורגן (שקילויות 2 ו־3) מופעלים על הפסוק עד שכל השלילות צמודות למשתנים; ולבסוף מוסרות שלילות כפולות על פי שקילות 1.

מקרה פרטי של NNF שכבר ראינו הוא נוסחה בצורת DNF. כבר ראינו קודם כי לכל פונקציה $f:\{\mathbf{T},\mathbf{F}\}^n\to\{\mathbf{T},\mathbf{F}\}$ מתאים פסוק בצורת DNF שטבלת האמת שלו היא f. נזכיר את האופן שבו מוגדרת צורה זו:

הגדרה 5.27 **פסוקית** DNF היא פסוק מהצורה $C=(l_1\wedge l_2\wedge\dots\wedge l_n)$ כך ש־$l_i\in\{X,\neg X\}$ עבור משתנה X כלשהו. l_i נקרא **ליטרל**.

פסוק DNF הוא פסוק מהצורה $C_1\vee C_2\vee\dots\vee C_m$ כאשר C_i היא פסוקית DNF לכל i.

לצורת DNF קיימת צורה דואלית, CNF (Conjunctive Normal Form):

הגדרה 5.28 **פסוקית** CNF היא פסוק מהצורה $C=(l_1\vee l_2\vee\dots\vee l_n)$ כך ש־$l_i\in\{X,\neg X\}$ עבור משתנה X כלשהו. l_i נקרא **ליטרל**.

פסוק CNF הוא פסוק מהצורה $C_1\wedge C_2\wedge\dots\wedge C_m$ כאשר C_i היא פסוקית CNF לכל i.

נכון לחשוב על פסוקי CNF בתור "מערכת של אילוצים" - כל C_i הוא אילוץ שהכרחי לעמוד בו, וה"תנאים" לעמידה בו מתוארים על ידי הליטרלים של C_i, שמספיק שאחד מהם יקבל ערך $\mathbf{T}$.

על מנת להראות שגם צורת CNF היא אוניברסלית נראה כיצד ניתן לבנות פסוק CNF לכל פונקציה f:

משפט 5.29 תהא $f:\{\mathbf{T},\mathbf{F}\}^n\to\{\mathbf{T},\mathbf{F}\}$ טבלת אמת כלשהי כך שקיים קלט עבורו f מחזירה $\mathbf{F}$. אז קיים פסוק φ בצורת CNF שטבלת האמת שלו היא f.

הוכחה: ראשית, נשים לב לכך שאם $C=(l_1\wedge l_2\wedge\cdots\wedge l_n)$ היא פסוקית DNF, אז $\neg C=\neg(l_1\wedge l_2\wedge\cdots\wedge l_n)$ שקולה לוגית לנוסחה $(\neg l_1\vee\neg l_2\vee\cdots\vee\neg l_n)$ על פי כללי דה־מורגן. כמו כן, על פי כלל השלילה הכפולה, אם l_i הוא מהצורה $l_i=\neg X$ אז $\neg l_i=\neg(\neg X)$ שקול לוגית ל־X. קיבלנו שקיימת פסוקית CNF שנסמן $\overline{C}$ כך ש־$\overline{C}$ שקולה לוגית ל־$\neg C$ (לא ניתן להשתמש ישירות ב־$\neg C$ כי זו איננה פסוקית CNF).

נתבונן כעת בפונקציה $\overline{f}=\neg f$ - הפונקציה שמחזירה ערך הפוך מ־f על כל קלט. מכיוון ש־$\overline{f}$ היא פונקציה לוגית, קיימת נוסחת DNF $\psi=C_1\vee C_2\vee\cdots\vee C_m$ עבורה.

נתבונן ב־$\neg\psi=\neg(C_1\vee C_2\vee\cdots\vee C_m)$. על פי כללי דה־מורגן, $\neg\psi$ שקול ל־$(\neg C_1\wedge\neg C_2\wedge\cdots\wedge\neg C_n)$, ופסוק זה שקול בתורו ל־$\varphi=\overline{C_1}\wedge\overline{C_2}\wedge\cdots\wedge\overline{C_m}$. קיבלנו ש־$\varphi$ הוא פסוק CNF השקול לוגית ל־$\neg\psi$; מכיוון ש־ψ מתאים ל־$\overline{f}$, קיבלנו ש־φ הוא בעל טבלת האמת f, כמבוקש. ■

נקודה מהותית שיש לתת עליה את הדעת בבניה של צורת ה־CNF של נוסחה היא שאם נתון לנו פסוק φ בצורת DNF, אמנם אנו יודעים למצוא פסוק ψ שקול בצורת CNF, אבל ה"המרה" כלל אינה משתמשת ב־φ! לצורך ההמרה אנו מתחילים מפסוק DNF דווקא עבור טבלת האמת **המשלימה** של φ. יש לנקודה זו חשיבות אלגוריתמית: בהינתן פסוק בצורת DNF, קל לוודא שהוא ספיק (די בכך שתהיה בו פסוקית אחת שאינה כוללת משתנה ושלילתו). לעומת זאת, לא ידוע אלגוריתם יעיל כלשהו לבדיקה האם פסוק CNF הוא ספיק. יותר במדויק, הבעיה של קביעה האם פסוק CNF נתון הוא ספיק (המכונה "בעיית SAT") היא בעיה NP־שלמה, ומשמעות הדבר היא שאלגוריתם יעיל לפתרון הבעיה יגרור כי P=NP, ופירוש הדבר הוא פתרון (מפתיע ולא צפוי) לבעיה הפתוחה המרכזית של מדעי המחשב.

אם היה אלגוריתם יעיל הממיר נוסחת CNF לנוסחת DNF שקולה, הרי שהיינו מקבלים פתרון טריוויאלי לבעיית SAT, אך מכיוון שההמרה דורשת שימוש לא בפסוק הנתון אלא דווקא בצורת ה־CNF של שלילתו, לא סביר כי מציאת צורת ה־CNF של השלילה היא קלה.

5.6 מערכת הוכחה לתחשיב הפסוקים

5.6.1 מבוא

הוכחה, במובנה המקובל במתמטיקה, היא סדרה **סופית** של טענות שכל אחת מהן היא או הנחה שלנו (הנחה שיכולה להיות **אקסיומה** - כלומר, הנחה בסיסית של התורה שלנו - או הנחה ספציפית עבור המשפט שאנו רוצים להוכיח), או נובעת מקודמותיה בעזרת **כללי היסק**. הטענה האחרונה בסדרת הטענות היא המשפט שאותו ההוכחה מוכיחה (אבל מובן מאליו שגם כל טענה אחרת שמופיעה במהלך ההוכחה "מוכחת" על ידה).

מערכת הוכחה כוללת, אם כן, רשימה של **אקסיומות** ושל **כללי היסק**. כאשר אנו בונים מערכת הוכחה, עומדות לנגד עינינו שלוש מטרות שאותה מערכת הוכחה באה למלא:

1. **נאותות**: המערכת צריכה להיות רק משפטים נכונים.
2. **שלמות**: המערכת צריכה להיות מסוגלת להוכיח כל דבר נכון.
3. **פשטות**: המערכת צריכה להיות פשוטה; בפרט, צריך שתהיה שיטה פשוטה לקרוא הוכחה במערכת ההוכחה ולוודא כי ההוכחה נכונה. מכאן שהאקסיומות וכללי ההיסק של המערכת צריכים להיות כאלו שניתנים לזיהוי והבנה על ידי הקורא.

למרבה השמחה, קיימות מערכות הוכחה עבור תחשיב הפסוקים שמקיימות את שלוש הדרישות הללו במלואן. נציג כאן דוגמא אחת למערכת הוכחה שכזו; קיימות מערכות הוכחה אחרות שמקיימות את אותה המטרה.

מערכת ההוכחה שנציג היא **סינטקטית** לחלוטין; פירוש הדבר הוא שכללי ההיסק אינם מתייחסים ל**משמעות** של הנוסחאות שהם פועלים עליהם, אלא רק למבנה התחבירי שלהם. במילים אחרות, זוהי מערכת הוכחה שניתן להפעיל **מבלי לחשוב כלל**, אלא רק לבצע "מניפולציה של סימבולים". העובדה שניתן לעשות זאת ועדיין לקבל **רק** משפטים נכונים, ואף יותר מכך - את **כל** המשפטים הנכונים, היא איננה מובנת מאליה כלל.

5.6.2 מערכת הוכחה לתחשיב הפסוקים

לצורך פשטות, מעתה ואילך נעסוק רק בקבוצת הפסוקים $\mathrm{WFF}_{\{\neg,\to\}}$. כבר ראינו כי לכל פסוק ב־WFF יש פסוק שקול ב־$\mathrm{WFF}_{\{\neg,\to\}}$ כך שאין זו מגבלה של ממש.

כללי היסק: במערכת ההוכחה שלנו יהיה כלל היסק יחיד ־ מודוס פוננס (Modus Ponens, קיצור של modus ponendo ponens בלטינית), אשר מתואר כך:

$$\frac{\alpha,\alpha\to\beta}{\beta}$$

כלומר, אם כבר הוכחנו את α והוכחנו את $\alpha\to\beta$, אז משניהם ניתן לגזור את β.

אקסיומות: במערכת האקסיומות שלנו יהיו שלוש "תבניות אקסיומה":

1. $\alpha\to(\beta\to\alpha)$
2. $(\alpha\to(\beta\to\gamma))\to((\alpha\to\beta)\to(\alpha\to\gamma))$
3. $(\neg\beta\to\neg\alpha)\to(\alpha\to\beta)$

כאשר α,β,γ הם פסוקים כלשהם. אקסיומות אלו מכונות "תבנית אקסיומה" כי כל אחת מהן אינה אקסיומה בודדת, אלא אינסוף האקסיומות שמתקבלות מהצבת פסוקים α,β,γ כלשהם בתבניות. אקסיומות אלו לא נבחרו, כמובן, באופן שרירותי; נבין בהמשך מדוע בחרנו ספציפית בהן.

ניתן כעת להגדיר פורמלית את קבוצת המשפטים הניתנים להוכחה:

הגדרה 5.30 תהא A קבוצת האקסיומות מהצורות 1־3 לעיל, ו־$\mathrm{MP}(\varphi,\psi)$ פונקציית יצירה המוגדרת כך: $\mathrm{MP}(\varphi,\psi)=\begin{cases}\beta & \psi=\varphi\to\beta\\ \varphi & \text{else}\end{cases}$

תהא Φ קבוצת פסוקים כלשהי. אז קבוצת **הפסוקים היכיחים** מ־Φ (או **המסקנות** מ־Φ) מוגדרת בתור $\mathrm{Ded}(\Phi)\triangleq X_{\{A\cup\Phi\},\{\mathrm{MP}\}}$.

אם φ יכיח מ־Φ נסמן זאת ב־$\Phi\vdash\varphi$. כאשר $\Phi=\emptyset$ נסמן פשוט $\vdash\varphi$.

מטרתנו היא להוכיח כי לכל קבוצת פסוקים Φ ופסוק φ מתקיים $\Phi\models\varphi\iff\Phi\vdash\varphi$.

כל אחד מכיווני המשפט הוא חשוב בפני עצמו וזוכה לשם משל עצמו: $\Phi\vdash\varphi\Rightarrow\Phi\models\varphi$ מכונה **משפט הנאותות** והוא מראה כי "כל מה שיכיח, נכון", ואילו הכיוון $\Phi\models\varphi\Rightarrow\Phi\vdash\varphi$ מכונה **משפט השלמות** והוא מראה כי "כל מה שנכון, יכיח". נוכיח כעת את משפט הנאותות, אבל הוכחת משפט השלמות קשה יותר ותדרוש עבודת הכנה.

משפט 5.31 (משפט הנאותות לתחשיב הפסוקים) $\Phi\vdash\varphi\Rightarrow\Phi\models\varphi$

הוכחה: ההוכחה היא באינדוקציית מבנה על $\mathrm{Ded}(\Phi)$. לכל $\varphi\in\mathrm{Ded}(\Phi)$ אנו רוצים להוכיח שמתקיימת התכונה $\Phi\models\varphi$, דהיינו שכל השמה שמספקת את Φ מספקת את φ.

בסיס: ראינו בטענה 5.16 כי כל האקסיומות הן טאוטולוגיות ולכן בוודאי נובעות לוגית מ־Φ. כמו כן לכל פסוק $\varphi\in\Phi$, כל השמה שמספקת את Φ מספקת בפרט את φ (אחרת היא לא הייתה מספקת את Φ).

סגור: יהיו φ,ψ פסוקים ב־$\mathrm{Ded}(\Phi)$ שעל פי הנחת האינדוקציה מקיימים $\Phi\models\varphi$ ו־$\Phi\models\psi$. אם ψ **אינו** מהצורה $\varphi\to\beta$, אז $\mathrm{MP}(\varphi,\psi)=\varphi$ ולכן כמובן ש־$\Phi\models\mathrm{MP}(\varphi,\psi)$.

נניח אם כן כי $\varphi\to\beta=\psi$. מכיוון ש־$\Phi\models\varphi\to\beta$ הרי מטענה 5.20 עולה ש־$\Phi\cup\{\varphi\}\models\beta$ ומכיוון שגם $\Phi\models\varphi$ הרי מטענה 5.22 עולה ש־$\Phi\models\beta=\mathrm{MP}(\varphi,\psi)$ כנדרש. ■

כדאי לבחון את התכונות של מערכת ההוכחה להן נזקקנו במהלך ההוכחה; כל מה שנזקקנו לו היה העובדה שהאקסיומות הלוגיות שלנו הן טאוטולוגיות ושכלל הגזירה שלנו משמר נביעה לוגית. זה מצביע על הקלות הגדולה יחסית שבה ניתן לבנות מערכות הוכחה ־ כל בחירה של טאוטולוגיות ושל כללי גזירה שמשמרים נביעה לוגית תניב מערכת הוכחה שמשפט הנאותות מתקיים בה.

עיקר הקושי הוא בכיוון השני, $\Phi\models\varphi\Rightarrow\Phi\vdash\varphi$, שמעיד על כך שמערכת ההוכחה שלנו חזקה מספיק כדי להוכיח את כל מה שנכון. לשם כך יהיה עלינו להבין לעומק את תכונות מערכת ההוכחה הספציפית שלנו.

5.6.3 הוכחות ומשפט הדדוקציה

הגדרה 5.32 **הוכחה** של פסוק φ מתוך קבוצת הנחות Φ היא סדרה **סופית** של פסוקים $\alpha_1, \alpha_2, \ldots, \alpha_n$ כך ש־$\varphi = \alpha_n$ וכמו כן לכל i מתקיים אחד מהבאים:

1. או ש־$\alpha_i \in A$ (אקסיומה).
2. או ש־$\alpha_i \in \Phi$.
3. או שקיימים $j, k < i$ כך ש־$\alpha_i = \mathrm{MP}\left(\alpha_j, \alpha_k\right)$.

במילים אחרות, הוכחה של פסוק היא סדרת יצירה שלו, במובן של הגדרה 3.32. ראינו בטענה 3.33 שאיבר שייך לקבוצה אינדוקטיבית אם ורק אם קיימת לו סדרת יצירה, ולכן נוכל להסיק את המקרה הפרטי הבא:

מסקנה 5.33 $\Phi \vdash \varphi$ אם ורק אם קיימת הוכחה ל־φ מתוך Φ.

כעת יש לנו שתי דרכי התבוננות על מערכת ההוכחה: גם בתור קבוצה שנוצרת באינדוקציית מבנה, וגם בתור קבוצת הפסוקים שקיימת להם הוכחה.

הצעד הראשון בדרך להוכחת משפט השלמות והנאותות הוא גרסה תחבירית של משפט הדדוקציה:

משפט 5.34 (משפט הדדוקציה) לכל קבוצת פסוקים Φ ופסוקים α, β, $\Phi \cup \{\alpha\} \vdash \beta$ אם ורק אם $\Phi \vdash \alpha \to \beta$.

הוכחה: להבדיל מהגרסה הסמנטית של משפט הדדוקציה, כאן ההוכחה איננה מיידית, שכן העובדה שאנו יודעים ליצור את המחרוזת β על ידי מניפולציה של המחרוזות ב־$\Phi \cup \{\alpha\}$ כלל אינה מבטיחה שניתן ליצור את המחרוזת $\alpha \to \beta$ (שהיא **יותר** מורכבת מ־β לבד) על ידי **פחות** מחרוזות.

עם זאת, כיוון אחד נותר טריוויאלי: אם $\Phi \vdash \alpha \to \beta$ אז נציג הוכחה ל־β מתוך $\Phi \cup \{\alpha\}$: פשוט לוקחים הוכחה ל־$\alpha \to \beta$ מתוך Φ, ומשרשרים לסופה את α (הנחה) ואת β (מתקבל מתוך $\alpha \to \beta$ ו־α על ידי MP).

בכיוון השני נוכיח את הטענה באינדוקציית מבנה על $\mathrm{Ded}\left(\Phi \cup \{\alpha\}\right)$.

יהי $\gamma \in B$, כלומר γ הוא אקסיומה או איבר של $\Phi \cup \{\alpha\}$. אנו רוצים להוכיח את $\alpha \to \gamma$ מתוך Φ. ראשית נניח כי $\gamma = \alpha$, אז ההוכחה הפורמלית במקרה זה היא:

1. $\left(\alpha \to \left(\left(\alpha \to \alpha\right) \to \alpha\right)\right) \to \left(\left(\alpha \to \left(\alpha \to \alpha\right)\right) \to \left(\alpha \to \alpha\right)\right)$ (תבנית אקסיומה 2 עם $\beta = \left(\alpha \to \alpha\right)$ ו־$\gamma = \alpha$).
2. $\alpha \to \left(\left(\alpha \to \alpha\right) \to \alpha\right)$ (תבנית אקסיומה 1 עם $\beta = \left(\alpha \to \alpha\right)$).
3. $\left(\alpha \to \left(\alpha \to \alpha\right)\right) \to \left(\alpha \to \alpha\right)$ (MP על 1 ו־2).
4. $\alpha \to \left(\alpha \to \alpha\right)$ (תבנית אקסיומה 1 עם $\beta = \alpha$).
5. $\alpha \to \alpha$ (MP על 3 ו־4).

נניח כעת כי $\gamma \in \Phi$ או ש־γ הוא אקסיומה. אנו רוצים להוכיח את $\alpha \to \gamma$. ההוכחה הפורמלית במקרה זה היא:

1. $\gamma \to \left(\alpha \to \gamma\right)$ (תבנית אקסיומה 1)
2. γ (הנחה/אקסיומה).
3. $\alpha \to \gamma$ (MP על 1 ו־2).

סיימנו את מקרי הבסיס. נניח כעת כי γ התקבל מהפסוקים $\beta, \beta \to \gamma$ על ידי MP ושעבור פסוקים אלו מתקיים $\Phi \vdash \alpha \to \beta$ ו־$\Phi \vdash \alpha \to \left(\beta \to \gamma\right)$. אז הוכחה של $\alpha \to \gamma$ תורכב ראשית כל משרשור שתי ההוכחות הללו, ולאחר מכן:

1. $\alpha \to \beta$ (סוף הוכחה 1)
2. $\alpha \to \left(\beta \to \gamma\right)$ (סוף הוכחה 2).
3. $\left(\alpha \to \left(\beta \to \gamma\right)\right) \to \left(\left(\alpha \to \beta\right) \to \left(\alpha \to \gamma\right)\right)$ (תבנית אקסיומה 2).
4. $\left(\alpha \to \beta\right) \to \left(\alpha \to \gamma\right)$ (MP על 2 ו־3).

5. $\alpha \to \gamma$ (MP על 1 ו־4).

■

הוכחה זו מבהירה את הצורך בשתי תבניות האקסיומה 1 ו־2; כפי שניתן לראות, הן קריטיות למהלך ההוכחה עצמו (בפרט ניתן לראות כיצד תבנית 2 "מהונדסת" כדי להתאים בדיוק לצעד האינדוקציה).

5.6.4 עקביות של קבוצת פסוקים

מכיוון שאנו מרשים לכל קבוצת פסוקים Φ לשמש כקבוצה של הנחות במערכת ההוכחה שלנו, אנחנו פותחים פתח לאפשרות שהפסוקים ב־Φ יסתרו אלו את אלו. כדי לתאר את המצב באופן פורמלי אנו משתמשים בהגדרה הבאה:

הגדרה 5.35 קבוצת פסוקים Φ היא **עקבית** אם לא קיים פסוק φ כך ש־$\Phi \vdash \varphi$ וגם $\Phi \vdash \neg\varphi$.

טענה 5.36 אם לקבוצת פסוקים Φ קיים מודל אז Φ היא עקבית.

הוכחה: נניח כי Φ אינה עקבית, כלומר קיים φ כך ש־$\Phi \vdash \varphi$ וגם $\Phi \vdash \neg\varphi$. ממשפט הנאותות לתחשיב הפסוקים נובע ש־$\Phi \models \varphi$ וגם $\Phi \models \neg\varphi$, אבל על פי הגדרה כל השמה שמספקת את φ אינה מספקת את $\neg\varphi$. לכן $\Phi \models \varphi \wedge \Phi \models \neg\varphi$ מתקיים רק אם לא קיימת השמה שמספקת את כל פסוקי Φ, כלומר אין ל־Φ מודל. ■

גם הכיוון השני של המשפט ־ לכל קבוצה עקבית קיים מודל ־ הוא נכון, אך ההוכחה שלו קשה בהרבה; כפי שנראה בהמשך, הוא מהווה מעין ניסוח שקול למשפט השלמות.

תכונה מהותית של עקביות הינה שהיא תכונה **סופית** של Φ:

טענה 5.37 אם Φ אינה עקבית אז קיימת $\Phi' \subseteq \Phi$ **סופית** כך ש־Φ' אינה עקבית.

הוכחה: אם Φ אינה עקבית, אז קיים φ כך ש־$\Phi \vdash \varphi$ וגם $\Phi \vdash \neg\varphi$. כלומר, קיימת ל־φ הוכחה מ־Φ וכך גם ל־$\neg\varphi$. נגדיר את Φ' להיות כל פסוקי Φ שנעשה בהם שימוש במהלך אחת משתי ההוכחות. כל הוכחה היא בעלת אורך סופי, ולכן בפרט Φ' סופית. ההוכחה שהראתה ש־$\Phi \vdash \varphi$ מראה גם ש־$\Phi' \vdash \varphi$ וכך גם עבור $\neg\varphi$. ■

מסקנה 5.38 Φ עקבית אם ורק אם כל תת־קבוצה סופית של Φ עקבית.

טענה 5.39 ("עקרון הפיצוץ") Φ אינה עקבית אם ורק אם לכל α, $\Phi \vdash \alpha$.

הוכחה: כיוון אחד קל: אם עבור Φ מתקיים $\Phi \vdash \alpha$ לכל α, אז בפרט עבור α שרירותי יתקיים גם $\Phi \vdash \neg\alpha$ ולכן Φ אינה עקבית.

בכיוון השני, נניח כי Φ אינה עקבית ונציג הוכחה עבור α מ־Φ. מכיוון ש־Φ אינה עקבית, קיימות הוכחות ממנה של φ ושל $\neg\varphi$ עבור φ כלשהי. ההוכחה של α תיפתח בהוכחה של פסוקים אלו, ואז:

ההוכחה תיפתח בהוכחה של φ ושל $\neg\varphi$, ולאחר מכן:

1. φ
2. $\neg\varphi$
3. $(\neg\alpha \to \neg\varphi) \to (\varphi \to \alpha)$ (תבנית אקסיומה 3).
4. $\neg\varphi \to (\neg\alpha \to \neg\varphi)$ (תבנית אקסיומה 1 עם $\alpha = \neg\varphi$ ו־$\beta = \neg\alpha$).
5. $\neg\alpha \to \neg\varphi$ (MP על 2 ו־4).
6. $\varphi \to \alpha$ (MP על 3 ו־5).
7. α (MP על 1 ו־6).

■

תופעה זו, לפיה קבוצת הנחות שאינה עקבית מוכיחה כל פסוק שהוא, היא נפוצה למדי במערכות הוכחה, אם כי קיימות גם מערכות הוכחה חלשות שבהן היא אינה מתקיימת.

הגענו אל טענת העזר המרכזית שלנו, שתהיה "כלי הנשק" העיקרי בהתמודדות עם משפט השלמות:

טענה 5.40 ("עקרון ההוכחה בשלילה") אם $\Phi \cup \{\neg\varphi\}$ אינה עקבית, אז $\Phi \vdash \varphi$.

הוכחה: אם $\Phi \cup \{\neg\varphi\}$ אינה עקבית אז לכל α קיימת הוכחה ל־α מתוך $\Phi \cup \{\neg\varphi\}$. בפרט עבור β שהיא אקסיומה כלשהי מתקיים $\Phi \cup \{\neg\varphi\} \vdash \neg\beta$. ממשפט הדדוקציה נובע כעת ש־$\Phi \vdash \neg\varphi \to \neg\beta$. כעת נקבל את ההוכחה הבאה ל־φ מתוך Φ:

1. $\neg\varphi \to \neg\beta$
2. $(\neg\varphi \to \neg\beta) \to (\beta \to \varphi)$ (אקסיומה 3).
3. $\beta \to \varphi$ (MP על 1 ו־2).
4. β (β היא אקסיומה).
5. φ (MP על 3,4).

■

שימו לב שהשתמשנו בתבנית אקסיומה מס' 3 הן בהוכחת עקרון הפיצוץ והן בהוכחת עקרון ההוכחה בשלילה, להם נזדקק בהמשך. בכך סיימנו להסביר את בחירת האקסיומות שלנו: אקסיומות 1,2,3 הן מה שנדרש לנו כדי שמערכת ההוכחה שלנו (בעלת כלל ההיסק היחיד MP) תקיים את שלוש התכונות הללו ־ דדוקציה, פיצוץ, הוכחה בשלילה.

5.6.5 הוכחת משפט השלמות

נפתח בהגדרה:

הגדרה 5.41 קבוצת פסוקים Φ היא **תורה** אם היא עקבית.
Φ תיקרא **תורה שלמה** (או **עקבית מקסימלית**) אם לכל פסוק $\varphi \in \mathrm{WFF}_{\{\neg,\to\}}$ מתקיים ש־$\Phi \vdash \varphi$ או ש־$\Phi \vdash \neg\varphi$.

במילים, תורה היא שלמה אם לכל פסוק, ניתן להוכיח מהתורה אותו או את שלילתו.
חשוב **ביותר** לשים לב לכך שאנו משתמשים במילה "שלמות" במספר משמעויות שונות. ראשית, ישנה "מערכת **שלמה** של קשרים". שנית, אנו מבקשים להוכיח את משפט **השלמות** עבור מערכת ההוכחה שלנו; וכעת הגדרנו מהי תורה **שלמה**. המשמעות של "שלמות" עבור שלושת מקרים אלו היא **שונה מהותית** וקיימת מסיבות היסטוריות בלבד; בפועל היה עדיף להשתמש בשמות שונים עבור מושגים אלו. נחדד את ההבדלים:

- מערכת שלמה של קשרים היא **מערכת קשרים** שבעזרתה ניתן לבנות פסוק שממדל כל טבלת אמת.
- מערכת הוכחה שלמה היא **מערכת הוכחה** (אוסף של אקסיומות וכללי היסק) שבה לכל קבוצת פסוקים Φ, אם $\Phi \models \varphi$ אז $\Phi \vdash \varphi$.
- תורה שלמה היא **תורה** (אוסף של פסוקים) כך שלכל φ מתקיים ש־$\Phi \vdash \varphi$ או ש־$\Phi \vdash \neg\varphi$.

מערכת הוכחה יכולה להיות שלמה, ועם זאת שיהיו קבוצת פסוקים Φ שאינן תורות שלמות, באותה מערכת הוכחה.
המקרה הידוע ביותר של בלבול שנגרם עקב השימוש הכפול במילה "שלמות" הוא הבלבול בין משפט השלמות של גדל לתחשיב היחסים, ומשפטי אי־השלמות של גדל. במקרה הראשון מדובר על שלמות של מערכת הוכחה, ובמקרה השני מדובר על אי־שלמות של תורות. לא נרחיב בנושא כעת.
כעת, את האסטרטגיה שלנו להוכחת משפט השלמות ניתן לחלק לשלושה צעדים עיקריים:

1. נוכיח שכל תורה ניתנת להרחבה לתורה שלמה.
2. נוכיח שלכל תורה שלמה יש מודל, ונסיק מכך ומשלב 1 שלכל תורה יש מודל.
3. נוכיח מתוך שלב 2 את משפט השלמות.

שלבים 1 ו־2 ידרשו עבודה טכנית רבה יחסית, אך שלב 3 נובע מהם כמעט מייד.

משפט 5.42 אם Φ תורה, אז קיימת תורה שלמה $\overline{\Phi}$ כך ש־$\Phi \subseteq \overline{\Phi}$.

הוכחה: הרעיון יהיה לעבור באופן סדרתי על כל הפסוקים הקיימים ב־$\mathrm{WFF}_{\{\neg,\rightarrow\}}$ ולכל פסוק φ, להוסיף את $\neg\varphi$ לתורה שלנו אם זה לא יוצר סתירה (הסיבה שבגללה מוסיפים דווקא את השלילה של φ תתבהר בקרוב). יש אינסוף פסוקים ב־$\mathrm{WFF}_{\{\neg,\rightarrow\}}$ ולכן ה"תהליך" של מעבר סדרתי על כולם יהיה אינסופי, אך נתגבר בקלות על בעיה זו.

ראשית, תהיה $\varphi_1,\varphi_2,\ldots$ מניה כלשהי של אברי $\mathrm{WFF}_{\{\neg,\rightarrow\}}$. קיימת כזו שכן $\mathrm{WFF}_{\{\neg,\rightarrow\}}$ בת מניה. כעת נגדיר סדרה $\Phi_0,\Phi_1,\Phi_2,\ldots$ באופן האינדוקטיבי הבא: $\Phi_0=\Phi$ ולכל $n>0$, אחד משניים: אם $\Phi_{n-1}\cup\{\neg\varphi_n\}$ היא עקבית, אז $\Phi_n=\Phi_{n-1}\cup\{\neg\varphi_n\}$, ואם $\Phi_{n-1}\cup\{\neg\varphi_n\}$ אינה עקבית $\Phi_n=\Phi_{n-1}$. נשים לב כי $\Phi_n\supseteq\Phi_{n-1}$ בכל אחד מהמקרים.

נשים לב שבאופן אינדוקטיבי נובע כי Φ_n עקבית לכל n; $\Phi_0=\Phi$ עקבית כי הנחנו ש־Φ תורה. נניח ש־Φ_{n-1} עקבית. אם $\Phi_n=\Phi_{n-1}$ אז בוודאי ש־Φ_n עקבית. אחרת, על פי בניית Φ_n, $\Phi_n=\Phi_{n-1}\cup\{\neg\varphi_n\}$ כך ש־$\Phi_{n-1}\cup\{\neg\varphi_n\}$ עקבית, ולכן Φ_n עקבית.

כעת נגדיר $\overline{\Phi}=\bigcup_{n=1}^{\infty}\Phi_n$.

עלינו להוכיח כי $\overline{\Phi}$ היא תורה (כלומר עקבית) וש־$\overline{\Phi}$ היא שלמה.

נוכיח ראשית כי $\overline{\Phi}$ עקבית. נניח בשלילה כי קיימות הוכחות $\overline{\Phi}\vdash\psi$ וגם $\overline{\Phi}\vdash\neg\psi$ עבור ψ כלשהו. מכיוון ששתי ההוכחות סופיות באורכן, יש רק מספר סופי של פסוקים $\psi_1,\ldots,\psi_m$ ב־$\overline{\Phi}$ שמופיעים בהן. לכל פסוק ψ_j קיים n_j כלשהו כך ש־$\psi_j\in\Phi_{n_j}$ (מהגדרת איחוד). נגדיר $n=\max\{n_1,\ldots,n_m\}$, אז מכיוון ש־$\Phi_n\supseteq\Phi_{n_j}$ לכל $1\le j\le m$ נקבל ש־$\psi_j\in\Phi_n$ לכל j כזה, ומכאן שכל ההנחות בהוכחות של ψ ו־$\neg\psi$ נמצאות כבר ב־Φ_n, ולכן $\Phi_n\vdash\psi$ וגם $\Phi_n\vdash\neg\psi$, כלומר Φ_n עצמה אינה עקבית – בסתירה לכך שהוכחנו קודם לכן שהיא עקבית. מכאן ש־$\overline{\Phi}$ עקבית.

נותר להוכיח כי $\overline{\Phi}$ היא תורה שלמה. יהא $\psi\in\mathrm{WFF}_{\{\neg,\rightarrow\}}$ פסוק כלשהו, אז $\psi=\varphi_n$ עבור n טבעי כלשהו. כעת נבדיל בין שתי אפשרויות:

אם $\Phi_{n-1}\cup\{\neg\varphi_n\}$ הייתה עקבית אז $\neg\psi=\neg\varphi_n\in\Phi_n\subseteq\overline{\Phi}$ ולכן קיימת ל־$\neg\psi$ הוכחה מאורך 1 מתוך $\overline{\Phi}$: $\neg\psi$ עצמו.

אם $\Phi_{n-1}\cup\{\neg\varphi_n\}$ איננה עקבית, אז מטענה 5.40 נובע ש־$\Phi_{n-1}\vdash\varphi_n=\psi$, ולכן $\overline{\Phi}\vdash\psi$ (אותה הוכחה, שכן כל הנחה שנמצאת ב־Φ_{n-1} נמצאת גם ב־$\overline{\Phi}$). ■

נשים לב לכך שההוכחה התבססה רק על תכונת ה"הוכחה בשלילה" של מערכת ההוכחה שלנו; ככזו, היא תעבוד עבור כל מערכת הוכחה שבה מתקיימת תכונת ההוכחה בשלילה. בנוסף הסתמכנו על כך ש־$\mathrm{WFF}_{\{\neg,\rightarrow\}}$ הנה בת מניה, אך זו הנחה כללית למדי (היא נובעת מכך שכל פסוק ב־WFF הוא מאורך סופי ומורכב מתווים שמגיעים מתוך קבוצה בת מניה; פסוקים מסוגים אחרים קשה ממילא לתאר).

השלב הבא בהוכחה הוא השלב העיקרי: נרצה להראות שלתורה שלמה Φ קיים מודל (השמה מספקת). הסיבה שבגללה אנו מטפלים בתורה **שלמה** ולא בתורה כלשהי היא שעבור תורה שלמה חופש הפעולה שלנו **קטן יותר**; כפי שנראה, יש בדיוק מודל פוטנציאלי יחיד עבור Φ שלמה. דווקא הגבלת חופש הפעולה הזה היא זו שמקלה עלינו את הגדרת ההשמה המספקת ואת ההוכחה. תופעה זו – הגבלת חופש פעולה שמקלה על ההוכחה – היא מוטיב חוזר בכל רחבי המתמטיקה.

משפט 5.43 לתורה שלמה Φ קיים מודל יחיד.

הוכחה: כדי לבנות את המודל עלינו להגדיר השמה $Z:\{p_i|i\in\mathbb{N}\}\to\{\mathbf{T},\mathbf{F}\}$. לכל i, p_i הוא פסוק (אטומי) ומכיוון ש־Φ היא תורה שלמה, $\Phi\vdash p_i$ או $\Phi\vdash\neg p_i$. במקרה הראשון נגדיר $Z(p_i)=\mathbf{T}$ ובמקרה השני נגדיר $Z(p_i)=\mathbf{F}$.

ראשית נראה כי כל השמה Z' שנבדלת מ־Z ולו במשתנה יחיד היא בהכרח **אינה** מודל של Φ (ולכן אם Z היא מודל של Φ זהו מודל יחיד). נניח כי $Z'(p_i)\neq Z(p_i)$ עבור i כלשהו. אם $\Phi\vdash p_i$ אז על פי ההגדרה, $Z'(p_i)=\mathbf{F}$. כמו כן, על פי משפט הנאותות, $\Phi\models p_i$, כלומר אם Z' מספקת את Φ אז Z' מספקת את p_i. מכיוון ש־Z' אינה מספקת את p_i אז בהכרח Z' אינה מספקת את Φ. באופן דומה, אם $\Phi\vdash\neg p_i$ אז על פי ההגדרה $Z'(\neg p_i)=\mathbf{T}$ ושוב נסיק ש־Z' אינה מספקת את Φ.

נותר להראות כי Z היא כן מודל של Φ. נוכיח באינדוקציית מבנה על $\mathrm{WFF}_{\{\neg,\rightarrow\}}$ כי $\Phi\vdash\varphi$ אם ורק אם $\overline{Z}(\varphi)=\mathbf{T}$ (ובפרט אם $\varphi\in\Phi$ אז $\overline{Z}(\varphi)=\mathbf{T}$).

הבסיס ל־$\mathrm{WFF}_{\{\neg,\rightarrow\}}$ הוא כל המשתנים p_i. $\Phi\vdash p_i$ אם ורק אם $\overline{Z}(p_i)=\mathbf{T}$ על פי הגדרת Z. נעבור לצעד האינדוקציה.

יהי $\psi=\neg\varphi$, אז:

$$\Phi\vdash\psi \iff_{(1)} \Phi\nvdash\varphi \iff_{(2)} \iff \overline{Z}(\varphi)=\mathbf{F} \iff_{(3)}\overline{Z}(\psi)=\mathbf{T}$$

השקילות הראשונה נובעת מכך ש־Φ תורה ולכן לא מוכיחה גם את φ וגם את $\psi=\neg\varphi$. השקילות השניה נובעת מהנחת האינדוקציה על φ. השקילות השלישית נובעת ישירות מהגדרת ערך האמת של השמות ומכך ש־$\psi=\neg\varphi$.

כעת יהי $\psi = \alpha \to \beta$. נניח כי $\Phi \vdash \alpha \to \beta$ ונוכיח כי $\overline{Z}(\psi) = \mathbf{T}$. אם $\overline{Z}(\alpha) = \mathbf{F}$, סיימנו, אז נניח כי $\overline{Z}(\alpha) = \mathbf{T}$ ונוכיח כי $\overline{Z}(\beta) = \mathbf{T}$. על פי הנחת האינדוקציה, די להוכיח כי $\Phi \vdash \beta$. מכיוון ש־$\overline{Z}(\alpha) = \mathbf{T}$ אז על פי הנחת האינדוקציה נתון לנו ש־$\Phi \vdash \alpha$, ולכן קיימת ההוכחה הבאה:

1. α (ניתן להוכחה מ־Φ).
2. $\alpha \to \beta$ (ניתן להוכחה מ־Φ).
3. β (MP על 1 ו־2).

נותר לטפל בכיוון השני. נניח כי $\overline{Z}(\psi) = \mathbf{T}$ ונוכיח כי $\Phi \vdash \alpha \to \beta$. נבדיל כעת בין שני מקרים: אם $\overline{Z}(\beta) = \mathbf{T}$ אז על פי הנחת האינדוקציה $\Phi \vdash \beta$ ולכן בפרט $\Phi \cup \{\alpha\} \vdash \beta$ וממשפט הדדוקציה נקבל $\Phi \vdash \alpha \to \beta$. אחרת, מכיוון ש־$\overline{Z}(\alpha \to \beta) = \mathbf{T}$ בהכרח $\overline{Z}(\alpha) = \mathbf{F}$, כלומר $\Phi \nvdash \alpha$, ומכיוון ש־Φ היא תורה שלמה, $\Phi \vdash \neg\alpha$. מכאן ש־$\Phi \cup \{\alpha\}$ אינה עקבית ומעקרון הפיצוץ, $\Phi \cup \{\alpha\} \vdash \beta$, וכעת נקבל ממשפט הדדוקציה ש־$\Phi \vdash \beta$ כנדרש.

בכך נסתיימה הוכחת המשפט. ■

מסקנה 5.44 (משפט השלמות לתחשיב הפסוקים, ניסוח ראשון) אם Φ תורה אז יש ל־Φ מודל.

הוכחה: $\Phi \subseteq \overline{\Phi}$ כך ש־$\overline{\Phi}$ היא תורה שלמה ולכן יש לה מודל יחיד. מודל זה הוא בפרט מודל של Φ. ■

הגענו סוף סוף אל היעד:

משפט 5.45 (משפט השלמות לתחשיב הפסוקים, ניסוח שני): אם $\Phi \models \varphi$ אז $\Phi \vdash \varphi$.

הוכחה: אם $\Phi \cup \{\neg\varphi\}$ אינה עקבית אז מטענה 5.40 עולה ש־$\Phi \vdash \varphi$. נניח בשלילה כי $\Phi \cup \{\neg\varphi\}$ היא עקבית אז (מהניסוח הראשון של משפט השלמות) קיים לה מודל, דהיינו קיימת השמה שמספקת את Φ ואת $\neg\varphi$ בו זמנית, בסתירה לכך ש־$\Phi \models \varphi$ (דהיינו, שכל השמה אשר מספקת את Φ מספקת את φ ולכן אינה מספקת את $\neg\varphi$). ■

5.7 משפט הקומפקטיות לתחשיב הפסוקים

מסקנה חזקה מיידית שניתן לגזור מתוך משפט השלמות לתחשיב הפסוקים היא **משפט הקומפקטיות**:

משפט 5.46 (משפט הקומפקטיות לתחשיב הפסוקים) תהא Φ קבוצת נוסחאות בתחשיב הפסוקים. אז ל־Φ קיים מודל אם ורק אם לכל תת־קבוצה סופית של Φ קיים מודל.

הוכחה: כזכור, מסקנה 5.38 הראתה ש־Φ היא עקבית אם ורק אם כל תת־קבוצה סופית של Φ היא עקבית. כמו כן Φ עקבית אם ורק אם קיים לה מודל, ומכאן נובעת התוצאה. ■

התופעה אשר מתקיימת במשפט ־ אם משהו מתקיים לכל תת־קבוצה סופית של A אז הוא מתקיים לכל A ־ איננה מובנת מאליה. הבה ונראה מספר דוגמאות נגדיות על מנת להשתכנע בכך:

- הדוגמה הטיפשית ביותר היא כמובן העובדה שעבור A אינסופית, העובדה שכל תת־קבוצה סופית של A היא סופית אינה גוררת ש־A עצמה היא סופית.
- אם $A = (0,1)$ אז לכל תת־קבוצה סופית של A קיים איבר מינימלי, אך ל־A עצמה אין איבר מינימלי.
- לכל תת־קבוצה סופית $A \subseteq \mathbb{N}$ קיים מספר $a = \mathrm{lcm}A \in \mathbb{N}$ שהוא המספר **החיובי** המינימלי שמתחלק בכל אברי A. עם זאת, עבור $\mathbb{N}$ לא קיים מספר שכזה.

שמו של משפט הקומפקטיות מגיע מתכונת הקומפקטיות בטופולוגיה; קיימת הוכחה אלטרנטיבית למשפט הקומפקטיות לתחשיב הפסוקים שאינה עוברת דרך משפט השלמות אלא דרך **משפט טיכונוף** הטופולוגי. נציג אותה כאן בקצרה עבור הבקיאים במושגים: **הוכחה:** (הוכחה טופולוגית למשפט הקומפקטיות לתחשיב הפסוקים). על כל השמה $Z : \{p_1, p_2, \dots\} \to \{\mathbf{T}, \mathbf{F}\}$ נחשוב בתור איבר של מרחב המכפלה $\{0,1\}^{\mathbb{N}}$ עם טופולוגיית המכפלה הרגילה כאשר לכל $\{0,1\}$ אנו לוקחים את הטופולוגיה הדיסקרטית הרגילה. כל מרחב $\{0,1\}$ הוא קומפקטי (שכן הוא סופי) וממשפט טיכונוף, $\{0,1\}^{\mathbb{N}}$ קומפקטי. בנוסף, במרחב זה קבוצה פתוחה היא סגורה.

לכל נוסחה $\varphi\in\Phi$ נגדיר קבוצה $A_{\varphi}\subseteq\{0,1\}^{\mathbb{N}}$ של כל ההשמות אשר מספקות את φ. מהגדרת טופולוגיית המכפלה, קבוצות הבסיס לטופולוגיה של $\{0,1\}^{\mathbb{N}}$ הן קבוצות של השמות שמזדהות כולן על קבוצה סופית מסויימת של משתנים והערכים שהן נותנות לשאר המשתנים נקבעים בחופשיות. את A_{φ} ניתן להציג כאיחוד של קבוצות בסיס אלו, כאשר האיחוד נלקח על פני כל ההשמות האפשריות למשתנים שמופיעים ב־φ ומספקות את φ (יש מספר סופי של משתנים כאלו שכן φ סופית). מכאן ש־A_{φ} היא קבוצה פתוחה ולכן גם סגורה.

כעת, אם כל תת־קבוצה סופית $\Phi'\subseteq\Phi$ היא עקבית אז $\bigcap_{\varphi\in\Phi'}A_{\varphi}\neq\emptyset$, כלומר $\{A_{\varphi}\}_{\varphi\in\Phi}$ מקיימת את תכונת החיתוכים הסופיים. מכיוון ש־$\{0,1\}^{\mathbb{N}}$ קומפקטי, נובע מכך ש־$\bigcap_{\varphi\in\Phi}A_{\varphi}\neq\emptyset$, ולכן קיימת השמה אשר מספקת את כל Φ. ■

בהערת אגב מעניין לציין כי יש דמיון בין אופי ההוכחה של משפט טיכונוף (המשפט ה"כבד" שעומד מאחורי ההוכחה הקצרה והפשוטה יחסית למשפט הקומפקטיות שהצגנו כרגע) ובין אופי ההוכחה של משפט השלמות לתחשיב הפסוקים (המשפט ה"כבד" שעמד מאחורי ההוכחה הקצרה והפשוטה שהצגנו קודם). בשני המקרים חלק מהותי בהוכחה הוא **הגבלת חופש הבחירה** שלנו בסיטואציה מסויימת (בחירת השמה מספקת לתורה Φ בהוכחת משפט השלמות; בניית איבר הנמצא בחיתוך של משפחה של קבוצות סגורות בהוכחת משפט טיכונוף) והגבלה זו מתבצעת על ידי **הרחבה** של הקבוצה שבה אנו עוסקים לקבלת קבוצה שהיא מקסימלית במובן מסויים. לא נרחיב עוד על הדמיון הזה כאן שכן הדבר יצריך גלישה לטופולוגיה קבוצתית.

נעבור למקצת משימושי המשפט. משפט הקומפקטיות מעניק לנו את ההזדמנות הראשונה לראות כיצד ניתן ליישם תוצאות מלוגיקה מתמטית על תחומים מתמטיים אחרים. ניתן להבין אותו כך: בכל פעם שבה אנו רוצים להוכיח טענה בסגנון "אם כל תת־קבוצה סופית של A מקיימת תכונה כלשהי אז A מקיימת אותה", אז משפט הקומפקטיות מראה לנו שכך אכן מתקיים, **בתנאי** שאנו מסוגלים לנסח את התכונה באמצעות תחשיב הפסוקים. מכיוון שכושר הביטוי של תחשיב הפסוקים מוגבל למדי, משפט הקומפקטיות יהיה שימושי רק עבור דוגמאות פשוטות למדי; בהמשך נראה את תחשיב היחסים שכוח ההבעה שלו רב הרבה יותר, וגם בו מתקיים משפט קומפקטיות דומה (שהוכחתו מסובכת יותר, כצפוי).

דוגמה: צביעה של גרפים **גרף** הוא זוג סדור $G=(V,E)$ כאשר V קבוצה כלשהי שאבריה נקראים **צמתי** הגרף ו־$E\subseteq V^{2}$ היא קבוצה כלשהי שאיבריה נקראים **קשתות** הגרף. **צביעה** ב־n צבעים של הגרף היא פונקציה $f:V\to\{1,2,\dots,n\}$ והיא **חוקית** אם לכל $(u,v)\in E$ מתקיים $f(u)\neq f(v)$. אם קיימת לגרף צביעה חוקית ב־n צבעים אז אומרים שהוא n**־צביע**.

תת־גרף מושרה של G הוא גרף $G'=(V',E')$ כך ש־$V'\subseteq V$ ו־$E'=\{(u,v)\in E|u,v\in V'\}$.

טענה 5.47 אם G הוא גרף כך ש־V בת מניה, אז G הוא n־צביע אם ורק אם כל תת־גרף מושרה שלו הוא n צביע.

הוכחה: לכל $v\in V$ נתאים משתנים $X_{1}^{v},\dots,X_{n}^{v}$ (מכיוון ש־V בת מניה אנו נזקקים רק למספר בן מניה של משתנים ולכן קיימת התאמה חח"ע ועל בין קבוצת המשתנים $p_{1},p_{2},\dots$ וקבוצה זו). אנו רוצים לחשוב על X_{i}^{v} כאומר האם הצומת v נצבע בצבע i.

כעת, לכל $v\in V$ נגדיר פסוק $\varphi_{v}=\bigvee X_{i}^{v}\wedge\bigwedge_{i\neq j}\left(\neg X_{i}^{v}\vee X_{j}^{v}\right)$. הפסוק מסתפק אם ורק אם בדיוק אחד מהמשתנים $X_{1}^{v},\dots,X_{n}^{v}$ קיבל ערך $\mathbf{T}$, ולכן בהינתן השמה למשתנים X_{i}^{v} היא מגדירה פונקציה $f:V\to\{1,\dots,n\}$ על ידי כך ש־$f(v)$ מוגדר להיות ה־i היחיד עבורו $X_{i}^{v}=\mathbf{T}$ בהשמה.

בנוסף, לכל קשת $e=(u,v)\in E$ נגדיר את הפסוק $\varphi_{e}=\bigwedge\neg\left(X_{i}^{v}\wedge X_{i}^{u}\right)$ שמבטיח שלכל צבע i, לא מתקיים שגם u וגם v נצבעו ב־i גם יחד.

כעת נגדיר קבוצת פסוקים $\Phi_{G}=\bigcup_{v\in V}\{\varphi_{v}\}\cup\bigcup_{e\in E}\{\varphi_{e}\}$. בבירור Φ_{G} ספיקה אם ורק אם G הוא n־צביע. אם G' הוא תת־גרף מושרה סופי של G אז בפרט $\Phi_{G'}$ סופית, ואם $\Phi'\subseteq\Phi$ היא סופית אז קיים תת־גרף מושרה סופי G' כך ש־$\Phi'\subseteq\Phi_{G'}$, ולכן התוצאה נובעת ממשפט הקומפקטיות. ■

5.8 גדירות בתחשיב הפסוקים

הבה ונחזור על הרעיונות המרכזיים בדוגמה שראינו ליישום משפט הקומפקטיות על n־צביעה של גרפים: בהינתן גרף G, פירשנו את המשתנים של תחשיב הפסוקים באופן כזה שבו הייתה לנו התאמה חח"ע ועל בין קבוצת ה**השמות** למשתנים ובין קבוצת ה**צביעות** של הגרף. לאחר מכן בנינו קבוצת פסוקים Φ_{G} באופן חכם כך שיתקיים שהשמה היא מודל של Φ_{G} אם ורק אם הצביעה המתאימה לה היא צביעה חוקית. במילים אחרות, קבוצת כל המודלים של Φ_{G} היא בדיוק קבוצת כל הצביעות החוקיות של G. ניתן לחשוב על כך כאילו קבוצת הנוסחאות Φ_{G} **הגדירה** את קבוצת הצביעות החוקיות של G.

זה מוביל אותנו להגדרה הכללית הבאה:

הגדרה 5.48 תהא Φ קבוצת פסוקים. נגדיר $M(\Phi) \triangleq \{Z | Z \models \Phi\}$ ־ קבוצת ההשמות שהן מודל ל־Φ. אם עבור קבוצת השמות כלשהי K קיימת קבוצת פסוקים Φ כך ש־$K = M(\Phi)$ אומרים ש־K היא **גדירה** (ניתנת להגדרה). אם Φ סופית ו־$K = M(\Phi)$ אז אומרים על K שהיא **גדירה באופן סופי**.

אבחנה ראשונה ופשוטה היא שקיימות קבוצות לא גדירות, ואפילו רוב קבוצות ההשמות אינן גדירות. כדי לראות זאת, נשים לב לכך שיש $\aleph_0$ משתנים בתחשיב הפסוקים, ולכן $2^{\aleph_0}$ השמות, ולכן $2^{\left(2^{\aleph_0}\right)}$ קבוצות של השמות; מצד שני, יש רק $\aleph_0$ פסוקים ולכן $2^{\aleph_0} < 2^{\left(2^{\aleph_0}\right)}$ קבוצות של פסוקים.

נעבור, אם כן, להצגת כמה קבוצות שהן **כן** גדירות:

1. קבוצת כל ההשמות גדירה על ידי $\Phi = \emptyset$.
2. $\emptyset$ גדירה על ידי $\Phi = \{X \wedge \neg X\}$. היא גדירה גם על ידי $\Phi = \mathrm{WFF}$, מה שמשמר את הדואליות עם הדוגמה הקודמת.
3. לכל השמה Z, הקבוצה $\{Z\}$ גדירה על ידי $\Phi = \{p_i | Z(p_i) = \mathbf{T}\} \cup \{\neg p_i | Z(p_i) = \mathbf{F}\}$ (ברור כי $Z \models \Phi$, והיחידות של Z מוכחת באופן דומה להוכחה במהלך הוכחת משפט השלמות שלתורה שלמה יש מודל יחיד).
4. השמה **מונוטונית** היא כזו שבה לכל $i < j$ מתקיים $Z(p_i) \le Z(p_j)$ כאשר אנו מגדירים $\mathbf{F} < \mathbf{T}$. קבוצת ההשמות המונוטוניות גדירה על ידי $\Phi = \bigcup_{i<j} \{p_i \to p_j\} = \bigcup_{i<j} \{p_j \vee \neg p_i\}$.
5. קבוצת כל ההשמות Z אשר נותנות ערך $\mathbf{T}$ לכל היותר למשתנה אחד גדירה על ידי $\Phi = \bigcup_{i \neq, j} \{\neg(p_i \wedge p_j)\}$.

את הדוגמה האחרונה ניתן להרחיב גם לקבוצת כל ההשמות אשר נותנות ערך $\mathbf{T}$ לכל היותר ל־n משתנים, וזאת עבור כל n: במקום לרוץ על זוגות, רצים על n־יות של משתנים ואוסרים על כולם להסתפק בו זמנית.

עם זאת, שינוי קטן בניסוח יניב לנו דוגמה קונקרטית ראשונה לקבוצה שאינה גדירה: קבוצת כל ההשמות Z אשר נותנות ערך $\mathbf{T}$ לכל היותר למספר סופי של משתנים (או בניסוח שקול, נותנות ערך $\mathbf{F}$ לכמעט כל המשתנים) איננה גדירה. לפני שנוכיח זאת, נראה טענת עזר שימושית שמצביעה במפורש על הדואליות שיש בין קבוצות של השמות וקבוצות של פסוקים:

טענה 5.49 עבור קבוצות פסוקים כלשהן A, B מתקיים $M(A \cup B) = M(A) \cap M(B)$.

הוכחה: תהא Z השמה כלשהי, אז:

$$\begin{aligned} Z \in M(A \cup B) &\iff Z \models A \cup B \\ &\iff Z \models A \wedge Z \models B \\ &\iff Z \in M(A) \wedge Z \in M(B) \\ &\iff Z \in M(A) \cap M(B) \end{aligned}$$

■

הטענה הדואלית, $M(A \cap B) = M(A) \cup M(B)$ היא שגויה; דוגמה נגדית פשוטה היא $A = \{p_1 \wedge p_2\}, B = \{\neg p_1 \wedge \neg p_2\}$. כאן $M(A \cap B) = M(\emptyset)$, כלומר קבוצת כל ההשמות; אך $M(A) \cup M(B)$ היא קבוצת כל ההשמות שבהן $Z(p_1) = Z(p_2)$, השונה מקבוצת כל ההשמות.

נוכיח כעת כי אם K היא קבוצת כל ההשמות אשר נותנות ערך $\mathbf{T}$ למספר סופי של משתנים אז K אינה גדירה. נניח בשלילה כי K גדירה, אז קיימת קבוצת פסוקים A כך ש־$K = M(A)$. נגדיר $B = \{p_0, p_1, p_2, \dots\}$ ־ קבוצת כל הפסוקים שכוללים משתנה ותו לא. אז $M(A \cup B) = M(A) \cap M(B) = K \cap M(B) = \emptyset$ שכן $M(B)$ כוללת השמה אחת ויחידה ־ זו שנותנת $\mathbf{T}$ לכל המשתנים, ועל פי הגדרת K השמה זו אינה ב־K.

מצד שני, נוכיח כעת כי $M(A \cup B) \neq \emptyset$ ונגיע לסתירה. את משפט הקומפקטיות לתחשיב הפסוקים ניתן לנסח גם כך: לכל קבוצה X של פסוקים, $M(X) \neq \emptyset$ אם ורק אם $M(X') \neq \emptyset$ לכל תת־קבוצה סופית $X' \subseteq X$. תהא $C \subseteq A \cup B$ תת־קבוצה סופית; נתבונן בהשמה שנותנת ערכי $\mathbf{T}$ לכל המשתנים שמופיעים כפסוקים אטומיים ב־C, וערך $\mathbf{F}$ ליתר המשתנים. מכיוון ש־C סופית, השמה זו נותנת ערך $\mathbf{T}$ רק למספר סופי של משתנים ולכן היא בפרט שייכת ל־$M(A)$ ומכאן בפרט שהיא מספקת כל נוסחה ב־A. מכאן שהיא מספקת כל נוסחה ב־C (כי בנינו אותה כדי לספק את כל נוסחאות B שנמצאות ב־C) ולכן $M(C) \neq \emptyset$, כמבוקש.

דוגמה זו ממחישה שיטה כללית להוכחה שקבוצות K של השמות אינן גדירות:

1. מניחים בשלילה ש־K גדירה על ידי קבוצת פסוקים A.

2. מוצאים קבוצת פסוקים B כך ש־$M(A)\cap M(B)=\emptyset$ (ומוכיחים זאת).

3. מסיקים כי $M(A\cup B)=\emptyset$.

4. מוכיחים כי $M(A\cup B)\neq\emptyset$ על ידי הוכחה כי $M(C)\neq\emptyset$ לכל תת קבוצה סופית $C\subseteq A\cup B$.

5. מ־3 ו־4 מקבלים סתירה ולכן הנחת השלילה של 1 אינה נכונה.

נציג דוגמה נוספת: נוכיח כי אם K היא קבוצת כל ההשמות אשר קיים משתנה שהן נותנות לו $\mathbf{T}$ וקיים משתנה שהן נותנות לו $\mathbf{F}$, אז K אינה גדירה (שימו לב כי K היא בעצם קבוצת כל ההשמות למעט שתיים).

נניח בשלילה ש־K גדירה על ידי קבוצת פסוקים A, ונגדיר קבוצת פסוקים $B=\{p_0,p_1,p_2,\dots\}$. אז $M(B)$ כוללת רק את ההשמה שנותנת $\mathbf{T}$ לכל המשתנים ולכן $M(A\cup B)=M(A)\cap M(B)=\emptyset$. מצד שני, כל תת־קבוצה סופית $C\subseteq A\cup B$ ספיקה על ידי השמה שנותנת $\mathbf{T}$ לכל המשתנים שהפסוק האטומי שלהם מופיע ב־C (ואם אין כאלו, אז נותנת $\mathbf{T}$ ל־p_0) ונותנת $\mathbf{F}$ למשתנה כלשהו שהפסוק האטומי שלו לא הופיע (קיים כזה כי C סופית), ולכן $M(C)\neq\emptyset$ ומקומפקטיות נובע ש־$M(A\cup B)\neq\emptyset$.

נציג כעת דוגמה מעט יותר קונקרטית. ניתן לחשוב על כל השמה Z כמייצגת מספר ממשי בקטע $[0,1]$ בייצוג בינארי, $0.a_0a_1a_2,\dots$ כאשר

$$a_i \quad = \quad \begin{cases}1 & Z(p_i)=\mathbf{T}\\ 0 & Z(p_i)=\mathbf{F}\end{cases}$$

כזכור, מספר הוא **רציונלי** אם החל ממקום כלשהו הוא מחזורי, כלומר קיים N ו־t כך שלכל $i>N$ מתקיים $a_i=a_{i+t}$.

נוכיח כי קבוצת ההשמות שמייצגות מספרים רציונליים אינה גדירה. לצורך כך ננקוט שוב בשיטה הכללית שהצגנו, כאשר B תיבנה באופן כזה ש־$M(B)$ תכלול השמה יחידה, אשר מייצגת את המספר $a=0.010011000111\dots$, כלומר מספר שמורכב בתחילה ממופע אחד של 0 ואז מופע אחד של 1, ולאחר מכן שני מופעים של 0 ושני מופעים של 1, וכן הלאה. בבירור מספר זה אינו רציונלי. B פשוט תוגדר באמצעות פסוקים אטומיים או שלילתם כדי להבטיח שתגדיר את a, כלומר אם $a_i=1$ אז $p_i\in B$ ואילו אם $a_i=0$ אז $\neg p_i\in B$.

כעת, כל תת־קבוצה סופית $C\subseteq A\cap B$ כוללת רק מספר סופי של פסוקים מ־B והם קובעים רק את ההתנהגות של קבוצה סופית של ספרות במספרים שמיוצגים על ידי אברי $M(C)$; לכן כל מספר רציונלי בתחום $[0,1]$ שבו המחזוריות מתחילה רק אחרי הספרות שמתאימות לפסוקי B יהיה שייך ל־C, כלומר $M(C)\neq\emptyset$.

כעת נראה מקום נוסף שבו משפט הקומפקטיות מסייע לנו בהקשר של גדירות - אפיון נוסף של גדירות סופית.

משפט 5.50 (אפיון שקול לגדירות סופית) תהא K קבוצת השמות כלשהי. התנאים הבאים שקולים:

1. K גדירה וגם $\overline{K}$ (המשלימה של K ביחס לקבוצת כל ההשמות) גדירה.

2. K גדירה באופן סופי.

3. קיים פסוק φ כך ש־$K=M(\{\varphi\})$

הוכחה: הגרירה המסובכת היא מ־1 אל 2. נטפל ראשית כל באחרות.

אם K גדירה באופן סופי אז $K=M(\{\varphi_1,\dots,\varphi_n\})$ וקל לראות כי $K=M(\{\varphi\})$ כאשר $\varphi=\varphi_1\wedge\dots\wedge\varphi_n$ (מכיוון שיש רק מספר סופי של פסוקים $\varphi_1,\dots,\varphi_n$ הרי ש־φ הוא מאורך סופי ולכן פסוק חוקי). מכאן ש־2 גורר את 3.

אם קיים φ כך ש־$K=M(\{\varphi\})$ קל לראות כי $\overline{K}=M(\{\neg\varphi\})$ ומכאן ש־3 גורר את 1.

נניח כעת כי K גדירה וגם $\overline{K}$ גדירה. נסמן $K=M(\Phi)$ ו־$\overline{K}=\{\Psi\}$. אז $M(\Phi\cup\Psi)=M(\Phi)\cap M(\Psi)=K\cap\overline{K}=\emptyset$. דהיינו, הקבוצה אינה ספיקה. ממשפט הקומפקטיות נובע שקיימת תת־קבוצה סופית $\Sigma\subseteq\Phi\cup\Psi$ שאיננה ספיקה. נסמן $\Sigma'=\Sigma\cap\Phi$. אם נראה כי $M(\Sigma')=K$ סיימנו.

מצד אחד, $\Sigma'\subseteq\Phi$ ולכן $M(\Sigma')\supseteq M(\Phi)=K$ (כי כל השמה שמספקת את Φ מספקת בפרט את Σ').

נותר להראות כי $M(\Sigma')\subseteq K$, או באופן שקול, כי $M(\Sigma')\cap\overline{K}=\emptyset$.

כעת, $M(\Sigma'\cup\Psi)=M(\Sigma')\cap M(\Psi)=M(\Sigma')\cap\overline{K}$. אנו נראה ש־$\Sigma\subseteq\Sigma'\cup\Psi$ ובכך נסיים, שכן Σ אינה ספיקה ולכן כך גם כל קבוצה שמכילה אותה.

על פי ההגדרה: $\Sigma'\cup\Psi=(\Sigma\cap\Phi)\cup\Psi=(\Sigma\cup\Psi)\cap(\Phi\cup\Psi)\supseteq\Sigma\cap\Sigma=\Sigma$, וסיימנו. ■

6 תחשיב היחסים

6.1 מבוא

תחשיב הפסוקים הוא אמנם פשוט ואינטואיטיבי, אבל כוח ההבעה שלו מוגבל עד מאוד. כדי לראות זאת נתבונן בדוגמה קלאסית שלקוחה מטיעון של אריסטו:

1. כל בני האדם הם בני תמותה.
2. סוקרטס הוא בן אדם.
3. מכאן שסוקרטס הוא בן תמותה.

במבט ראשון אולי נדמה שיש לנו כאן טיעון MP סטנדרטי, אך לא כך הדבר. לב הבעיה היא בכך שביטוי כמו "כל בני האדם הם בני תמותה" הוא ביטוי אטומי בתחשיב הפסוקים; הוא יכול לקבל ערך "אמת" או "שקר" אך אי אפשר לפרק אותו הלאה מבלי לפגוע במשמעותו. לכל היותר ניתן לסמן אותו ב־X, את "סוקרטס הוא בן אדם" ב־Y ואת "סוקרטס הוא בן תמותה" ב־Z ולכתוב את הפסוק $X \wedge Y \rightarrow Z$ ("אם כל בני האדם הם בני תמותה וסוקרטס הוא בן אדם אז סוקרטס הוא בן תמותה") אבל פסוק זה אינו טאוטולוגיה כלל ולכן לא ניתן להוכיח אותו ללא הנחות נוספות, בעוד שתחושתנו היא שהטיעון יישאר תקף בלי תלות במה שנכתוב במקום "בני אדם", "בני תמותה" ו"סוקרטס". שימו לב שאת ה"כל" דווקא איננו יכולים להחליף (אם נחליף את "כל" ב"חלק", הטיעון יאבד את תוקפו) ולכן "כל" צריך להיות חלק מ**השפה** עצמה.

כמו כן, במשפט "כל בני האדם הם בני תמותה" מעורבים במובהק שני רכיבים שונים ־ "בני אדם" ו"בני תמותה", והמשפט קושר ביניהם באופן שלא ברור איך לבצע בתחשיב הפסוקים. נראה שאנחנו צריכים להעשיר את השפה שלנו על ידי הוספת **תכונות** שמשתנים יכולים לקבל. במקום שמשתנה X יקבל רק ערך $\mathbf{T}$ או $\mathbf{F}$, אנו רוצים שאפשר יהיה לבדוק "האם X הוא בן אדם? האם X הוא בן תמותה?" וכדומה.

נעבור לדוגמה נוספת. אחת מההנחות הבסיסיות בתורת הקבוצות היא קיומה של קבוצה ריקה. כיצד ניתן לנסח את המשפט "קיימת קבוצה ריקה" באופן פורמלי? הניסוח יהיה בסגנון "קיימת קבוצה A כך שלכל איבר a, a אינו שייך לקבוצה A". שימו לב לרכיבי המשפט ־ "קיימת", "לכל", ו"שייך". בפרט, "שייך" הוא דוגמה נוספת ל**תכונה**, רק שכעת זוהי תכונה שמתקיימת על ידי זוגות של איברים ולא איברים בודדים. מכאן שאנחנו רוצים להיות מסוגלים לתאר בשפה שלנו **יחסים** באופן כללי; מכאן מגיע השם "תחשיב היחסים" (או "הפרדיקטים" בלועזית).

התחביר של תחשיב היחסים כולל את הרכיבים של תחשיב הפסוקים ־ משתנים $v_0, v_1, v_2, v_3, \ldots$ (הסימון שונה כדי להבדיל אותנו מתחשיב הפסוקים), והסימנים הלוגיים $\rightarrow, \neg, \wedge, \vee$ שמורכבים לכדי פסוקים והקריאה היחידה שלהם מובטחת על ידי שימוש נכון בסוגריים. עם זאת, התחביר של תחשיב היחסים מרחיב מאוד את תחביר תחשיב הפסוקים כדי להגדיל משמעותית את יכולת ההבעה שלנו:

1. לשפה נוספים **הסימנים הלוגיים** $\exists, \forall$ שמייצגים את "קיים" ($\exists$ הוא מעין E הפוכה, מלשון Exists) ו"לכל" ($\forall$ הוא מעין A הפוכה, מלשון All).
2. לשפה נוספים **סימני יחס** שמאפשרים לתאר יחסים כמו "x הוא בן אדם", "x שייך ל־y" וכדומה. יש גם סימן יחס מיוחד, $\approx$, שנמצא בכל שפה ומשמעותו היא תמיד שוויון.
3. לשפה נוספים **סימני קבועים** שמאפשרים לדבר על אובייקטים קונקרטיים (למשל 0 או הקבוצה הריקה).
4. לשפה נוספים **סימני פונקציה** שמאפשרים לתאר בניה של אובייקטים מתוך אובייקטים אחרים (למשל סימנים לחיבור או כפל).

אם אנו מעוניינים לתאר את תורת הקבוצות, אנו נזקקים לסימן יחס יחיד ־ $\in$ ־ ותו לא. לעומת זאת, אם אנו מעוניינים לתאר את המספרים הטבעיים אנו נזקקים לסימני הפונקציה S, $+, -$ (כאשר S היא פונקציית העוקב), כמו גם לסימן הקבוע 0. כפי שניתן לשער, הסימנים שאנו זקוקים להם תלויים בשאלה מה אנחנו בדיוק מנסים לתאר. על כן, בניגוד לתחשיב הפסוקים, בתחשיב היחסים אין לנו שפה אחת ויחידה אלא מגוון רב של שפות, כאשר כל שפה כוללת את הסימנים הלוגיים הרגילים בתוספת $\exists, \forall$ ואינסוף משתנים, אך בנוסף לכך כל שפה מאופיינת על ידי **מילון** שכולל את סימני היחס, הקבועים והפונקציות שבהם ניתן להשתמש בשפה זו.

לשפות שאנחנו נבנה במסגרת התחביר של תחשיב היחסים קוראים **שפות מסדר ראשון** ולתחשיב היחסים שנציג קוראים לעתים **לוגיקה מסדר ראשון** (First order logic ־ FOL). כפי שניתן לשער, קיימות גם שפות מסדרים גבוהים יותר ותחשיב יחסים לסדרים גבוהים יותר, אך לא נעסוק בהם כאן; נסביר את ההבדל הטכני (ואת הסיבה שבגללה אנו עוסקים בשפות מסדר ראשון דווקא) בהמשך.

הבדל משמעותי עוד יותר בין תחשיב הפסוקים ותחשיב היחסים הוא ב**סמנטיקה**. בעוד שבתחשיב הפסוקים, הסמנטיקה כללה השמה של ערכי אמת למשתנים ותו לא, בתחשיב היחסים הסיטואציה מורכבת פי כמה וכמה. כל פירוש אפשרי לשפה של תחשיב היחסים כולל **מבנה** שמורכב מקבוצה X כלשהי של איברים, קבוצה של יחסים על X שמתאימים לסימני היחס בשפה, התאמה של איבר מ־X לכל אחד מסימני הקבועים, וקבוצה של פונקציות על X שמתאימות לסימני הפונקציות בשפה. הכמתים $\forall,\exists$ מתייחסים לאיברים שנלקחים **מתוך** X (כלומר, $\forall x$ פירושו "לכל האיברים ב־X" ו־$\exists x$ פירושו "קיים ב־X"), ובפרט כעת המשתנים לא מקבלים ערכי $\mathbf{T},\mathbf{F}$ בהכרח אלא איברים כלשהם ב־X.

כך למשל ניתן להגדיר שפה שמתאימה לתיאור של שדות, ולכתוב קבוצת פסוקים שמתאימה לאקסיומות השדה. דוגמאות למבנים שיספקו את קבוצות הפסוקים הללו הן המספרים הרציונליים $\mathbb{Q}$; המספרים הממשיים $\mathbb{R}$; שדה המספרים השלמים מודולו ראשוני p, $\mathbb{Z}_p$ ועוד. בתחשיב היחסים, **מודל** לתורה איננו סתם השמה שמספקת את כל פסוקי התורה, אלא **אובייקט מתמטי כלשהו** שמתאים לתיאור שהתורה מספקת. בשל כך, לתורות בתחשיב היחסים יכולים להיות מודלים רבים ושונים אלו מאלו בצורות מהותיות, מה שמצריך שימוש במושגים חדשים לזיהוי מודלים שהם "שונים אבל בעצם אותו הדבר" דוגמת **איזומורפיזם** של מודלים ("המודלים הם אותו דבר") **ושקילות אלמנטרית** של מודלים ("השפה שלנו לא מסוגלת להבדיל בין המודלים").

הטיפול הבסיסי בתחשיב היחסים דומה באופיו לטיפול בתחשיב הפסוקים: מתחילים בהגדרה מדוייקת של **התחביר** (סימנים לוגיים, מילונים, האופן שבו הם מורכבים לכדי נוסחאות חוקיות); עוברים להגדרה של **הסמנטיקה** (מבנים והאופן שבו הם מגדירים ערכי אמת לפסוקים), ולאחר מכן מציגים **מערכת הוכחה** לתחשיב היחסים ומוכיחים כי היא מקיימת **שלמות ונאותות**. כמו בתחשיב הפסוקים ישנן מערכות הוכחה אפשריות רבות; הוכחת השלמות בדרך כלל מתבססת, בדומה לזו של תחשיב הפסוקים, על הוכחה שלכל תורה (קבוצה עקבית של פסוקים) קיים מודל; באופן לא מפתיע, זוהי הוכחה קשה יותר מאשר ההוכחה עבור תחשיב הפסוקים (בפרט, בניית המודל מצריכה כעת יותר מאשר השמה של ערכי אמת למשתנים ־ יש להגדיר קבוצה X עם יחסים ופונקציות וקבועים מתאימים).

משפט השלמות לתחשיב היחסים מכונה **משפט השלמות של גדל** על שם המתמטיקאי קורט גדל שהוכיח אותו לראשונה (ההוכחה הפופולרית יותר בספרות היא ההוכחה המאוחרת יותר של הנקין). לאחר משפט השלמות של גדל נהוג לעבור לטיפול במשפטי **אי השלמות** של גדל. בעוד שמשפט השלמות של גדל מראה כי קיימת לתחשיב היחסים מערכת הוכחה שלמה ונאותה, משפטי אי השלמות עוסקים ספציפית ב**תורות** שמתארות (אולי בין היתר) את המספרים הטבעיים עם פעולות החיבור והכפל. גדל הראה שעבור תורות כאלו, אם ניתן לבדוק אלגוריתמית האם פסוק הוא אקסיומה של התורה או לא (התורה **אפקטיבית**) אז התורה איננה תורה שלמה, כלומר קיימים פסוקים שאינם ניתנים להוכחה או הפרכה ממנה (ובאופן שקול, קיימים לתורה שני מודלים שאינם שקולים). מתוצאה זו (**משפט אי השלמות הראשון של גדל**) נובע שהאריתמטיקה אינה יכולה להוכיח את העקביות שלה עצמה (**משפט אי השלמות השני של גדל**) משפטי אי השלמות של גדל מצביעים על בעיה משמעותית בכל נסיון לביצוע אקסיומטיזציה אפקטיבית של כל המתמטיקה (שכן אקסיומטיזציה כזו בפרט תכלול את האריתמטיקה ולכן תהיה חשופה למשפטי אי השלמות של גדל). לרוע המזל, משפטי אי השלמות מתוארים לעתים בספרות פופולרית בצורות שגויות ("קיימים משפטים שאינם ניתנים להוכחה", "לכל מערכת חייב להיות צופה חיצוני", "האדם נעלה על המחשב", "מתמטיקאים לא יודעים הכל" ועוד כהנה וכהנה ניסוחים ומסקנות שהקשר בינם ובין תוכנו האמיתי של המשפט הוא קלוש). פרט לעניין המתמטי שמהווה **תוצאת** משפטי אי השלמות, יש גם עניין לא מבוטל ב**הוכחה** של גדל, שמשלבת מספר רעיונות מבריקים (של גאורג קנטור ושל גדל עצמו) והשפיעה בצורה חזקה מאוד על התפתחותם של מדעי המחשב.

מפאת קוצר הזמן, בקורס זה לא נוכל להציג בצורה מדויקת את משפטי השלמות או את משפטי אי־השלמות.

6.2 התחביר של תחשיב היחסים

ההגדרת הפורמלית של אוסף הנוסחאות הבנויות היטב של תחשיב היחסים דומה לזו של תחשיב הפסוקים, בהבדל משמעותי אחד: בתחשיב היחסים ישנן שפות רבות, שכל אחת מאופיינת על ידי **מילון** שמגדיר מהם הסימנים הלא־לוגיים שנמצאים בשפה:

הגדרה 6.1 מילון τ עבור שפה מסדר ראשון כולל קבוצה (ריקה, סופית או אינסופית) של **סימני קבועים** $\{c_i|i\in I\}$ (I היא קבוצת אינדקסים) ולכל $n>0$ טבעי חיובי קבוצה של **סימני פונקציה** על n משתנים $\{f_i^n|i\in J_n\}$ **וסימני יחס** על n איברים $\{R_i^n|i\in K_n\}$. אברי קבוצות המילון נקראים "סימנים לא לוגיים".

לרוב יהיה נוח לכתוב את המילון פשוט בתור $\tau=(R_1,R_2,\ldots,f_1,f_2,\ldots,c_1,c_2,\ldots)$ מבלי לציין במפורש את מספר המשתנים שמתאימים לכל יחס ולכל סימן פונקציה ותוך הנחה שיש לכל היותר מספר בן מניה של סימנים מכל סוג (לא נעסוק בשפות שבהן זה לא כך).

הגדרה 6.2 שפה מסדר ראשון כוללת מילון כלשהו עבור שפה מסדר ראשון, וכמו כן קבוצה של **סימנים לוגיים** הכוללת סדרה אינסופית של משתנים $v_0,v_1,v_2,v_3,\ldots$ ואת הסימנים $\neg,\vee\wedge,\rightarrow,\leftrightarrow,\exists,\forall,(,),\approx$ והסימן , (פסיק). **נוסחה** (לאו דווקא בנויה היטב) בשפה היא סדרה **סופית** של סימנים (לוגיים או לא לוגיים) מתוך השפה.

בהערת אגב נציין שקיימים רבים אשר מגדירים שפות מסדר ראשון ללא הכנסתו המפורשת של סימן השוויון $\approx$, אך לרוב נוח (ולא מפריע) להוסיף גם אותו להגדרה (מאוחר יותר, כאשר נגדיר את הסמנטיקה של תחשיב היחסים נצטרך להתייחס אליו במיוחד).

ניתן כעת להגדיר את WFF באינדוקציית מבנה כמו בתחשיב הפסוקים, אבל מבחינה רעיונית כדאי להגדיר קודם קבוצה מובחנת של סימנים: **שמות העצם**. בניסוח אינטואיטיבי, שם עצם הוא כל רצף סימנים שבפרשנות של הפסוק יותאם לאיבר ספציפי מתחום הפרשנות.

הגדרה 6.3 קבוצת **שמות העצם** (Terms) של שפה מסדר ראשון מוגדרת באינדוקציית מבנה בתור $\mathrm{T}=X_{B,F}$ כאשר $B=\{c_i|i\in I\}\cup\{v_0,v_1,v_2,\dots\}$ (סימני הקבועים והמשתנים) ו־$F=\{F_i^n|n\in\mathbb{N},i\in J_n\}$ כך ש־$F_i^n(t_1,\dots,t_n)=f_i^n(t_1,\dots,t_n)$ (כאן $f_i(t_1,\dots,t_n)$ היא **מחרוזת** שמתחילה בסימן f_i^n, לאחר מכן סוגר שמאלי, לאחר מכן המחרוזות המתאימות לשמות העצם $t_1,\dots,t_n$ כשהן מופרדות בפסיקים, ולבסוף סוגר ימני.

נתבונן במספר דוגמאות מציאותיות:

1. בשפה מסדר ראשון של המספרים הטבעיים קיים סימן הפונקציה $S(x)$ שמשמעותו "עוקב" וסימן הקבוע 0. שמות העצם בשפה זו הם מהצורה $S(S(S(\dots S(x_i))))$ ו־$S(S(S(\dots S(0))))$. לצורך פשטות נהוג לסמן S^k כדי לתאר הפעלה של S במשך k פעמים (אבל חשוב לשים לב שזהו קיצור **לא פורמלי**; אין משמעות ל"S בחזקת k" כמחרוזת פורמלית), ופישוט נוסף הוא להשתמש בסימון $k\triangleq S^k(0)$ (ושוב, זהו סימון **לא פורמלי**; אין סימני קבועים $1,2,3,\dots$ בשפה אלא רק סימן קבוע יחיד, 0).

2. בשפה מסדר ראשון של שדות סדורים קיימים סימני הקבועים 0 ו־1, וסימני הפונקציה $+,\cdot$. דוגמה לשם עצם בשפה זו: $\cdot(+(0,1),v_5)$. סימון מקובל לפונקציות של שפה זו הוא כתיבת $+(t_1,t_2)$ בתור t_1+t_2 ו־$\cdot(t_1,t_2)=t_1+t_2$, כך ש־$\times(+(0,1),v_5)$ ייכתב כ־$(0+1)\cdot v_5$, אך חשוב לזכור כי זהו סימון **לא פורמלי**.

באופן לא מפתיע, שמות עצם מקיימים **משפט קריאה יחידה**: בהינתן שם עצם, יש דרך יחידה לפרק אותו למרכיביו. ההוכחה אינה שונה מהותית מההוכחה שראינו בתחשיב הפסוקים ולא נציג אותה כאן.

משהגדרנו שמות עצם, ניתן לעבור להגדרה של נוסחאות בנויות היטב:

הגדרה 6.4 בהינתן שפה מסדר ראשון L הקבוצה WFF עבור L מוגדרת באינדוקציית מבנה $\mathrm{WFF}=X_{B,F}$ כאשר $B=\{R_i^n(t_1,\dots,t_n)\mid n\ge1,i\in K_n,t_1,\dots,t_n\in\mathrm{T}\}\cup\{(t_1\approx t_2)\mid t_1,t_2\in\mathrm{T}\}$ כלומר, האטומים הם בדיוק סימני היחס ש"מופעלים" על שמות העצם, ו־$F=\{F_\vee,F_\wedge,F_\neg,F_\to,F_\leftrightarrow\}\cup\{F_\exists^{v_i},F_\forall^{v_i}|i\in\mathbb{N}\}$ כאשר $F_\vee,F_\wedge,F_\neg,F_\to,F_\leftrightarrow$ הן אותן פונקציות מתחשיב הפסוקים (למעט $F_\leftrightarrow(\alpha,\beta)=(\alpha\leftrightarrow\beta)$ שלא הזכרנו בתחשיב הפסוקים פשוט כי לא נזקקנו לה), ואילו $F_\exists^{v_i}(\alpha)=\exists v_i(\alpha)$ ו־$F_\forall^{v_i}(\alpha)=\forall v_i(\alpha)$.

גם לנוסחאות בנויות היטב קיים משפט קריאה יחידה, בדומה לתחשיב הפסוקים.

הגדרה 6.5 תורה מסדר ראשון מורכבת משפה מסדר ראשון L וקבוצת נוסחאות ב־WFF של L שנקראות **אקסיומות לא לוגיות** (כמובן, "לא לוגיות" כאן אין פירושו שהאקסיומות אינן הגיוניות, אלא שאלו אינן בהכרח טאוטולוגיות).

שימו לב שבניגוד לתחשיב הפסוקים, כאן איננו דורשים שקבוצת הנוסחאות תהיה עקבית כדי שתיקרא "תורה" (למעשה, טרם הגדרנו את מושג העקביות שכן לא הגדרנו מערכת הוכחה) וכי כאן השפה L היא חלק מהגדרת התורה.

כרגיל, כאשר אנו כותבים נוסחאות נשתמש בכתיבה לא פורמלית שבה אנו משמיטים סוגריים מיותרים, כותבים $a+b$ במקום $+(a,b)$ וכדומה, מתוך הנחה שהקורא יכול לבצע את התרגום חזרה לנוסחה פורמלית אם יהיה בכך צורך.

נעבור למספר דוגמאות:

תורת יחסי השקילות: השפה של תורת יחס השקילות כוללת סימן יחס יחיד $\sim$ ואין בה סימני פונקציות או קבועים (כלומר, המילון הוא $\tau=(\sim)$), והיא בעלת שלוש האקסיומות הבאות:

1. $\forall x(x\sim x)$ (רפלקסיביות)
2. $\forall x\forall y(x\sim y\to y\sim x)$ (סימטריה)
3. $\forall x\forall y\forall z((x\sim y\wedge y\sim z)\to x\sim z)$ (טרנזיטיביות)

תורת החבורות: השפה של תורת החבורות כוללת סימן פונקציה יחיד $\cdot$ וסימן קבוע יחיד e ($\tau = (\cdot, e)$), ואת האקסיומות הבאות:

1. $\forall x \forall y \forall z \left((x \cdot y) \cdot z \approx x \cdot (z \cdot y) \right)$ (אסוציאטיביות)
2. $\forall x \left(x \cdot e \approx x \wedge e \cdot x \approx x \right)$ (איבר יחידה)
3. $\forall x \exists y \left(x \cdot y \approx e \wedge y \cdot x \approx e \right)$ (איבר הופכי)

שימו לב שאין בתורה זו שום סימן יחס פרט ל־$\approx$, שנמצא "אוטומטית" בשפה.

תורת החבורות האבליות: השפה של תורת החבורות האבליות כוללת סימן פונקציה יחיד $+$ וסימן קבוע יחיד 0 ($\tau = (0, +)$) ואת האקסיומות הבאות:

1. $\forall x \forall y \forall z \left((x + y) + z \approx x + (z + y) \right)$ (אסוציאטיביות)
2. $\forall x \left(x + 0 \approx x \right)$ (איבר יחידה)
3. $\forall x \exists y \left(x + y \approx 0 \right)$ (איבר נגדי)
4. $\forall x \forall y \left(x + y \approx y + x \right)$ (אבליות)

זוהי למעשה תורת החבורות עם תוספת אקסיומה 4 ("אבליות") ופישוט קל של אקסיומות 2,3 שניתן לבצע בזכות האבליות; כמו כן, אנו משתמשים בסימון השונה $+$ במקום $\cdot$ ו־0 במקום e.

תורת החוגים עם יחידה: השפה של תורת החוגים עם יחידה כוללת שני סימני פונקציה, $+, \cdot$, שני סימני קבוע $0, 1$ ($\tau = (0, 1, +, \cdot)$), את כל האקסיומות של תורת החבורות האבליות ואת האקסיומות הנוספות הבאות:

1. $\forall x \forall y \forall z \left((x \cdot y) \cdot z \approx x \cdot (z \cdot y) \right)$ (אסוציאטיביות הכפל)
2. $\forall x \left(x \cdot 1 \approx x \wedge 1 \cdot x \approx x \right)$ (איבר יחידה כפלי)
3. $\forall x \forall y \forall z \left(x \cdot (y + z) \approx x \cdot y + x \cdot z \right)$ (דיסטריביוטיביות הכפל מעל החיבור משמאל)
4. $\forall x \forall y \forall z \left((y + z) \cdot x \approx y \cdot x + z \cdot x \right)$ (דיסטריביוטיביות הכפל מעל החיבור מימין)

שתי האקסיומות הראשונות מגיעות מתורת החבורות (עם 1 במקום e), אך שתי האקסיומות האחרונות הן חדשות. כדאי להעיר כי יש תורות חוגים שבהן אקסיומה 2 וסימן הקבוע 1 אינם קיימים כלל ("חוגים ללא יחידה"; מכיוון שחוגים נקראים Rings יש הקוראים לחוגים כאלו Rngs; מצד שני, רבים אלו אשר משתמשים ב־Rings כדי לתאר מראש חוגים ללא יחידה, כתלות בהקשר) ויש אפילו כאלו אשר משמיטים את אקסיומה 1.

תורת השדות: השפה של תורת השדות זהה לזו של תורת החוגים עם יחידה ומכילה את אותן אקסיומות, ובנוסף גם את האקסיומות הבאות:

1. $\forall x \forall y \left(x \cdot y \approx y \cdot x \right)$ (קומוטטיביות הכפל)
2. $\forall x \exists y \left(\neg (x \approx 0) \to (x \cdot y \approx 1) \right)$(קיום הופכי לכל איבר שונה מאפס)

תורת הגרפים המכוונים: השפה של תורת הגרפים המכוונים כוללת סימן יחס דו מקומי יחיד E, שום פונקציות, שום קבועים ושום אקסיומות ("אז מה הופך אותה לשפה של תורת הגרפים דווקא?")

תורת הגרפים הלא מכוונים הפשוטים: באופן מפתיע (או שלא?), לצורך תיאור גרפים לא מכוונים פשוטים אנו נזקקים דווקא לאקסיומות.

השפה של תורת הגרפים הלא מכוונים הפשוטים כוללת סימן יחס דו מקומי יחיד E, שום פונקציות, שום קבועים ואת האקסיומות:

1. $\forall x \forall y \left(E(x, y) \leftrightarrow E(y, x) \right)$ (קשת היא לא מכוונת)
2. $\forall x \left(\neg E(x, x) \right)$ (אין חוגים עצמיים)

אין צורך באקסיומה מפורשת עבור "אין קשתות מקבילות" שכן היחס E לא מאפשר זאת; כדי להגדיר תורת גרפים שמאפשרת קשתות מקבילות צריך להשתמש בתחביר שונה (בפרט, משתנים שייצגו גם קשתות).

תורת הקבוצות (ZFC): השפה של תורת הקבוצות כוללת את סימן היחס $\in$ ותו לא. מה שנציג אינו הגדרה מדויקת של ZFC: "נעגל פינות" פה ושם לצורך שיפור ההבנה.
האקסיומות הן:

1. $\forall A\forall B\left[\left(x\in A\leftrightarrow x\in B\right)\to A\approx B\right]$ (אקסיומת ההיקפיות - שתי קבוצות הן שוות אם יש להן אותם איברים)
2. $\exists y\left(\forall x\left(\neg x\in y\right)\right)$ (אקסיומת הקבוצה הריקה; קיימת קבוצה ללא איברים)
3. לכל פסוק $\varphi\left(x\right)$ עם משתנה x: $\forall A\exists B\left[\forall x\left(x\in B\iff x\in A\wedge\varphi\left(x\right)\right)\right]$ (תבנית אקסיומת ההפרדה: כל תת קבוצה של A קיימת)
4. $\forall x\forall y\exists A\left(x\in A\wedge y\in A\right)$ (אקסיומת הזיווג: אם x,y קיימים כך גם $\{x,y\}$, כתוצאה מאקסיומת ההפרדה ואקסיומה זו)
5. $\forall\mathcal{F}\exists U\forall a\left[a\in U\leftrightarrow\exists A\left(A\in\mathcal{F}\wedge a\in A\right)\right]$ (אקסיומת האיחוד: אם $\mathcal{F}$ היא משפחה של קבוצות אז $\bigcup\mathcal{F}$ קיימת)
6. $\forall A\exists\mathcal{P}\left[B\in\mathcal{P}\leftrightarrow\forall b\left(b\in B\to b\in A\right)\right]$ (אקסיומת קבוצת החזקה: אם A קבוצה אז 2^{A}, שמסומנת כאן $\mathcal{P}$, קיימת)
7. $\exists A\left[\emptyset\in A\wedge\forall x\left(x\in A\to x\cup\{x\}\in A\right)\right]$ (אקסיומת האינסוף: קיימת קבוצה אינדוקטיבית, כלומר שמכילה את כל הטבעיים. כאן $\emptyset$ ו־$x\cup\{x\}$ אינם חלק מהשפה אלא הם קיצורים של נוסחאות שמתארות קבוצות אלו במפורש)
8. $\forall A\left[A\neq\emptyset\to\exists x\left(x\in A\wedge x\cap A=\emptyset\right)\right]$ (אקסיומת הרגולריות: בכל קבוצה לא ריקה קיים איבר שזר לה. זה מבטיח בפרט שלא תהיה קבוצה שמכילה את עצמה או סדרת הכלות מוזרה כמו $A\in B\in A$)
9. לכל פסוק $\varphi\left(x,y\right)$ עם משתנים x,y: $\forall A\left[\forall x\left(x\in A\to\exists!y\varphi\left(x,y\right)\right)\to\exists B\forall x\left(x\in A\to\exists y\left(y\in B\wedge\varphi\left(x,y\right)\right)\right)\right]$ (אקסיומת ההחלפה: אם f פונקציה ו־A קבוצה אז הקבוצה $f\left(A\right)$ קיימת. כאן $\exists!$ פירושו "קיים ויחיד")
10. $\forall\mathcal{F}\exists f\forall A\left[\left(A\in\mathcal{F}\wedge A\neq\emptyset\right)\to f\left(A\right)\in A\right]$ (אקסיומת הבחירה: לכל משפחה $\mathcal{F}$של קבוצות קיימת פונקציה $f:\mathcal{F}\to\bigcup\mathcal{F}$ כך שלכל A לא ריקה ב־$\mathcal{F}$מתקיים $f\left(A\right)\in A$; כאן f מתארת פונקציה ואנו משמיטים את החלק באקסיומה שדורש זאת במפורש)

אקסיומות פיאנו: אקסיומות פיאנו מנסות למדל את המספרים הטבעיים. השפה כוללת את סימן הקבוע 0, את סימני הפונקציה $\cdot,+$ הבינאריים, סימן הפונקציה S ("עוקב") האונרי וסימן היחס $<$. האקסיומות הן:

1. $\forall x\left(\neg\left(S\left(x\right)\approx0\right)\right)$ (אין קודם לאפס)
2. $\forall x\forall y\left(S\left(x\right)\approx S\left(y\right)\to\left(x\approx y\right)\right)$ ("עוקב" הוא יחס חח"ע)
3. $\forall x\left(x+0\approx x\right)$ (0 הוא נייטרלי לחיבור; בסיס הגדרת החיבור)
4. $\forall x\forall y\left(x+S\left(y\right)\approx S\left(x+y\right)\right)$ (הגדרת החיבור, השלב הרקורסיבי)
5. $\forall x\left(x\cdot0\approx0\right)$ (בסיס הגדרת הכפל)
6. $\forall x\forall y\left(x\cdot S\left(y\right)\approx x\cdot y+x\right)$ (הגדרת הכפל, השלב הרקורסיבי)
7. $\forall x\left(\neg\left(x<0\right)\right)$ (0 הוא איבר מינימלי)
8. $\forall x\forall y\left(x<S\left(y\right)\leftrightarrow\left(x<y\vee x\approx y\right)\right)$ (הקשר בין יחס הסדר ופעולת העוקב)
9. $\forall x\forall y\left(x<y\vee x\approx y\vee x>y\right)$ (יחס הסדר הוא מלא)
10. $\varphi_{x}\left(0\right)\to\forall x\left(\varphi\to\varphi_{x}\left(S\left(x\right)\right)\right)\to\varphi$ (תבנית אקסיומת האינדוקציה)

האקסיומה האחרונה היא **תבנית אקסיומה** - קיימת אקסיומה אחת כזו לכל נוסחה בנויה היטב φ. כאשר $\varphi_{x}\left(a\right)$ מסמן את הנוסחה המתקבלת מ־φ על ידי החלפת x ב־a.

6.3 הסמנטיקה של תחשיב היחסים

כעת נסביר כיצד ניתן לתת ערך אמת לפסוק. נתחיל מדוגמה: נתבונן בתורת החבורות שהגדרנו קודם. היינו רוצים שכל חבורה תהיה מודל לתורה זו, ואובייקט שאיננו חבורה לא יהיה מודל. דוגמה נפוצה לחבורה היא $\mathbb{Z}$ עם פעולת החיבור $+$ ועם איבר היחידה 0; מה שאנו רוצים לומר הוא שהפעולה $+$ מתאימה לסימן הפונקציה $\cdot$ שבתורת החבורות, ושאיבר היחידה 0 מתאים לסימן הקבוע e.

עם זאת, $\mathbb{Z}$ עם פעולת הכפל $\cdot$ ו"איבר היחידה" 0 אינו מתאים לתורת החבורות שכן אקסיומה 2 אינה מתקיימת; כך למשל $1\cdot 0\neq 1$. אנחנו בעצם אומרים ש**תחת ההשמה** $x=1$, נקבל שהפסוק $x\cdot e=x\wedge e\cdot x=x$ אינו מתקיים.

אפשר לנסות לשנות זאת: המודל שלנו עדיין יהיה $\mathbb{Z}$ עם פעולת הכפל, אך איבר היחידה יהיה 1. במקרה זה, אקסיומה 3 לא תתקיים תחת ההשמה $x=2$; לכל y, לא יתקיים $x\cdot y=e\wedge y\cdot x=e$ שכן $2\cdot y\neq 1$ לכל y שלם.

מכאן ש־$\mathbb{Z}$ עם פעולת הכפל נכשל להיות מודל לתורת החבורות בשתי הפרשנויות של e להיות 0 ולהיות 1.

נסכם את הדיון האינטואיטיבי הזה: "מועמד" להיות מודל כולל קבוצה ($\mathbb{Z}$ בדוגמה) שמכונה "העולם", ובנוסף לכך **פרשנויות** לסימני היחסים, הפונקציות והקבועים שבשפה. העולם בתוספת פרשנויות אלו נקראת **מבנה** של השפה. לאחר שקבענו מבנה, ניתן לבדוק אם הוא מקיים נוסחה כלשהי או לא על ידי **הצבה בנוסחאות**; בהצבה כזו, לכל משתנה בנוסחה בוחרים איבר מתוך העולם של המבנה והבחירה הזו מניבה ערך אמת או שקר לנוסחה.

יש עוד נקודה שיש להתייחס אליה. לנוסחה כגון $x=x+x$ לא ברור אם יש ערך אמת או שקר, שכן קיימים x־ים עבורם תכונה זו מתקיימת, ו־x־ים עבורם תכונה זו אינה מתקיימת. לכן צריך להבהיר חד משמעית מה קורה במקרה של x־ים "ללא כמתים עליהם", ולצורך כך נזדקק להגדרות:

הגדרה 6.6 משתנה x הוא **חופשי** בנוסחה φ אם הוא אינו נופל תחת הטווח של כמת $\forall x$ או $\exists x$ (**הטווח** של הכמת הוא כל תת־הנוסחה שבסוגריים שאחרי הכמת). משתנה שאינו חופשי נקרא **קשור**.

נוסחה שאין בה משתנים חופשיים נקראת **פסוק** או **נוסחה סגורה**. נוסחה שאיננה סגורה נקראת **נוסחה פתוחה**.

לכל נוסחה φ, **הסגור** של φ הוא הפסוק $\forall x\forall y\dots\forall z\left(\varphi\right)$ כאשר $x,y,\dots,z$ הם כל המשתנים החופשיים ב־φ.

נוכל להגדיר ערך אמת לפסוקים; מכאן נרחיב אותו לנוסחאות באופן כללי על ידי הגדרת ערך האמת של נוסחה להיות ערך האמת של הסגור שלה.

נעבור כעת להגדרה המרכזית שלנו: **מבנה**.

הגדרה 6.7 תהא L שפה מסדר ראשון עם מילון τ. **מבנה** $\mathcal{M}$ עבור L מורכב מהחלקים הבאים:

- $D^{\mathcal{M}}$ - **התחום** ("העולם") - קבוצה לא ריקה.
- לכל סימן יחס $R_i\in\tau$ n־מקומי, תת־קבוצה $R_i^{\mathcal{M}}\subseteq\left(D^{\mathcal{M}}\right)^n$ (כלומר, יחס n־מקומי מעל $D^{\mathcal{M}}$).
- לכל סימן פונקציה $f_i\in\tau$ ב־n משתנים, פונקציה $f_i^{\mathcal{M}}:\left(D^{\mathcal{M}}\right)^n\to D^{\mathcal{M}}$ (כלומר, פונקציה ב־n משתנים מעל $D^{\mathcal{M}}$).
- לכל סימן קבוע $c_i\in\tau$, איבר $c_i^{\mathcal{M}}\in D^{\mathcal{M}}$.

מרגע שנקבע מבנה, אפשר להגדיר באמצעותו השמה:

הגדרה 6.8 השמה Z עבור מבנה $\mathcal{M}$ היא פונקציה $Z:\{v_0,v_1,\dots\}\to D^{\mathcal{M}}$.

ההשמה המורחבת $\overline{Z}$ מוגדרת על T באמצעות אינדוקציית מבנה: לכל משתנה v_i, $\overline{Z}\left(v_i\right)=Z\left(v_i\right)$ ולכל סימן קבוע c_i, $\overline{Z}\left(c_i\right)=c_i^{\mathcal{M}}$, ולכל שם עצם $f_i\left(t_1,\dots,t_n\right)$ כך ש־$\overline{Z}$ כבר הוגדרה על $t_1,\dots,t_n$, נגדיר $\overline{Z}\left(f_i\left(t_1,\dots,t_n\right)\right)=f_i^{\mathcal{M}}\left(\overline{Z}\left(t_1\right),\dots,\overline{Z}\left(t_n\right)\right)$.

אנו נזקקים להגדרה אחת נוספת כדי להיות מסוגלים להגדיר מתי מבנה מספק פסוק, וזאת על מנת לטפל בכמתים:

הגדרה 6.9 תהא Z השמה עבור $\mathcal{M}$ ויהיו v_i משתנה ו־$d\in D^{\mathcal{M}}$. נסמן ב־$Z\left[v_i\leftarrow d\right]$ את ההשמה המקיימת $Z\left[v_i\leftarrow d\right]\left(v_j\right)=\begin{cases}d & i=j\\ Z\left(v_j\right) & i\neq j\end{cases}$, כלומר ההשמה זהה ל־$Z$ פרט לכך שלמשתנה v_i היא נותנת את הערך d. השמה זו נקראת **השמה מתוקנת**.

כעת ניתן להגדיר מתי מבנה $\mathcal{M}$ מספק פסוק φ:

הגדרה 6.10 יהא $\mathcal{M}$ מבנה ו־φ נוסחה. לכל השמה Z עבור $\mathcal{M}$ נסמן $\mathcal{M}\models_Z\varphi$ ונאמר ש־$\mathcal{M}$ **מספק** את φ בהשמה Z באינדוקציית מבנה על WFF:
בסיס:

- אם $R_i\in\tau$ כלשהו אז $\mathcal{M}\models_Z R_i\left(t_1,\ldots,t_n\right)$ אם ורק אם $\left(\overline{Z}\left(t_1\right),\ldots,\overline{Z}\left(t_n\right)\right)\in R_i^{\mathcal{M}}$.
- $\mathcal{M}\models_Z t_1\approx t_2$ אם ורק אם $\overline{Z}\left(t_1\right)=\overline{Z}\left(t_2\right)$.

סגור:

- $\mathcal{M}\models_Z\neg\varphi$ אם ורק אם $\mathcal{M}\not\models_Z\varphi$
- $\mathcal{M}\models_Z\varphi_1\vee\varphi_2$ אם ורק אם $\mathcal{M}\models_Z\varphi_1\vee\mathcal{M}\models_Z\varphi_2$
- $\mathcal{M}\models_Z\varphi_1\wedge\varphi_2$ אם ורק אם $\mathcal{M}\models_Z\varphi_1\wedge\mathcal{M}\models_Z\varphi_2$
- $\mathcal{M}\models_Z\varphi_1\to\varphi_2$ אם ורק אם $\mathcal{M}\models_Z\varphi_1\Rightarrow\mathcal{M}\models_Z\varphi_2$
- $\mathcal{M}\models_Z\varphi_1\leftrightarrow\varphi_2$ אם ורק אם $\mathcal{M}\models_Z\varphi_1\iff\mathcal{M}\models_Z\varphi_2$
- $\mathcal{M}\models_Z\forall v_i\left(\varphi\right)$ אם ורק אם לכל $d\in D^{\mathcal{M}}$ מתקיים $\mathcal{M}\models_{Z\left[v_i\leftarrow d\right]}\varphi$
- $\mathcal{M}\models_Z\exists v_i\left(\varphi\right)$ אם ורק אם קיים $d\in D^{\mathcal{M}}$ כך שמתקיים $\mathcal{M}\models_{Z\left[v_i\leftarrow d\right]}\varphi$

טענה 6.11 אם φ הוא פסוק (נוסחה ללא משתנים חופשיים), אז ערך האמת שלו עבור מבנה $\mathcal{M}$ אינו תלוי בהשמה. כלומר, לכל שתי השמות Z_1,Z_2 עבור $\mathcal{M}$ מתקיים $\mathcal{M}\models_{Z_2}\varphi\iff\mathcal{M}\models_{Z_1}\varphi$.

הוכחה: נוכיח באינדוקציית מבנה על WFF טענה חזקה מעט יותר - אם Z_1,Z_2 שתי השמות שמסכימות על כל משתנה חופשי ב־φ, אז $\mathcal{M}\models_{Z_2}\varphi\iff\mathcal{M}\models_{Z_1}\varphi$. מכאן תנבע הטענה המקורית שכן בפסוק אין משתנים חופשיים.

טענת הבסיס מתקיימת באופן טריוויאלי, שכן בפסוקים אטומיים כל המשתנים חופשיים ולכן Z_1,Z_2 מסכימות על כל המשתנים שמופיעים ב־φ ומכאן בוודאי שמתקיים $\mathcal{M}\models_{Z_2}\varphi\iff\mathcal{M}\models_{Z_1}\varphi$.

לכל נוסחה מהצורה $\neg\varphi$, $\varphi_1\vee\varphi_2$, $\varphi_1\wedge\varphi_2$, $\varphi_1\to\varphi_2$ או $\varphi_1\leftrightarrow\varphi_2$, המשתנים החופשיים של φ הם גם המשתנים החופשיים של φ_1,φ_2 ולכן ניתן להשתמש בהנחת האינדוקציה על פסוקים אלו והטענה נובעת מייד.

נותר לטפל בפסוקים מהצורה $\forall x\left(\varphi\right)$ ו־$\exists x\left(\varphi\right)$. בשני המקרים ייתכן ש־$x$ חופשי ב־φ למרות שהוא איננו חופשי ב־$Qx\left(\varphi\right)$.

תהיינה Z_1,Z_2 שתי השמות שמסכימות על כל המשתנים החופשיים ב־$\forall x\left(\varphi\right)$. אז בפרט הן מסכימות על כל המשתנים החופשיים ב־φ למעט אולי x. נניח ש־$\mathcal{M}\models_{Z_1}\forall x\left(\varphi\right)$, אז לכל $d\in D^{\mathcal{M}}$ מתקיים $\mathcal{M}\models_{Z_1\left[x\leftarrow d\right]}\varphi$. מכיוון ש־$Z_1$ שווה ל־Z_2 לכל משתנה חופשי מלבד x, הרי ש־$Z_1\left[x\leftarrow d\right],Z_2\left[x\leftarrow d\right]$ מסכימות על כל משתנה חופשי של φ **כולל** x (שערכו d בשתיהן) ולכן מהנחת האינדוקציה $\mathcal{M}\models_{Z_2\left[x\leftarrow d\right]}\varphi$ לכל $d\in D^{\mathcal{M}}$, ומכאן ש־$\mathcal{M}\models_{Z_2}\forall x\left(\varphi\right)$. עבור $\exists$ ההוכחה דומה. ■

מכאן אנחנו מגיעים להגדרה המרכזית שלנו:

הגדרה 6.12 עבור פסוק φ נסמן $\mathcal{M}\models\varphi$ אם $\mathcal{M}\models_Z\varphi$ לכל השמה Z (באופן שקול, עבור השמה Z כלשהי). נאמר ש־$\mathcal{M}$ **מספק** את φ או שהוא **מודל** של φ.

עבור נוסחה φ נסמן $\mathcal{M}\models\varphi$ ונאמר ש־$\mathcal{M}$ מספק את φ (או מודל ל־φ) אם $\mathcal{M}$ הוא מודל של הסגור של φ.

עבור קבוצת פסוקים Φ נסמן $\mathcal{M}\models\Phi$ ונאמר ש־$\mathcal{M}$ הוא מודל של Φ אם הוא מודל של כל $\varphi\in\Phi$.

הגדרה 6.13 נוסחה φתקרא **אמת לוגית** אם $\mathcal{M}\models\varphi$ לכל מודל $\mathcal{M}$ (עבור השפה של L). בתחשיב הפסוקים השתמשנו במילה "טאוטולוגיה" כדי לתאר נוסחאות שכאלו, אולם בתחשיב היחסים המילה "טאוטולוגיה" שמורה לתיאור דבר מה אחר.

נוסחה φתקרא **סתירה** אם לכל מודל $\mathcal{M}$ ולכל השמה Z עבור $\mathcal{M}$ מתקיים $\mathcal{M}\not\models_Z\varphi$.

נוסחה φ תקרא **ספיקה** אם קיים מודל $\mathcal{M}$ והשמה Z כך ש־$\mathcal{M}\models_Z\varphi$.

כמו בתחשיב הפסוקים כך גם כאן ניתן לדבר על נביעה לוגית:

הגדרה 6.14 נוסחה φ **נובעת לוגית** מתורה Φ אם לכל מבנה $\mathcal{M}$ והשמה Z, אם $\mathcal{M}\models_Z\Phi$ אז $\mathcal{M}\models_Z\varphi$. נסמן זאת $\Phi\models\varphi$.

אם φ ו־Φ כולם פסוקים אז די לנו בכך שלכל מבנה $\mathcal{M}$ מתקיים שאם $\mathcal{M} \models \Phi$ אז $\mathcal{M} \models \varphi$.

הגדרה 6.15 שתי נוסחאות φ, ψ הן **שקולות לוגית** אם $\psi \models \varphi$ וגם $\varphi \models \psi$. נסמן זאת $\varphi \equiv \psi$.

הבה ונראה כמה שקילויות לוגיות פשוטות כדוגמה.

טענה 6.16 יהיו α, β נוסחאות כלשהן.

1. $\alpha \leftrightarrow \beta \equiv (\alpha \to \beta) \wedge (\beta \to \alpha)$
2. $\forall x\alpha \equiv \neg\exists x\,(\neg\alpha)$

הוכחה: יהי $\mathcal{M}$ מבנה ו־Z השמה.

1. נניח כי $\mathcal{M} \models_Z \alpha \leftrightarrow \beta$, אז אחד משניים: או ש־$\mathcal{M} \models_Z \alpha$ וגם $\mathcal{M} \models_Z \beta$ או ש־$\mathcal{M} \not\models_Z \alpha$וגם $\mathcal{M} \not\models_Z \beta$. בכל אחד מהמקרים מתקיים $\mathcal{M} \models_Z \alpha \to \beta$ ו־$\mathcal{M} \models_Z \beta \to \alpha$ (כי כדי שיתקיים $\mathcal{M} \not\models_Z \alpha \to \beta$, למשל, צריך שיתקיים $\mathcal{M} \models_Z \alpha$ אבל $\mathcal{M} \not\models_Z \beta$) ולכן $\mathcal{M} \models_Z (\alpha \to \beta) \wedge (\beta \to \alpha)$. הכיוון השני דומה.
2. נניח כי $\mathcal{M} \models_Z \forall x\alpha$, כלומר $\mathcal{M} \models_{Z[x\leftarrow d]} \alpha$ לכל $d \in D^{\mathcal{M}}$. נוכיח כי $\mathcal{M} \models_Z \neg\exists x\,(\neg\alpha)$ על ידי כך שנוכיח כי $\mathcal{M} \not\models_Z \exists x\,(\neg\alpha)$. נניח בשלילה כי $\mathcal{M} \models_Z \exists x\,(\neg\alpha)$, כלומר קיים $d \in D^{\mathcal{M}}$ כך ש־$M \models_{Z[x\leftarrow d]} \neg\alpha$. מכאן, על פי ההגדרה, ש־$M \not\models_{Z[x\leftarrow d]} \alpha$ בסתירה לכך שראינו כי $\mathcal{M} \models_{Z[x\leftarrow d]} \alpha$ לכל $d \in D^{\mathcal{M}}$. הוכחת הכיוון השני דומה.

■

6.4 הצורה הנורמלית Prenex

כשם שבתחשיב הפסוקים היה לנו נוח לעתים לעבוד עם נוסחאות בצורה נורמלית, כך גם בתחשיב היחסים לעתים עדיף לעבוד עם נוסחאות בעלות מבנה שניתן להניח עליו הנחות מקלות. במקרה שלנו נרצה לתאר צורה נורמלית הנקראת Prenex (מהמילה הלטינית praenexus שמשמעותה המילולית היא "קשור מלפנים"). בצורה נורמלית זו, כל הכמתים מופיעים בתחילת הפסוק, ולאחר מכן מופיע פסוק חסר כמתים:

הגדרה 6.17 נוסחה φ היא בצורה הנורמלית Prenex אם היא מהצורה $\varphi = Q_1v_1Q_2v_2\ldots Q_kv_k\psi$ כאשר ψ נוסחה שאינה מכילה כמתים, ו־$Q_1, \ldots, Q_k \in \{\forall, \exists\}$.
שימו לב שגם נוסחה שאינה כוללת כמתים כלל נחשבת כשייכת לצורת Prenex.

טענה 6.18 לכל נוסחה α קיימת נוסחה α' בצורת Prenex כך ש־$\alpha \equiv \alpha'$.

הוכחה: ראשית נמיר את α לנוסחה שכולל רק כמתים ואת הקשרים $\neg, \to$ על ידי ההמרות שראינו בתחשיב הפסוקים, דהיינו:

- נחליף כל $A \leftrightarrow B$ ב־$(A \to B) \wedge (B \to A)$.
- נחליף כל $A \wedge B$ ב־$\neg(A \to \neg B)$
- נחליף כל $A \vee B$ ב־$\neg A \to B$

נכונות ההמרות הללו נובעת מטענה 6.16 וטענות דומות שמוכחות באופן דומה.
מכאן ואילך נניח כי α כוללת רק את הקשרים $\neg, \to$ והכמתים $\exists, \forall$.
נשים לב כעת לשקילויות הבאות שגם הן מוכחות בדומה להוכחות של טענה 6.16:

1. $\neg\forall x\psi \equiv \exists x\neg\psi$
2. $\neg\exists x\psi \equiv \forall x\neg\psi$
3. $(\psi \to Qx\varphi) \equiv Qx\,(\psi \to \varphi)$ עבור $Q \in \{\exists, \forall\}$ בתנאי ש־x אינו חופשי ב־ψ.
4. $(Qx\psi \to \varphi) \equiv Qx\,(\psi \to \varphi)$ עבור $Q \in \{\exists, \forall\}$ בתנאי ש־x אינו חופשי ב־φ.

כעת נוכיח באינדוקציית מבנה על $\mathrm{WFF}_{\{\to,\neg\}}$ כי לכל נוסחה α קיימת נוסחה α' שקולה בצורת Prenex:

1. הבסיס מתקיים באופן טריוויאלי כי כל נוסחה אטומית היא חסרת כמתים ולכן ב־Prenex.

2. אם α שקולה ל־α' בצורת Prenex, גם $Qx\alpha$ שקולה ל־$Qx\alpha'$ עבור $Q \in \{\exists, \forall\}$ ו־$Qx\alpha'$ נמצאת בצורת Prenex.

3. אם α שקולה ל־α' בצורת Prenex, אז $\neg\alpha$ שקולה ל־$\neg\alpha'$. $\neg\alpha'$ איננה בצורת Prenex אבל נוכל להפעיל את שקילויות 1 ו־2 לעיל על מנת להכניס את $\neg$ אל תוך החלק חסר הכמתים של α'. פורמלית, מכיוון ש־α' בצורת Prenex אז $\alpha' = Q_1 v_1 \ldots Q_n v_n \psi$ כך ש־ψ חסר כמתים; אז $\neg\alpha' \equiv \overline{Q_1} v_1 \cdots \overline{Q_n} v_n \neg\psi$ כך ש־$\overline{Q_i} = \begin{cases} \forall & Q_i = \exists \\ \exists & Q_i = \forall \end{cases}$. למשל, $\neg(\forall x \exists y \forall z \psi) \equiv \exists x \forall y \exists z \neg\psi$.

4. נותר לטפל במקרה של $\alpha \to \beta$ כאשר הנחת האינדוקציה תקפה עבור α, β, כלומר יש α', β' בצורת Prenex ששקולות ל־α, β בהתאמה.

   כעת, אם משתנה כלשהו מופיע מכומת ב־α' אז החלפה שלו בכל משתנה אחר שאינו מופיע ב־α' אינה משנה את הסמנטיקה של הנוסחה; לא נוכיח זאת כעת. נבצע החלפות כאלו אם הן נדרשות כדי להבטיח שאף משתנה מכומת ב־α' לא מופיע כלל ב־β' (בפרט לא חופשי). נעשה את אותו הדבר עבור β' כדי להבטיח שאף משתנה מכומת המופיע ב־β' לא מופיע כלל ב־α'.

כעת ניתן להשתמש בשקילויות 3-4 לעיל על מנת להוציא את כל הכמתים מתוך $\alpha' \to \beta'$ (סדר ההוצאה אינו חשוב; אפשר לקבוע שרירותית שקודם כל מוציאים את כל הכמתים מ־α' ולאחר מכן מוציאים את כל הכמתים מ־β').

■

6.5 מערכת הוכחה לתחשיב היחסים ומשפט השלמות והנאותות

משהגדרנו תחביר וסמנטיקה עבור תחשיב היחסים, הצעד המתבקש הבא הוא להגדיר **מערכת הוכחה** ולהראות כי היא שלמה ונאותה. אחד מהיתרונות של לוגיקה מסדר ראשון (להבדיל מלוגיקה מסדרים גבוהים יותר) היא שמערכת הוכחה כזו קיימת; למעשה, קיימות מערכות הוכחה **רבות מאוד** עבור תחשיב היחסים, וכמעט כל ספר לוגיקה מציג גרסה משל עצמו. כמובן שישנם רעיונות משותפים רבים לכל מערכות ההוכחה, אך הבחירה הסופית של מערכת ההוכחה היא בעיקר עניין של אופי.

באופן כללי יש איזון כלשהו שמערכת ההוכחה מבצעת בין **כללי ההיסק** ובין **האקסיומות** שלה. ככל שיש יותר כללי היסק כך ניתן לחסוך יותר באקסיומות, ולרוב כללי ההיסק מצביעים על הסקות אינטואיטיביות יחסית. עם זאת, כעת נציג מערכת הוכחה שהיא חסכונית מאוד בכללי ההיסק שלה: כלל ההיסק היחיד יהיה MP שהכרנו כבר מתחשיב הפסוקים.

מכיוון שזהו כלל ההיסק היחיד, ברור שהאקסיומות יצטרכו לתאר בצורה אינטנסיבית נוסחאות עם הכמתים $\forall, \exists$, שכן MP לא מסוגל "לייצר" את הכמתים הללו בעצמו.

נזדקק לשתי הגדרות:

הגדרה 6.19 טאוטולוגיה בתחשיב היחסים היא פסוק WFF שמתקבל מהצבת פסוקי WFF של תחשיב היחסים במקום המשתנים של טאוטולוגיה בתחשיב הפסוקים.

הגדרה 6.20 הכללה של פסוק ψ היא כל פסוק מהצורה $\forall v_1 \ldots \forall v_n \psi$.

כמו כן נאמר ש**חוקי** להציב שם עצם t במקום משתנה x בפסוק ψ אם לא קיים ב־ψ כמת מהצורה Qy כך שיש מופע חופשי של x שנופל בטווח הכמת הזה, וכמו כן y מופיע ב־t.

כעת ניתן להציג פורמלית את כל קבוצות האקסיומות של מערכת ההיסק שלנו. האקסיומות כוללות את כל ההכללות של פסוקים השייכים לאחת משש הקבוצות הבאות:

1. כל הטאוטולוגיות.

2. $\forall x \alpha(x) \to \alpha(t)$, כאשר $\alpha(t)$ הוא הפסוק שמתקבל מ־$\alpha(x)$ על ידי החלפת כל מופע חופשי של המשתנה x במופע של שם העצם t, וזאת בתנאי שחוקי להציב את t במקום x.

3. $\forall x (\alpha \to \beta) \to (\forall x \alpha \to \forall x \beta)$.

4. $\alpha \to \forall x \alpha$ אם x לא מופיע חופשי ב־α.

5. $x \approx x$.

6. $x \approx y \to (\alpha \to \alpha')$ לכל α אטומי כך ש־α' מתקבל מ־α על ידי החלפת מספר שרירותי כלשהו של מופעים של x ב־y.

למרות שהאקסיומות נראות ברובן הגיוניות, כלל לא ברור למה בחרנו דווקא אותן; מן הסתם, כל אחת מהן נדרשת עבור שלב כלשהו בהוכחת משפט השלמות, כפי שקרה בתחשיב הפסוקים.

התנאי של האקסיומות מהצורה 2 נראה שרירותי למדי. ניתן דוגמה להכרחיות שלו. נתבונן בפסוק הבא:
$\forall x\left(\neg\forall y\left(x\approx y\right)\right)\to\neg\forall y\left(y\approx y\right)$

חציו הראשון של הפסוק נראה הגיוני - עבור כל מבנה שכולל לפחות שני איברים, לכל x קיים y השונה ממנו, ולכן $\neg\forall y\left(x\approx y\right)$. עם זאת, חציו השני של הפסוק אשר מתקבל מהצבת שם העצם $t=y$ בתוך x, הוא בבירור שגוי תמיד כי הוא אומר שקיים איבר שאינו שווה לעצמו. הבעיה כאן היא בדיוק בהצבה של $t=y$ ש"נופל" בתוך הכמת $\forall y$.

נוכיח מספר משפטים פשוטים על כוחה של מערכת ההוכחה שלנו כדי לקבל תחושה עבור נחיצות חלק מהאקסיומות.

משפט 6.21 ("משפט ההכללה") אם $\Phi\vdash\alpha$ ו־x אינו חופשי באף נוסחה של Φ, אז $\Phi\vdash\forall x\alpha$.

הוכחה: נוכיח באינדוקציית מבנה על $\mathrm{Ded}\left(\Phi\right)$.

אם $\alpha\in A$ (אקסיומה) אז מכיוון שכל הכללה של אקסיומה גם היא אקסיומה, $\forall x\alpha$ גם היא אקסיומה ולכן שייכת ל־$\mathrm{Ded}\left(\Phi\right)$.

אם $\alpha\in\Phi$, אז מכיוון שהנחנו ש־x אינו חופשי באף נוסחה של Φ הוא בפרט אינו חופשי ב־α ונקבל את ההוכחה הבאה של $\forall x\alpha$:

1. α (הנחה).
2. $\alpha\to\forall x\alpha$ (תבנית אקסיומה 4)
3. $\forall x\alpha$ (MP על 1,2).

נותר לטפל במקרה שבו α התקבלה על ידי MP. נניח אם כן כי הנחת האינדוקציה תקפה עבור $\beta,\beta\to\alpha$ עבור β כלשהו כך ש־$\Phi\vdash\beta$ ו־$\Phi\vdash\beta\to\alpha$. מהנחת האינדוקציה נקבל ש־$\Phi\vdash\forall x\beta$ ו־$\Phi\vdash\forall x\left(\beta\to\alpha\right)$. כעת נקבל את ההוכחה הבאה של $\forall x\alpha$:

1. $\forall x\beta$ (משפט).
2. $\forall x\left(\beta\to\alpha\right)$ (משפט).
3. $\forall x\left(\beta\to\alpha\right)\to\left(\forall x\beta\to\forall x\alpha\right)$ (תבנית אקסיומה 3).
4. $\forall x\beta\to\forall x\alpha$ (MP על 2,3).
5. $\forall x\alpha$ (MP על 1,4).

■

תבניות אקסיומה 3 ו־4 היו נחוצות ספציפית על מנת להוכיח את המשפט הזה. לעתים מנסחים את מערכת ההוכחה לתחשיב היחסים בלי תבניות אקסיומה אלו, אך עם כלל היסק חדש Gen שמאפשר להסיק מתוך $\varphi\left(y\right)$ את $\forall x\varphi\left(x\right)$ בתנאי ש־x אינו חופשי ב־$\varphi\left(y\right)$.

משפט 6.22 ("משפט הדדוקציה") $\Phi\cup\left\{\alpha\right\}\vdash\beta$ אם ורק אם $\Phi\vdash\alpha\to\beta$.

הוכחה: ההוכחה היא במהותה אותה הוכחה כמו בתחשיב הפסוקים. אם $\Phi\vdash\alpha\to\beta$ אז בבירור $\Phi\cup\left\{\alpha\right\}\vdash\beta$ על ידי הוכחה מההנחות $\alpha,\alpha\to\beta$ ושימוש ב־MP. את הכיוון השני מוכיחים באינדוקציית מבנה על $\mathrm{Ded}\left(\Phi\cup\left\{\alpha\right\}\right)$, כשעבור כל אחד מהמקרים לוקחים בדיוק את אותה הוכחה פורמלית כפי שביצענו בתחשיב הפסוקים. האקסיומות שבהן השתמשנו אז הן גם אקסיומות של תחשיב היחסים, שכן הן מתקבלות מהצבת נוסחאות בתחשיב היחסים בתוך משתני האקסיומה. ■

משפט 6.23 ("משפט ההוכחה בשלילה") אם $\Phi\cup\left\{\neg\alpha\right\}$ אינה עקבית אז $\Phi\vdash\alpha$.

הוכחה: גם כאן זהו אותו משפט מתחשיב הפסוקים. מכיוון ש־$\Phi\cup\{\neg\alpha\}$ אינה עקבית אז $\Phi\cup\{\neg\alpha\}\vdash\beta$ ו־$\Phi\cup\{\neg\alpha\}\vdash\neg\beta$ עבור טאוטולוגיה כלשהי, ועל ידי שימוש בטאוטולוגיה $(\neg\alpha\to\neg\beta)\to(\beta\to\alpha)$ ובמשפט הדדוקציה שמסיק מ־$\Phi\cup\{\neg\alpha\}\vdash\neg\beta$ שמתקיים $\Phi\vdash\neg\alpha\to\neg\beta$ מגיעים לתוצאה המבוקשת. ■

אם כן, מערכת ההוכחה לתחשיב היחסים מתנהגת באופן דומה לזו של תחשיב הפסוקים, באופן לא מפתיע במיוחד.

בשל קוצר זמן לא נוכל להציג בקורס הוכחה מלאה למשפט השלמות והנאותות ולכן נסתפק בציטוט וסקירה קצרה:

משפט 6.24 (**משפט השלמות של גדל**) לכל קבוצה עקבית של נוסחאות בתחשיב היחסים יש מודל.

משפט 6.25 (**משפט השלמות והנאותות לתחשיב היחסים**): לכל קבוצת נוסחאות Φ ונוסחה φ מתקיים $\Phi\models\varphi$ אם ורק אם $\Phi\vdash\varphi$.

הוכחת משפט הנאותות אינה קשה במיוחד, אך יכולה להיות מעייפת למדי שכן הכרחי לבדוק שכל האקסיומות שלנו הן תקפות לוגית, דהיינו כל מבנה הוא מודל שלהן.

הוכחת משפט השלמות בניסוח $\Phi\models\varphi\Rightarrow\Phi\vdash\varphi$ זהה להוכחת המשפט המקביל בתחשיב הפסוקים: אם $\Phi\cup\{\neg\varphi\}$ אינה עקבית אז ממשפט ההוכחה בשלילה (שראינו כי הוא תקף גם עבור תחשיב היחסים), $\Phi\vdash\varphi$. אחרת, אם $\Phi\cup\{\neg\varphi\}$ עקבית אז קיים לה מודל (ממשפט השלמות של גדל), אבל כל מודל של Φ הוא גם מודל של φ כי $\Phi\models\varphi$ והגענו לסתירה כי מצאנו מבנה שהוא מודל גם של φ וגם של $\neg\varphi$.

עיקר הקושי, אם כן, הוא בהוכחה שלכל קבוצה עקבית של נוסחאות יש מודל. ההוכחה קשה מכדי שניתן אותה כאן, אך נסקור בכל זאת את הרעיונות העיקריים בה (נציג את הרעיונות שמאחורי ההוכחה שנתן הנקין מספר שנים לאחר גדל, והיא שונה באופיה מההוכחה של גדל):

ראשית, בהינתן Φ עקבית מרחיבים אותה ל־Φ' עקבית מקסימלית, בדומה לתחשיב הפסוקים. כמו בתחשיב הפסוקים, Φ' מקיימת את התכונה שלכל נוסחה ψ או ש־$\Phi'\vdash\psi$ או ש־$\Phi\vdash\neg\psi$. עם זאת, אנחנו דורשים מ־Φ' תכונה נוספת שלא הייתה בתחשיב הפסוקים: שהיא **תכיל עדים להפרכה**. פורמלית, לכל נוסחה $\psi(x)$ ומשתנה x, יש קבוע c כך ש־$\neg\forall x\psi(x)\to\neg\psi(c)\in\Phi$.

במילים אחרות, אם ψ איננה נכונה לכל הצבה של ערך אפשרי במשתנה x, אז קיים קבוע c שהוא "עד להפרכה" הזו, והפסוק שמתאר פורמלית את ההפרכה שייך ל־Φ.

על מנת להבטיח קיום של קבועים שהם "עדים להפרכה", לעתים קרובות יש הכרח **להרחיב את השפה** שאיתה אנו עובדים ולהוסיף קבועים נוספים (הרחבת השפה איננה בעיה במובן זה שכל מודל ל־Φ' בעלת השפה העשירה יותר יהיה גם מודל של Φ בעלת השפה ה"רזה").

השלב הבא הוא בניית המודל עבור Φ'. כאן בא לידי ביטוי הרעיון הגאוני המרכזי בהוכחה: במודל הזה $D^{\mathcal{M}}$ תהיה קבוצת **כל שמות העצם** של השפה של Φ'. כלומר, המודל עצמו נבנה מתוך השפה. למשל, אם $f(x,y)$ הוא שם עצם בשפה של Φ' אז $f(x,y)$ יהיה **איבר בודד** ב־$D^{\mathcal{M}}$. כעת אפשר להגדיר את היחסים, הקבועים והפונקציות בהתאם: למשל, אם $R(t_1,\ldots,t_n)\in\Phi'$ אז $(t_1,\ldots,t_n)\in R^{\mathcal{M}}$. בדומה, $f^{\mathcal{M}}(x,y)=f(x,y)$ (באגף שמאל זוהי הפעלה של פונקציה; באגף ימין זוהי מחרוזת) וכדומה.

בניה זו "כמעט עובדת", אבל נתקלת בבעיה עבור שמות עצם שונים שאמורים לייצג את אותו איבר בדיוק מכיוון שב־Φ' נכללות נוסחאות עם $\approx$ שאומרות זאת (למשל, $g(c_1,c_2)\approx f(c_1,c_2)\in\Phi'$ פירושו שהאיברים $g(c_1,c_2)$ ו־$f(c_1,c_2)$ במודל צריכים להיות אותו איבר בדיוק). הפתרון לבעיה זו הוא באמצעות הגדרת יחס שקילות מתאים על $D^{\mathcal{M}}$ והגדרת $D^{\mathcal{M}}$ הסופי בתור אוסף מחלקות השקילות המתאימות.

זוהי סקיצה בלבד של ההוכחה; הפרטים המדוייקים סבוכים בהרבה, כצפוי.

6.6 גדירות בתחשיב היחסים (מבוא לתורת המודלים)

האקסיומות של תורת החבורות שהצגנו נבנו בצורה כזו שהבטיחה שכל מודל עבור תורת החבורות הוא אכן המבנה המתמטי המכונה **חבורה**. כך היה גם עבור חוגים ושדות. ומה לגבי אקסיומות פיאנו? האם כל מודל שלהן הוא בדיוק המספרים הטבעיים?

נפתח בהגדרה האנלוגית לזו של תחשיב הפסוקים:

הגדרה 6.26 תהא Φ תורה. נגדיר את הקבוצה $\mathrm{MOD}(\Phi)\triangleq\{\mathcal{M}|\mathcal{M}\models\Phi\}$ - קבוצת המבנים ש־Φ **מגדירה**. נאמר שקבוצת מבנים K **מוגדרת** על ידי Φ אם $K=\mathrm{MOD}(\Phi)$.

השאלה "בהינתן K, האם היא גדירה?" היא אחת מהשאלות העומדות במרכז התחום הנקרא **תורת המודלים**. לפעמים התשובה לשאלה פשוטה, כמו במקרה של חבורות; לעתים התשובה מורכבת וקשה ביותר. נתחיל בכמה דוגמאות טריוויאליות:

1. עבור מילון ריק, קבוצת המודלים עבורם $\left|D^{\mathcal{M}}\right| \ge 2$ מוגדרת על ידי התורה שכוללת רק את הפסוק $\exists x \exists y \neg (x \approx y)$.

2. עבור מילון ריק, קבוצת המודלים עבורם $\left|D^{\mathcal{M}}\right| = 1$ מוגדרת על ידי התורה שכוללת רק את הפסוק $\forall x \forall y \, (x \approx y)$. כאן אנו מתבססים על הדרישה שלנו ש־$D^{\mathcal{M}} \neq \emptyset$, אך זה לא מהותי כי הפסוק $\forall x \forall y \, (x = y) \wedge \exists x \, (x = x)$ מגדיר את קבוצת המודלים גם ללא הנחה זו.

3. עבור מילון ריק, קבוצת המודלים עבורם $\left|D^{\mathcal{M}}\right| = \infty$ מוגדרת על ידי התורה $\{\varphi_1, \varphi_2 \ldots\}$ כאשר φ_i הוא פסוק שאומר "במודל יש לפחות i איברים שונים" בדומה לפסוק של דוגמא 1: $\varphi_i = \exists x_1 \ldots \exists x_i \left(\bigwedge_{i,j} \neg (x_i \approx x_j) \right)$.

כעת נציג, ללא הוכחה, את הכלי הבסיסי המועיל ביותר בתורת המודלים:

משפט 6.27 (משפט הקומפקטיות לתחשיב היחסים): לתורה Φ יש מודל אם ורק אם לכל תת־תורה סופית של Φיש מודל.

המשפט אנלוגי לחלוטין למשפט עבור תחשיב הפסוקים, וגם הוכחתו זהה בהינתן שהוכחנו את משפט השלמות לתחשיב היחסים. עם זאת, השלכותיו הן מרחיקות לכת בהרבה מהשלכות המשפט האנלוגי עבור תחשיב הפסוקים ונראה לכך מספר דוגמאות.

טענה 6.28 עבור מילון ריק, קבוצת המודלים עבורם $\left|D^{\mathcal{M}}\right| < \infty$ **אינה** גדירה.

הוכחה: נניח בשלילה כי קבוצה זו גדירה על ידי התורה Φ. נרחיב את Φ ל־$\Phi' = \Phi \cup \{\varphi_1, \varphi_2, \ldots\}$ כאשר φ_i הנוסחאות מדוגמא 3 שמבטיחות קיום של לפחות i איברים שונים במודל. תת־קבוצה סופית של Φ' תכלול רק פסוקים מ־Φ ופסוקים φ_i עבור $i < N$ עם N טבעי כלשהו. ברור כי כל מודל עבורו $N < \left|D^{\mathcal{M}}\right| < \infty$ יספק את Φ', ולכן ממשפט הקומפקטיות קיים מודל ל־$\Phi \cup \{\varphi_1, \varphi_2, \ldots\}$. מדוגמא 3 עולה שמודל זה חייב להיות אינסופי, ומצד שני הוא מודל של Φ, בסתירה לכך ש־Φ מגדיר רק מבנים סופיים. ■

באופן דומה ניתן להוכיח שאקסיומות פיאנו **אינן** מגדירות רק את המספרים הטבעיים!

משפט 6.29 קיים מודל של אקסיומות פיאנו שאינו $\mathbb{N}$.

הוכחה: נרחיב את אקסיומות פיאנו על ידי הוספת סימן קבוע חדש a ונוסחאות $\varphi_n : (n < a)$ לכל n טבעי (כזכור, $n \triangleq S^n(0)$). קל לראות כי כל תת־קבוצה סופית של נוסחאות מהקבוצה המורחבת של אקסיומות פיאנו היא ספיקה (על ידי המודל $\mathbb{N}$), ולכן ממשפט הקומפקטיות נקבל קיום של מודל $\mathcal{M}$ עבור מערכת האקסיומות המורחבת. עם זאת, במודל זה האיבר $a^{\mathcal{M}}$ גדול מכל מספר טבעי ולכן $\mathcal{M} \neq \mathbb{N}$. מכיוון ש־$\mathcal{M}$ הוא מודל של מערכת האקסיומות המורחבת של פיאנו, הוא ודאי מודל עבור מערכת האקסיומות הלא מורחבת. ■

המודל $\mathcal{M}$ שקיבלנו במהלך ההוכחה מכונה **מודל לא סטנדרטי של האריתמטיקה** (לרוע המזל, קשה לתת לו תיאור מפורש פשוט ולכן נוותר על תיאור נוסף שלו). כאן המילה "סטנדרטי" באה לציין שהמספרים הטבעיים הם מודל שאנחנו "חושבים עליו" כאשר אנו משתמשים באקסיומות פיאנו (עבור תורת החבורות, למשל, לא קיים מודל סטנדרטי שכזה כי איננו מנסים למדל אובייקט יחיד אלא מחלקה גדולה של אובייקטים).

מה שאנו רואים כאן הוא ש**השפה** של תחשיב היחסים היא חלשה מכדי להבדיל בין המודל הסטנדרטי ומודלים לא סטנדרטיים עבור האריתמטיקה (שימו לב שבהוכחה שלנו השתמשנו רק במשפט הקומפקטיות ולא בתכונות של אקסיומות פיאנו). לרוע המזל, חולשה היא גם בדיוק מה שמאפשר לנו להוכיח את משפט השלמות (שממנו נובע משפט הקומפקטיות); בלוגיקה מסדר שני אמנם קיימת מערכת אקסיומות שהמספרים הטבעיים הם המודל היחיד שלה, אך לא קיימת מערכת הוכחה ללוגיקה מסדר שני (כלומר, לא ניתן להוכיח בה אנלוג למשפט השלמות).

התנהגות מוזרה זו של מודלים מתוארת בצורה כללית יותר באמצעות המשפט הבא, שלא נוכיח כאן:

משפט 6.30 (**משפט לוונהיים־סקולם־טרסקי**): תהא Φ תורה מסדר ראשון מעל **שפה בת מניה**. אם קיים ל־Φ מודל אינסופי, אז קיים ל־Φ מודל מעוצמה κ עבור כל עוצמה אינסופית κ.

גם מבלי להציג את פרטי ההוכחה, הרעיון הבסיסי אינו קשה במיוחד. ראשית, אם Φ היא תורה שקיים לה מודל אז היא כמובן עקבית, ולכן קיים עבורה ספציפית המודל שנבנה עבור Φ בהוכחת משפט השלמות של גדל. בדיקה זהירה של פרטי ההוכחה (שלא הצגנו) מראה כי המודל הזה הוא בן מניה, בתנאי ששפת Φ היא בת־מניה. מכאן שאם קיים ל־Φ מודל כלשהו, קיים לה מודל שהוא לכל היותר בן מניה. תוצאה זו לכשעצמה מכונה "משפט לוונהיים־סקולם".

חלקו של טרסקי הוא האבחנה שאם המודל של Φ הוא אינסופי אז קיים ל־Φ מודל מכל עוצמה אינסופית κ. קל להראות זאת בעזרת משפט הקומפקטיות: מרחיבים את השפה של Φ על ידי הוספת κ קבועים, ואת הפסוקים $\neg (c_i \approx c_j)$ לכל זוג

קבועים שונים. משפט הקומפקטיות מראה כי כל תת־קבוצה סופית של Φ יחד עם פסוקים אלו היא ספיקה (כאן הכרחי שהמודל של Φ יהיה אינסופי, אחרת תתי־קבוצות גדולות מדי של פסוקים לא יהיו בהכרח ספיקות), ולכן קיים מודל לתורה המורחבת, שעוצמתו היא בהכרח κ. טרסקי עצמו הוכיח את התוצאה בסמינר שלו **לפני** הוכחת משפט הקומפקטיות, ולאיש (ובפרט לטרסקי עצמו) אין מושג איך הוא עשה זאת.

משפט לוונהיים־סקולם־טרסקי הוא רב עוצמה ומפתיע ביותר. ניתן דוגמא אחת לפרדוקסליות שלכאורה מתעוררת ממנו, שעליה הצביע סקולם עצמו, ונקראת על שמו **פרדוקס סקולם**: בהנחה שלתורת הקבוצות ZF קיים מודל, אז נובע מהאקסיומות שהוא אינסופי, ומכאן שקיים ל־ZF מודל מכל עוצמה אינסופית. בפרט קיים מודל בן מניה. פירוש הדבר הוא שכל קבוצה במודל הזה חייבת להיות בעצמה בת מניה (כי היא איננה יכולה לכלול יותר איברים מאשר קיימים מלכתחילה במודל של ZF). עם זאת, באמצעות האקסיומות של ZF אפשר להוכיח את הטענה "קיימת קבוצה A שאיננה בת מניה" (זכרו את האלכסון של קנטור)!

הפתרון לפרדוקס הזה הוא עדין ומבלבל ממבט ראשון. הטענה שאותה מוכיחים ב־ZF איננה בדיוק "קיימת קבוצה שאיננה בת מניה", אלא "קיימת קבוצה A שאין התאמה חח"ע ועל בינה ובין קבוצת הטבעיים $\mathbb{N}$". יש לזכור ש"התאמה חח"ע ועל" היא קבוצה במודל **בעצמה**! במודל בן המניה של ZF מה שקורה הוא שאין במודל קבוצה שמהווה פונקציה חח"ע ועל בין A ובין $\mathbb{N}$; זה לא אומר ש־A איננה בת מניה, אלא רק שבמודל בן המניה של ZF **אין עדות** לכך שהיא בת מניה.

נסיים בעוד דוגמה למודל "לא סטנדרטי" שקיומו דווקא מאפשר דרך התבוננות חדשה על מושגים מסויימים. נגדיר שפה מסדר ראשון עבור המספרים הממשיים $\mathbb{R}$, כך שהשפה עשירה מאוד: **לכל** יחס n־מקומי $R\subseteq\mathbb{R}^{n}$ יהיה לנו סימן בשפה, וכך גם לכל פונקציה על $\mathbb{R}^{n}$ (וזאת לכל n) וכמו כן יהיה לנו סימן קבוע c_{r} לכל $r\in\mathbb{R}$. במילים אחרות, השפה שלנו מלכתחילה מהונדסת כדי לתאר באופן מושלם את המספרים הממשיים. נסמן ב־$\mathcal{R}$ את המבנה שהעולם שלו הוא $\mathbb{R}$ והפרשנות שהוא נותן לסימני המילון היא המשמעות המיועדת שלהם (למשל, $c_{r}^{\mathcal{R}}=r$). זהו "המודל הסטנדרטי" של השפה הזו.

כעת נגדיר $\Phi=\{\varphi\mid\mathcal{R}\models\varphi\}$ - שפת כל הפסוקים שמסופקים על ידי $\mathcal{R}$. קבוצת הפסוקים הזו היא האפיון המלא ביותר של $\mathbb{R}$ שניתן לתת על ידי השפה שלנו (ולכן שניתן לתת בכלל, בלוגיקה מסדר ראשון).

כעת ננקוט באותו תעלול בו נקטנו עבור הטבעיים: נרחיב את השפה עוד יותר על ידי הוספת קבוע חדש a, ונוסיף את הפסוקים $c_{r}<a$ עבור כל $r\in\mathbb{R}$ לקבוצה שלנו לקבלת קבוצת פסוקים חדשה Φ'. כעת, $\mathbb{R}$ הוא מודל של כל תת־קבוצה סופית של Φ' (פשוט בוחרים להתאים ל־a מספר ממשי גדול דיו כדי להיות גדול יותר מכל ה־r־ים של הפסוקים מהצורה $c_{r}<a$ שמופיעים בתת־הקבוצה של Φ'), ולכן עולה ממשפט הקומפקטיות שקיים מודל ל־Φ'. במודל זה, האיבר שמתמפה ל־a הוא גדול מכל מספר טבעי, וניתן לחשוב עליו כעל "אינסוף". מצד שני, המודל של Φ' מקיים כל נוסחה ש־$\mathbb{R}$ קיים, ולכן בפרט קיים הופכי ל־a (כי במספרים הממשיים לכל מספר שונה מאפס יש הופכי). על ההופכי הזה ניתן לחשוב בתור "אינפיניטסימל" - מספר שגדול מאפס אך קטן מכל מספר ממשי.

תוך שימוש בכך שכל התכונות של $\mathbb{R}$ שניתנות לניסוח בשפה שלנו מתקיימות גם במודל החדש ניתן לפתח מחדש את החשבון האינפיניטסימלי בתוך המודל החדש הזה. ניתן לאפיין קבוצות של מספרים "אינסופיים" ושל מספרים "אינפיניטסימליים" בתוך המודל; ניתן להגדיר $\lim_{x\to x_{0}}f\left(x\right)=L$ בתור "אם $|x-x_{0}|$ הוא מספר אינפיניטסימלי אז $|f\left(x\right)-L|$ הוא מספר אינפיניטסימלי" וכדומה. בצורה זו ניתן ביסוס מתמטי פורמלי ומדויק לגישתם של ניוטון ולייבניץ לחשבון אינפיניטסימלי (עם זאת, חסרון שיטה זו הוא בכך שהמודל הלא סטנדרטי הוא מורכב לתיאור ובנייתו כוללת בהכרח צעד לא קונסטרוקטיבי).

6.7 גדירות עבור תורת הגרפים

נעבור כעת להצגת תוצאות בתורת המודלים על **תורת הגרפים**. המילון שלנו יהיה פשוט במיוחד: $\tau=\langle E\rangle$ כאשר E הוא יחס דו מקומי ותו לא. כל מודל $\mathcal{M}$ לשפה זו כולל קבוצה $D^{\mathcal{M}}$ ויחס דו מקומי עליה $E^{\mathcal{M}}$, כך שניתן לחשוב על $\mathcal{M}$ כגרף $G=(V,E)$ עם $V=D^{\mathcal{M}}$ ו־$E=E^{\mathcal{M}}$ (חוגים עצמיים מותרים, קשתות מקבילות לא). נשתמש אם כן בטרמינולוגיה של תורת הגרפים כדי לתאר את כל מה שנעשה מעתה ואילך.

6.7.1 גדירות של תכונות של גרפים

ב"תכונה של גרף" נרצה לתאר תכונה שאיננה תלויה בשמות הספציפיים שאנו בוחרים לצמתי הגרף. לצורך כך נזדקק ראשית כל להגדרה:

הגדרה 6.31 שני גרפים $G_{1}=\left(V_{1},E_{1}\right),G_{2}=\left(V_{2},E_{2}\right)$ הם **איזומורפיים** אם קיימת פונקציה חח"ע ועל $f:V_{1}\to V_{2}$ כך ש־$\left(f\left(u\right),f\left(v\right)\right)\in E_{2}\iff\left(u,v\right)\in E_{1}$. אם G_{1} איזומורפי ל־G_{2} נסמן זאת על ידי $G_{1}\cong G_{2}$.

הגדרה זו אומרת שהגרפים הם אותו הדבר עד כדי שינוי שמות הצמתים. בפרט, הקשתות הן אותן הקשתות.

הגדרה 6.32 תכונה של גרפים היא קבוצה $\mathcal{P}$ של גרפים הסגורה תחת איזומורפיזם; כלומר, אם $G_{1}\cong G_{2}$ אז $G_{1}\in\mathcal{P}\iff G_{2}\in\mathcal{P}$.

השאלה המרכזית שתעניין אותנו תהיה: מהן התכונות של גרפים לא מכוונים **סופיים** שהן גדירות בלוגיקה מסדר ראשון? כלומר, בהינתן קבוצה $\mathcal{P}$ של גרפים סופיים הסגורים תחת איזומורפיזם, האם קיימת קבוצת פסוקים Φ כך שלכל גרף סופי G, $G\in\mathcal{P}$ אם ורק אם $G\in\mathrm{Mod}\left(\Phi\right)$? שימו לב ש־$\mathrm{Mod}\left(\Phi\right)$ יכולה להכיל בנוסף ל־$\mathcal{P}$ גם גרפים אינסופיים וגרפים מכוונים (כלומר, כאלו שבהם $E\left(a,b\right)$ לא בהכרח גורר $E\left(b,a\right)$, מה שמצדיק את הסימון הבא:

הגדרה 6.33 נסמן ב־$\mathcal{F}$ את קבוצת כל הגרפים הלא מכוונים הסופיים. נגדיר $\mathrm{Mod}_{f}\left(\Phi\right)\triangleq\mathrm{Mod}\left(\Phi\right)\cap\mathcal{F}$.

שימו לב כי $\mathcal{F}$ עצמה אינה גדירה (זהו שימוש סטנדרטי של משפט הקומפקטיות שראינו קודם) ולכן ההגדרה אינה מיותרת.

טענה 6.34 אם G הוא גרף סופי כלשהו, אז התכונה $\mathcal{P}_{G}=\left\{ G'|G'\cong G\right\}$ היא גדירה על ידי פסוק יחיד, כלומר קיים φ כך ש־$\mathrm{Mod}_{f}\left(\varphi\right)=\mathcal{P}$.

הוכחה: נמספר את צמתי $G=\left(V_{G},E_{G}\right)$: $V_{G}=\left\{ v_{1},\dots,v_{n}\right\}$. כעת נגדיר

$$\varphi_{G}\;=\;\exists x_{1}\dots\exists x_{n}\left(\bigwedge_{i\ne j}\neg\left(x_{i}=x_{j}\right)\wedge\bigwedge_{\left(v_{i},v_{j}\right)\in E_{G}}E\left(x_{i},x_{j}\right)\wedge\bigwedge_{\left(v_{i},v_{j}\right)\notin E_{G}}\neg E\left(x_{i},x_{j}\right)\wedge\forall y\left(\bigvee_{i=1}^{n}y=x_{i}\right)\right)$$

קל לבדוק כי אכן $\mathrm{Mod}_{f}\left(\varphi_{G}\right)=\mathcal{P}_{G}$. ■

מסקנה 6.35 כל תכונה $\mathcal{P}$ של גרפים סופיים היא גדירה על ידי קבוצה Φ.

הוכחה: נגדיר $\Phi=\left\{ \neg\varphi_{G}\mid G\notin\mathcal{P}\right\}$. כעת $\mathrm{Mod}_{f}\left(\Phi\right)$ כוללת בדיוק את כל הגרפים הסופיים שאינם איזומורפיים לאף גרף שאינו ב־$\mathcal{P}$, ולכן בפרט הם עצמם ב־$\mathcal{P}$. ■

אם כן, גדירות במובן ה"קלאסי" של המילה מתקיימת אוטומטית לכל קבוצה של גרפים סופיים. עם זאת, מבחינה אלגוריתמית יש כאן בעיה מהותית, שכן בהינתן גרף G אין דרך ברורה לבדוק את שייכותו ל־$\mathrm{Mod}_{f}\left(\Phi\right)$. ניתן אמנם לעבור פסוק־פסוק ב־Φ ואם יתגלה פסוק ש־G אינו מספק נדע כי $G\notin\mathrm{Mod}_{f}\left(\Phi\right)$, אך אם $G\in\mathrm{Mod}_{f}\left(\Phi\right)$ לעולם לא נדע זאת בודאות בדרך זו.

לכן אנו עוברים לדרוש הגדרה מחמירה יותר של גדירות:

הגדרה 6.36 תכונה $\mathcal{P}$ של גרפים היא **גדירה סופית** אם קיימת קבוצה **סופית** Φ כך ש־$\mathrm{Mod}_{f}\left(\Phi\right)=\mathcal{P}$.

טענה 6.37 $\mathcal{P}$ היא גדירה סופית אם ורק אם קיים פסוק יחיד φ כך ש־$\mathrm{Mod}_{f}\left(\varphi\right)=\mathcal{P}$.

הוכחה: כיוון אחד הוא ברור. בכיוון השני, אם Φ סופית ומגדיר את $\mathcal{P}$, אז הפסוק $\varphi=\bigwedge_{\psi\in\Phi}\psi$ מגדיר את $\mathcal{P}$. ■

מעתה ואילך כל שימוש שלנו במילה "גדירות" יהיה במשמעות של "גדירות סופית" גם בלי לציין זאת במפורש.

נדגים כעת את הגדירות של מספר תכונות פשוטות בגרפים:

1. קבוצת הגרפים הריקים (ללא קשתות) גדירה על ידי הנוסחה $\forall x\forall y\left(\neg E\left(x,y\right)\right)$.
2. קבוצת הגרפים המלאים (כל הקשתות האפשריות) גדירה על ידי הנוסחה $\forall x\forall y\left(E\left(x,y\right)\right)$. שימו לב כי הגדרה זו כוללת בפרט קשתות מצומת לעצמו.
3. קבוצת הגרפים שמכילים משולש גדירה על ידי הנוסחה

$$\exists x\exists y\exists z\left(\neg\left(x=y\right)\wedge\neg\left(x=z\right)\wedge\neg\left(y=z\right)\wedge E\left(x,y\right)\wedge E\left(x,z\right)\wedge E\left(y,z\right)\right)$$

4. נכליל את דוגמה 3. יהי $G=\left(V,E\right)$ גרף סופי כלשהו, כלומר $V=\left\{ v_{1},\dots,v_{n}\right\}$. נרצה להגדיר את קבוצת כל הגרפים שמכילים את G כתת־גרף. נעשה זאת באמצעות הנוסחה:

$$\exists x_{1},\dots,x_{n}\left(\bigwedge_{i\ne j}\neg\left(x_{i}=x_{j}\right)\wedge\bigwedge_{\left(v_{i},v_{j}\right)\in E}E\left(x_{i},x_{j}\right)\wedge\bigwedge_{\left(v_{i},v_{j}\right)\notin E}\neg E\left(x_{i},x_{j}\right)\right)$$

5. קבוצת הגרפים עם לפחות n צמתים גדירה על ידי $\exists x_1,\ldots,x_n\left(\bigwedge_{i\neq j}\neg\left(x_i=x_j\right)\right)$ (ראינו כבר דוגמה דומה עבור מילון ריק, וכאן כמובן שאין הבדל).

נעבור כעת לתכונה אחרת: קשירות. גרף G הוא קשיר אם לכל שני צמתים $a,b\in V$ קיים מסלול $a=v_0\to v_1\to\cdots\to v_{n+1}=b$, או באופן שקול ־ אם בכל חלוקה של V לשתי קבוצות זרות ולא ריקות $V=A\cup B$ קיימים $a\in A,b\in B$ כך ש־$(a,b)\in E$. הבה וננסה להגדיר תכונה זו:

הנסיון הראשון הוא באמצעות הפסוק $\forall a\forall b\left(\exists x_0,\ldots,x_n\left(\left(a=x_0\right)\wedge\bigwedge_{i=0}^{n-1}E\left(x_i,x_{i+1}\right)\wedge\left(a_n=b\right)\right)\right)$. לרוע המזל, ההגדרה הזו אינה עובדת: היא מגדירה את אוסף הגרפים שבהם בין כל שני צמתים קיים מסלול מאורך n **בדיוק**. הסיבה לכך היא שבביטוי $\exists x_0,\ldots,x_n$ n הוא מספר **קבוע**, כלומר, הפסוק מכיל $n+1$ מופעים בדיוק של הכמת $\exists$; הוא אינו יכול להכיל מספר משתנה, ובפרט לא חסום, שלהם.

נסיון תיקון אפשרי אחד הוא זה: $\forall a\forall b\left(\exists n:\exists x_0,\ldots,x_n\left(\left(a=x_0\right)\wedge\bigwedge_{i=0}^{n-1}E\left(x_i,x_{i+1}\right)\wedge\left(a_n=b\right)\right)\right)$. לרוע המזל, אין משמעות לסימון כמו $\exists n:\exists x_0,\ldots,\exists x_n$ בשפה שלנו; מבחינה תחבירית, הפסוק הזה פשוט אינו קיים.

אם כן, אולי ההגדרה האלטרנטיבית באמצעות חלוקה תעבוד? ננסה באמצעות הנוסחה הבאה:

$$\exists A\exists B\left(\forall x\left(x\in A\vee x\in B\right)\wedge\forall x\neg\left(x\in A\wedge x\in B\right)\wedge\exists x\exists y\left(x\in A\wedge y\in B\wedge E\left(x,y\right)\right)\right)$$

הנוסחה הזו אכן מגדירה את כל הגרפים שהם קשירים, אבל היא לא מתאימה לשפה שלנו: A,B אינם משתנים שמקבלים צמתים, אלא **קבוצות** של צמתים, וסימן השייכות $\in$ צץ לו משום מקום. אמנם, אפשר להוסיף את סימן השייכות לשפה, ואולי גם לבנות אקסיומות שמבטיחות שהוא יתנהג כפי שאנו מצפים שהוא יתנהג, אבל המודלים שלנו כבר לא יהיו גרפים: הם יהיו חייבים להיות אוספים של צמתים ושל **קבוצות** של אותם הצמתים כדי שהמשתנים A,B יוכלו לקבל ערכים של קבוצות.

אם כן, השינוי שנדרש מאיתנו כדי שהנוסחה שלעיל תעבוד הוא עמוק יותר: עלינו לשנות את **הלוגיקה** שלנו (ולא רק את המילון) כדי שהכמת $\exists$ יוכל לטפל לא רק במשתנים אלא גם בקבוצות של משתנים. לוגיקה שבה הדבר אפשרי נקראת **לוגיקה מסדר שני.** הפסוק שהצגנו הוא אכן המחשה לכך שתכונת הקשירות של גרפים היא גדירה בלוגיקה מסדר שני, אך לא אומרת מאום על קשירות של גרפים בלוגיקה מסדר ראשון.

שני הכשלונות שלנו בנסיון להגדיר קשירות של גרפים בלוגיקה מסדר ראשון לא היו מקריים; התכונה פשוט איננה גדירה על ידי פסוק יחיד בלוגיקה מסדר ראשון. כדי לראות מדוע, נצטרך לפתח כלים נוספים.

6.7.2 משחקי Ehrenfeucht–Fraïssé

נפתח בהגדרה:

הגדרה 6.38 עומק הכמתים של נוסחה φ, שנסמן $D_Q\left(\varphi\right)$ מוגדר באינדוקציית מבנה:

- $D_Q\left(\varphi\right)=0$ עבור נוסחה אטומית φ.
- $D_Q\left(\neg\varphi\right)=D_Q\left(\varphi\right)$ ו־$D_Q\left(\varphi\odot\psi\right)=\max\left\{D_Q\left(\varphi\right),D_Q\left(\psi\right)\right\}$ לכל $\odot\in\left\{\rightarrow,\vee,\wedge,\leftrightarrow\right\}$.
- $D_Q\left(\forall x\varphi\right)=D_Q\left(\exists x\varphi\right)=D_Q\left(\varphi\right)+1$

במילים: עומק הכמתים של φ הוא המספר הגדול ביותר של צמתים המכילים כמת בתוך מסלול כלשהו בעץ המבנה של φ.

הגדרה 6.39 שני גרפים G_1,G_2 הם **שקולים אלמנטרית** מסדר n אם לכל פסוק φ (בשפת הגרפים מסדר ראשון) מעומק כמתים לכל היותר n מתקיים $G_1\models\varphi\iff G_2\models\varphi$. אם G_1,G_2 שקולים אלמנטרית מסדר n נסמן זאת ב־$G_1\equiv_n G_2$.

אם $G_1\cong G_2$ אז $G_1\equiv_n G_2$ לכל n, אך ההפך אינו נכון, והדבר מעיד על חולשה הביכולת הביטוי של לוגיקה מסדר ראשון ומאפשר לנו לדבר על אי־גדירות של תכונות:

משפט 6.40 תכונה $\mathcal{P}$ של גרפים איננה גדירה בלוגיקה מסדר ראשון אם לכל n טבעי קיימים $G_1\in\mathcal{P},G_2\notin\mathcal{P}$ כך ש־$G_1\equiv_n G_2$.

הוכחה: נניח כי $\mathcal{P}$ גדירה על ידי φ ויהי $n=D_Q(\varphi)$. אז מכיוון ש־$G_1\equiv_n G_2$ נקבל ש־$G_2\models\varphi \iff G_1\models\varphi$. מצד שני, $G_1\in\mathcal{P}=\mathrm{Mod}_f(\varphi)$ ולכן $G_1\models\varphi$ ואילו $G_2\notin\mathcal{P}=\mathrm{Mod}_f(\varphi)$ ולכן $G_2\not\models\varphi$ - סתירה. ■

המשפט לעיל מצביע על דרך קונקרטית מאוד להראות אי־גדירות של תכונה: לכל n טבעי, בסך הכל יש למצוא זוג גרפים שקולים מסדר n שהאחד מקיים אותה והשני לא, ושניהם שקולים. האתגר, כמובן, הוא בהוכחת השקילות שלהם. הכלי שבו נשתמש לצורך כך הוא משחקי Ehrenfeucht–Fraïssé .

הגדרה 6.41 בהינתן זוג גרפים (G_1,G_2) ומספר טבעי n, משחק Ehrenfeucht–Fraïssé עבור $((G_1,G_2),n)$ הוא משחק ב־n סיבובים בין שני שחקנים: ה"קלקלן" (Spoiler) וה"שכפלן" (Duplicator) המתנהל כך, בכל סיבוב $i\in 1,2,\dots,n$:

1. הקלקלן בוחר צומת $x\in G_1$ או צומת $y\in G_2$ שטרם נבחרה עד כה; אם הוא בחר צומת מ־G_1 אז נגדיר $a_i=x$, ואם הוא בחר צומת מ־G_2 אז נגדיר $b_i=y$.

2. השכפלן בוחר צומת $x\in G_1$ או צומת $y\in G_2$ שטרם נבחרה עד כה, ונלקחת מתוך הגרף שממנו הקלקלן **לא** בחר צומת בסיבוב זה. אם הוא בחר צומת מ־G_1 אז נגדיר $a_i=x$, ואם הוא בחר צומת מ־G_2 אז נגדיר $b_i=y$.

בסיום n הסיבובים נתונות שתי סדרות של צמתים, $a_1,\dots,a_n$ ו־$b_1,\dots,b_n$. השכפלן מנצח אם תתי הגרפים של G_1,G_2 המושרים על צמתי הסדרות הללו הם איזומורפיים; אחרת, הקלקלן מנצח.

בפני עצמו המשחק הוא חביב ומאתגר להפתיע, אך העניין שלנו בו נובע מהמשפט הבא:

משפט 6.42 זוג גרפים מקיים $G_1\equiv_n G_2$ אם ורק אם השכפלן יכול לשחק בצורה שמבטיחה נצחון בלי תלות בצעדי הקלקלן במשחק ב־n סיבובים על (G_1,G_2).

לא נוכיח כאן את המשפט. עם זאת, נשתמש במשפט כדי להוכיח כי קשירות אינה גדירה. נגדיר גרף $G_1=(\mathbb{Z},E_1)$ כך ש־$E_1=\{(a,a+1)\,|a\in\mathbb{Z}\}$, כלומר, צמתי הגרף ממוספרים במספרים שלמים כלשהם ויש קשת בדיוק בין שני מספרים סמוכים - הגרף נראה כמו "שרוך" אינסופי, ו־$G_2=(\mathbb{Z}\times\{0,1\},E_2)$ כך ש־$E_2=\{((a,1),(a+1,1))\,|a\in\mathbb{Z}\}\cup\{((a,2),(a+1,2))\,|a\in\mathbb{Z}\}$, כלומר G_2 הוא פשוט שני עותקים של G_1. בבירור G_1 קשיר בעוד ש־G_2 איננו קשיר.
יהא n טבעי כלשהו. השיטה שבה השכפלן צריך לשחק היא זו: אחרי הסיבוב הראשון אפשר להניח בלי הגבלת הכלליות ש־$a_1=0$ ו־$b_1=(0,1)$ (אחרת פשוט מבצעים שינוי מתאים לשמות צמתי הגרפים). כעת, לכל צומת חדשה שהקלקלן מסמן, אם היא במרחק n לכל היותר מצומת c_i שכבר נבחרה באותו הגרף, השכפלן בוחר בצומת שהעתק שלה מהתאומה של c_i בגרף השני זהה; ואם הצומת החדשה של הקלקלן אינה במרחק n מצומת קיימת, אז השכפלן בוחר עבורה צומת שרירותית כלשהי בגרף השני שנמצאת במרחק 2^n מכל צומת שכבר נבחרה. קל לראות שזוהי אכן אסטרטגיה שמבטיחה נצחון לשכפלן.

6.7.3 תורות שלמות: כללי ה־0־1 של גרפים ומבחן Łoś-Vaught

נציג כעת תוצאה חזקה ומפתיעה על גרפים, שהמפתח להוכחתה יעבור דרך הוכחה שתורה מסויימת היא שלמה; האופן שבו נוכיח שהתורה היא שלמה יהיה באמצעות משפט של Łoś-Vaught בתורת המודלים שנותן קריטריון לשלמות של תורה שמתבסס על איזומורפיזם של מודלים.
נתחיל עם הצגת התוצאה. בהינתן תכונה $\mathcal{P}$ של גרפים, נגדיר $p_n(\mathcal{P})\triangleq\frac{|\{G=(V,E)\in\mathcal{P}||V|=n\}|}{|\{G=(V,E)||V|=n\}|}$ כאשר אצלנו גרף בעל n צמתים הוא תמיד בעל קבוצת הצמתים $V=\{1,2,\dots,n\}$. אם כן, $p_n(\mathcal{P})$ הוא הפרופורציה של מספר הגרפים על n צמתים בעלי התכונה $\mathcal{P}$ ביחס למספרם הכולל של הגרפים בעלי n צמתים (זוהי **ההסתברות** שגרף מקרי על n צמתים יהיה בעל התכונה $\mathcal{P}$, אך לא נזדקק לנקודת מבט זו בהמשך). כעת נגדיר:
$p(\mathcal{P})\triangleq\lim_{n\to\infty}p_n(\mathcal{P})$.
במילים, $p(\mathcal{P})$ היא הפרופורציה לטווח ארוך בין מספר הגרפים בעלי התכונה ומספר הגרפים הכולל. אם למשל $p(\mathcal{P})=\frac{1}{2}$ אז אפשר לומר "בערך חצי מהגרפים הם בעלי התכונה $\mathcal{P}$", ואם $p(\mathcal{P})=1$ אז אפשר לומר "כמעט כל הגרפים הם בעלי התכונה $\mathcal{P}$" (שימו לב שלא ניתן לומר ש**כל** הגרפים הם בעלי התכונה $\mathcal{P}$, או אפילו לא ש"קיים n כך שכל הגרפים על n צמתים הם בעלי התכונה $\mathcal{P}$").
מכיוון שהגרפים הם בעלי צמתים ממוספרים, ויש $\binom{n}{2}$ קשתות פוטנציאליות בכל גרף, הרי שיש $2^{\binom{n}{2}}$ גרפים על n צמתים בסך הכל. לכן כדי שתכונה כלשהי תהיה בעלת פרופורציה גדולה מאפס צריך ש־$O\left(2^{\binom{n}{2}}\right)$ מהגרפים יהיו בעלי התכונה עבור לפחות חלק מה־n־ים.
לרוע המזל, חישוב מדויק של $p(\mathcal{P})$ יכול להיות קשה אפילו עבור תכונות פשוטות יחסית. לכן התוצאה הבאה חזקה ומפתיעה כל כך:

משפט 6.43 (כלל ה־0־1 של גרפים): אם $\mathcal{P}$ גדירה בלוגיקה מסדר ראשון, אז $p(\mathcal{P}) = 0$ או $p(\mathcal{P}) = 1$.

למעשה, קיימות למשפט הכללות מרחיקות לכת אך הן מצריכות הצגת מושגים מתורת הגרפים האקראיים ולכן נמנע מכך כעת.

במובן מסויים, מה שהמשפט מראה הוא שלוגיקה מסדר ראשון היא חלשה למדי בכל הנוגע ליכולת התיאור שלה: היא יכולה לתאר (על ידי פסוק יחיד) רק תכונות שממילא מתקיימות "כמעט בכל" הגרפים או "כמעט באף" גרף. עם זאת, מכיוון שתכונות טבעיות מסויימות ניתנת עדיין להגדרה בעזרת לוגיקה מסדר ראשון, המשפט מעניק לנו תובנה על אופן התנהגותן של תכונות אלו ־ תובנה שנובעת אך ורק מ**השפה** שבה אנו משתמשים כדי לתאר את התכונות הללו!

לצורך הוכחת המשפט נגדיר את התורה הבאה:

$$\mathrm{T} \triangleq \{\mathcal{P} | p(\mathcal{P}) = 1\}$$

דהיינו, T כוללת את כל הפסוקים בשפה שלנו שהתכונה שהם מגדירים היא בעלת פרופורציה 1. הטענה המרכזית שלנו היא ש־T היא תורה שלמה, כלומר לכל פסוק φ, $\mathrm{T} \vdash \varphi$ או ש־$\mathrm{T} \vdash \neg\varphi$ (במערכת ההוכחה הסטנדרטית של תחשיב היחסים).

נניח כי T שלמה ויהא φ פסוק כלשהו. אז אם $\mathrm{T} \vdash \varphi$ אז קיימת הוכחה ל־φ מתוך T ומכיוון שהיא סופית היא מערבת רק מספר סופי של פסוקים $\psi_1, \dots, \psi_k$. כלומר, $\{\psi_1, \dots, \psi_k\} \vdash \varphi$ וממשפט הנאותות לתחשיב היחסים, $\{\psi_1, \dots, \psi_k\} \models \varphi$, כלומר כל גרף שמקיים בו זמנית את כל התכונות $\psi_1, \dots, \psi_k$ מקיים גם את φ. ניתן להראות כי אם הפרופורציה של כל אחת מהתכונות $\psi_1, \dots, \psi_k$ היא 1, כך גם הפרופורציה של $\psi_1 \wedge \dots \wedge \psi_k$ ולכן הפרופורציה של φ היא 1. אם לעומת זאת $\mathrm{T} \vdash \neg\varphi$ אז נובע מכך שהפרופורציה של $\neg\varphi$ היא 1, כלומר הפרופורציה של φ היא אפס. מכאן שלכל תכונה $\mathcal{P}$, אם היא גדירה על ידי פסוק יחיד φ אז הפרופורציה שלה היא 0 או 1, כשל φ.

האתגר הוא להראות כי T היא תורה שלמה. כאן נחלץ לעזרתנו משפט מתורת המודלים, שנציג כאן ניסוח מפושט שלו:

משפט 6.44 (מבחן Łoś-Vaught) אם T תורה ללא מודלים סופיים וכל שני מודלים בני מניה שלה הם איזומורפיים, אז T שלמה.

הוכחה: אם T אינה שלמה אז יש פסוק φ כך ש־$\mathrm{T} \cup \{\varphi\}$ עקבית וגם $\mathrm{T} \cup \{\neg\varphi\}$ עקבית. ממשפט השלמות לתחשיב היחסים לשתי התורות הללו קיים מודל, וממשפט לוונהיים־סקולם נובע שלכל אחת מהתורות הללו יש מודל בן מניה. כלומר קיימים M_1, M_2 בני מניה כך ש־$M_1 \models \mathrm{T} \cup \{\varphi\}$ ו־$M_2 \models \mathrm{T} \cup \{\neg\varphi\}$.

בפרט M_1 ו־M_2 הם מודלים של T, ומכיוון ששניהם בני מניה, $M_1 \cong M_2$, אבל זו סתירה לכך ש־φ מתקיים באחד מהם ו־$\neg\varphi$ מתקיים בשני. ■

עלינו אם כן להראות כי ל־T יש מודל בן מניה יחיד עד כדי איזומורפיזם ואין לה מודלים סופיים. ראשית, נשים לב לכך שהתכונה "בגרף יש לפחות n צמתים" היא כמובן גדירה בלוגיקה מסדר ראשון (כבר ראינו זאת מוקדם יותר) והפרופורציה שלה היא 1 (כי היא מתקיימת לכל הגרפים מגודל n לפחות). לכן כל תכונה כזו שייכת ל־T ומכאן שאין ל־T מודלים סופיים (כי מודל בן n צמתים לא מקיים את התכונה "בגרף יש לפחות $n+1$ צמתים").

אם כן, הוכחת כלל ה־0־1 של גרפים קמה ונופלת על קיום גרף **אינסופי** בן מניה יחיד שמקיים כל תכונה שהיא בעלת פרופורציה 1 על גרפים **סופיים**. זה מראה שבאופן מפתיע, עלינו להבין גרפים אינסופיים כדי להבין גרפים סופיים.

נניח בשלילה שיש שני גרפים G_1, G_2 שהם בני מניה עם קבוצות צמתים $V_1 = \{a_1, a_2, \dots\}$ ו־$V_2 = \{b_1, b_2, \dots\}$ ושניהם מודלים של T. נרצה להראות שהם איזומורפיים, כלומר שקיימת פונקציה $f: V_1 \to V_2$ כך ש־$(u,v) \in E_1$ אם ורק אם $(f(u), f(v)) \in E_2$. נגדיר את f באופן אינדוקטיבי, בשיטה שהומצאה על ידי קנטור.

נתחיל בהגדרה $f(a_1) = b_1$. כעת, נניח באינדוקציה כי כבר הגדרנו את f עבור כל הצמתים $\{a_1, \dots, a_n\}$ ונגדיר אותה עבור a_{n+1}. ללא הגבלת הכלליות נניח כי $f(a_i) = b_i$ עבור $1 \le i \le n$ (ניתן להניח זאת על ידי מספור מחדש של צמתי V_2 במידת הצורך). נגדיר תת־קבוצה $S \triangleq \{a_i | 1 \le i \le n \wedge (a_i, a_{n+1}) \in E_1\}$, כלומר S היא קבוצת כל השכנים של a_{n+1} מקרב $\{a_1, \dots, a_n\}$. נסמן $\overline{S} = \{a_1, \dots, a_n\} \backslash S$. אם קיים $b \in V_2$ שאינו שייך לקבוצה $\{b_1, \dots, b_n\}$ ומקיים את התכונה ש־b מחובר לכל אברי $f(S)$ ואינו מחובר לכל אברי $f(\overline{S})$, סיימנו; נגדיר $b_{n+1} = f(a_{n+1}) = b$. נותר רק להוכיח כי **תמיד** קיים ב־G_2 צומת כזה.

כדי לראות שב־G_2 קיים צומת שכזה, נוכיח כי בין הפסוקים של T (שאת כולם G_2 מקיים) קיים אחד שאומר בדיוק את מה שאנחנו רוצים. ספציפית, עבור $n \ge m$, נגדיר את "אקסיומת ההרחבה" $\mathrm{EA}_{n,m}$ בתור הפסוק שאומר "לכל קבוצה X מגודל n ותת־קבוצה שלה $Y \subseteq X$ שלה מגודל m קיים איבר שאינו ב־X שמחובר לכל אברי Y ואינו מחובר לכל איבר ב־X שאינו ב־Y" (אצלנו $X = \{b_1, \dots, b_n\}$, $Y = f(S)$). בכתיבת אקסיומה זו לא ניתקל באותן בעיות שנתקלנו בהן בעת הנסיונות לכתיבת נוסחה עבור קשירות, מכיוון ש־n, m הם קבועים (עבור $\mathrm{EA}_{n,m}$ ספציפית). פורמלית האקסיומה נכתבת כך:

$$\mathrm{EA}_{n,m} \;=\; \forall x_1,\ldots,x_n\left[\left(\left(\bigwedge_{i\neq j}\neg\left(x_i=x_j\right)\right)\rightarrow\exists y\left(\bigwedge_{i=1}^{n}y\neq x_i\wedge\bigwedge_{i\leq m}E\left(y,x_i\right)\wedge\bigwedge_{i>m}\neg E\left(y,x_i\right)\right)\right)\right]$$

ההוכחה איננה שלמה שכן יש להראות כי $\mathrm{EA}_{n,m}\in\mathrm{T}$, דהיינו שהפרופורציה של הגרפים שמקיימים את התכונה היא 1. לא נראה זאת כאן, מכיוון שהדרך הפשוטה להראות זאת כרוכה בשימוש בשיקולים הסתברותיים. רק נציין כי העובדה שהמודל G עבור T מקיים את $\mathrm{EA}_{n,m}$ לכל $n\geq m$ מעידה על כך ש־G הוא גרף מיוחד, במובן זה ש**כל** תבנית סופית נמצאת בו. לגרף זה שם מיוחד: גרף Rado (או גרף Erdős–Renyi).

6.8 סיכום: התוכנית של הילברט ומשפטי אי השלמות של גדל

נסכם את הקורס על ידי סקירה היסטורית קצרה של התפתחות הלוגיקה במאה ה־20 לאור מה שנלמד בקורס.

6.8.1 התוכנית של הילברט

הלוגיקה המתמטית המודרנית הומצאה בידי המתמטיקאי הגרמני גוטלוב פרגה בשנות השבעים של המאה ה־19. הניסוחים המדוייקים (והסימונים) היו שונים למדי מאלו של הלוגיקה מסדר ראשון שראינו בקורס, אך רוח הדברים הייתה זהה. פרגה קיווה שהלוגיקה תוכל לתאר את כל המתמטיקה, אך גילויי הפרדוקסים של תורת הקבוצות הנאיבית (ובפרט הפרדוקס של ראסל) ריפו את ידיו במידת מה.

המתמטיקאי הבולט ביותר שהמריץ את העיסוק בלוגיקה במאה ה־20 היה דויד הילברט. בשנת 1899 פורסם ספר של הילברט שבו ניסח מחדש את הגאומטריה האוקלידית בגרסה אקסיומטית מדוייקת יותר מזו של אוקלידס. בהשראת עבודה זו, הילברט סבר שניתן לטפל באופן אקסיומטי גם בתחומים מתמטיים אחרים, ובמאמר משנת 1900 פרסם מערכת אקסיומטית עבור המספרים הממשיים (ולכן עבור האנליזה).

בהגדרות שראינו בקורס ניתן לחשוב על **מערכת אקסיומטית** כעל **תורה**, דהיינו אוסף של פסוקים בלוגיקה מסדר ראשון. מערכת אקסיומטית עבור המספרים הממשיים, אם כן, היא תורה ש־$\mathbb{R}$ הוא מודל שלה. אפשר למדוד את "איכות" המערכת האקסיומטית במספר דרכים שונות:

1. עקביות: אם ניתן להוכיח סתירה מתוך התורה, זהו אסון מוחלט. פירוש הדבר הוא שלתורה **אין מודל**, ולכן בפרט המספרים הממשיים אינם מודל של התורה. כמו כן פירוש הדבר הוא שאפשר להוכיח "הכל" מהתורה ולכן היא איננה מעניינת.

2. שלמות: מטרתה של תורה היא להוכיח דברים. קל לתת תורה ש־$\mathbb{R}$ היא מודל שלה ־ "תורה" ללא אקסיומות כלל, אך בתורה זו לא ניתן יהיה להוכיח שום תוצאה שהיא נכונה עבור $\mathbb{R}$ אבל לא נכונה עבור מודלים פוטנציאליים אחרים. אם כן, ככל שישנן יותר אקסיומות והתיאור של $\mathbb{R}$ הוא יותר טוב, כך תגבר היכולת שלנו להוכיח דברים שנכונים ב־$\mathbb{R}$. שימו לב כי בעיות כמו זו שמשפט לוונהיים־סקולם מצביע עליהן אינן רלוונטיות פה; משפט לוונהיים־סקולם מראה כי לתורה עבור $\mathbb{R}$ עשויים להיות מודלים אחרים, מעוצמות אחרות, אך מודלים אלו הם שקולים אלמנטרית ל־$\mathbb{R}$, במובן זה שאין משפט שאפשר לנסח בלוגיקה מסדר ראשון והוא נכון ב־$\mathbb{R}$ אך אינו נכון בהם. במילים אחרות, משפט לוונהיים־סקולם לא עומד בסתירה לשלמות האפשרית של תורה.

3. אפקטיביות: האקסיומות צריכות להיות פשוטות. יותר מכך ־ רצוי שהן יהיו **אמינות**, במובן זה שיהיה קשה לפקפק בנכונותן.

הבעיה העיקרית של הילברט עם מערכת האקסיומות שלו עבור $\mathbb{R}$ הייתה בעיית העקביות. את עקביות הגאומטריה שלו הילברט הוכיח על ידי בניית מודל מפורש עבור אקסיומות הגאומטריה. מרגע שהראינו מודל שכזה, המערכת אינה יכולה שלא להיות עקבית כי אם היא הייתה מוכיח פסוק והיפוכו, אז גם הפסוק וגם היפוכו היו צריכים להתקיים במודל וזה בלתי אפשרי. עבור $\mathbb{R}$ לעומת זאת לא היה ניתן לנקוט בתעלול דומה, כי **הבניות של הממשיים עצמן היו שנויות במחלוקת**.

לכל אורך המאה ה־19 "נאבקו" המתמטיקאים במושג האינסוף. בפרט קושי ו־ויירשטראס המציאו את מושג הגבול על מנת לנסח מחדש את החשבון האינפיניטסימלי מבלי להזדקק ליצורים שהם "קטנים באופן אינסופי" או "גדולים באופן אינסופי". לרוע המזל, החשבון האינפיניטסימלי עדיין נוסח על המספרים הממשיים, ובניה פורמלית שלהם לא הייתה קיימת עד לקראת סוף המאה ה־19. אז נתנו קנטור ודדקינד בניות שונות עבור הממשיים. שתי הבניות מעניינות ולכל אחת שימושים והכללות משל עצמה, אך התכונה שמשותפת לשתיהן היא שבשתיהן התיאור של כל מספר ממשי הוא **אינסופי**, מה שהחזיר את האינסוף

חזרה אל תוך המתמטיקה (כדאי לשים לב לכך שהדבר הכרחי; אם כל מספר ממשי היה ניתן לתיאור סופי היה נובע מכך שקיימים רק $\aleph_0$ מספרים ממשיים).

מכיוון שהאינסוף היה בגדר "חשוד" באותם ימים במתמטיקה, הבניות של קנטור ודדקינד לא נתפסו כאילו הן בהכרח "מוכיחות" את קיומם של המספרים הממשיים, וזאת בגלל הסתמכותן על האינסוף. הילברט קיווה שניתן יהיה לנקוט בגישה שונה לגמרי ־ להוכיח שהמערכת הפורמלית שהוא הגדיר עבור המספרים הממשיים אינה מובילה לסתירה. בבסיס גישה זו עמדה אמונתו של הילברט כי די בכך שמערכת אקסיומות לא תוביל לסתירה כדי שהאובייקט המתמטי אותו היא מתארת ייחשב קיים:

> But if it can be proved that the attributes assigned to the concept can never lead to a contradiction by the application of a finite number of logical processes, I say that the mathematical existence of the concept (for example, of a number or a function which satisfies certain conditions) is thereby proved.

הילברט הציג את הוכחת העקביות של מערכת האקסיומות שלו בתור הבעיה השניה מבין 23 הבעיות שלו בנאומו המפורסם בקונגרס המתמטי של פריז ב־1900. לאחר מכן פחת עיסוקו בנושאי לוגיקה ל־20 שנה בערך.

בשנות ה־20 של המאה ה־20 הילברט חזר לעסוק בנושאים הללו במלוא כוחו. היעד שלו כעת ־ שזכה לשם "תוכנית הילברט" ־ היה ברור יותר ושאפתני יותר ־ למצוא מערכת אקסיומטית עבור **כל המתמטיקה**, וכזו שתהיה "סופית" באופיה, ובוודאי שתהיה נאותה ושלמה. האתגר המרכזי היה לטפל במספרים הטבעיים: ברור כי כל מערכת אקסיומות שתתאר את כל המתמטיקה תצטרך לטפל גם בהם בין היתר. מערכות אקסיומות כאלו הוצעו, אך לא הושגה הצלחה בהוכחת עקביות ושלמות עבורן.

יעד שאפתני נוסף שהגה הילברט היה מציאת אלגוריתם שיהיה מסוגל, בהינתן תורה מסדר ראשון כלשהי Φ ופסוק φ, לקבוע האם φ נובע לוגית מתוך Φ. בעיה זו כונתה "בעיית הכרעה" (ומכיוון שהילברט היה גרמני, Entscheidungsproblem). נשים לב כי אם Φהיא תורה שלמה, כלומר אם לכל φ מתקיים $\Phi\vdash\varphi$ או $\Phi\vdash\neg\varphi$, ובהנחה שקיים אלגוריתם שמסוגל לבדוק אם פסוק כלשהו שייך ל־Φ או לא, אז **קיים** פתרון טריוויאלי לבעיית ההכרעה הזו: פשוט מייצרים באופן סדרתי את **כל** ההוכחות האפשריות מתוך Φ עד אשר נתקלים בהוכחה ל־φ (ואז φ נובע לוגית מ־Φ) או בהוכחה ל־$\neg\varphi$ (ואז φ אינו נובע לוגית מתוך Φ). אם כן, מערכת אקסיומות לכל המתמטיקה שהיא עקבית, שלמה ואפקטיבית תפתור מאליה את בעיית ההכרעה של הילברט, אך אי קיומה של מערכת אקסיומות שכזו לא שולל את האפשרות התיאורטית של קיום אלגוריתם שכזה.

6.8.2 משפטי אי השלמות של גדל

בשנת 1931 פרסם מתמטיקאי צעיר בשם קורט גדל מאמר בשם "על טענות בלתי ניתנות להוכחה ב־Principa Mathematica ומערכות דומות" שהראה כי תוכנית הילברט היא שאפתנית מדי והיעד אליו היא חותרת הוא בלתי אפשרית. יתר על כן, הבעיה איננה במערכת אקסיומות ספציפית שהתוכנית של הילברט מקדמת, אלא בחוסר יכולת **עקרונית** לבנות מערכת אקסיומות טובה.

למשפטים שגדל הוכיח במאמרו יש ניסוחים פופולריים שגויים רבים (שנציג בקרוב), ולכן ננסה לנסח אותם באופן זהיר. אנו עוסקים כאן **רק** בלוגיקה מסדר ראשון, אף שניתן בתיאוריה להכליל את משפט גדל גם ללוגיקות אחרות, **הכללה כזו אינה מיידית**.לדוגמה, עבור לוגיקה מסדר שני משפט גדל כלל אינו תקף, אך עבור לוגיקה מסדר שני לא קיימת מערכת הוכחה שלמה ונאותה כך שהיא אינה רלוונטית כלל לדיון כולו.

הבה ונגדיר במסודר מספר תכונות שתורה Φ בלוגיקה מסדר ראשון (עבור מילון כלשהו) יכולה לקיים:

1. עקביות: לא קיים ψ כך ש־$\Phi\vdash\psi$ וגם $\Phi\vdash\neg\psi$.
2. שלמות: לכל ψ מתקיים $\Phi\vdash\psi$ או $\Phi\vdash\neg\psi$.
3. אפקטיביות: קיים אלגוריתם כך שבהינתן פסוק ψ עוצר אחרי מספר סופי של צעדים ועונה האם $\psi\in\Phi$ או $\psi\notin\Phi$.
4. אריתמטיות: לצורך פשטות ננסח דרישה זו בתור "התורה כוללת בתוכה את אקסיומות פיאנו". דהיינו, המילון של השפה של Φ מכיל סימן קבוע עבור 0, מכיל סימן פונקציה חד מקומית S עבור פעולת העוקב, מכיל סימני פונקציה $+,\cdot$ עבור פעולות הכפל, סימן יחס $<$ עבור היחס "קטן מ" ואת האקסיומות המתאימות לסימנים הללו. עם זאת, גם מערכות שאינן כוללות בדיוק את אקסיומות פיאנו אלא משהו דומה להן עדיין יהיו פגיעות למשפט אי השלמות של גדל, אך צריך להיות זהירים למדי כאן (נראה בהמשך דוגמה למורכבות של דרישה זו).

את משפט אי השלמות הראשון של גדל ניתן כעת לנסח כך: לא קיימת תורה Φ שהיא בו זמנית עקבית, שלמה, אפקטיבית ואריתמטית. בניסוח מעט שונה: אם Φ היא תורה עקבית, אפקטיבית ואריתמטית אז היא אינה שלמה, כלומר יש פסוק φ

כך ש־φ ⊭ Φ וגם $\neg\varphi$ ⊭ Φ. מכיוון ש**מערכת ההוכחה** של תחשיב היחסים היא שלמה (זהו משפט ה**שלמות** של גדל), פירוש הדבר הוא שקיימים ל־Φ שני מודלים $\mathcal{M}_1, \mathcal{M}_2$ כך ש־$\mathcal{M}_1 \models \varphi$ ו־$\mathcal{M}_2 \models \neg\varphi$.

ברור כי דרישות העקביות והאפקטיביות הן הכרחיות לכל תורה מתמטית בעלת ערך (אין טעם בתורה שממנה ניתן להוכיח הכל כי אינה מתארת כלום ולכן עקביות היא הכרחית; ואין טעם בתורה שלא ניתן לבדוק הוכחות שנובעות ממנה כי כלל לא ניתן לבדוק אם פסוק הוא אכן אקסיומה של התורה או לא). לעומת זאת, דרישת האריתמטיות **אינה** נפוצה עד כדי כך, וקיימות תורות מתמטיות רבות ש**אינן** מקיימות אותה.

בפרט, שלוש דוגמאות לתורות שהן עקביות, אפקטיביות ושלמות הן אלו: הגאומטריה האוקלידית, התורה של שדות ממשיים סגורים (שלא נתאר כאן במפורש) ו**אריתמטיקת פרסבורגר**, כאשר השלישית היא תיאור של המספרים הטבעיים הדומה מאוד לאקסיומות פיאנו, וההבדל המהותי בין שתי התורות הללו הוא שבאריתמטיקת פרסבורגר פעולת הכפל אינה קיימת. פירוש הדבר הוא שכמות הטענות שניתן **לנסח** באמצעות השפה של אריתמטיקת פרסבורגר על הטבעיים הוא קטן יותר, אך היתרון הוא שלכל טענה שכן ניתן לנסח במסגרת אריתמטיקת פרסבורגר קיימת הוכחה או הפרכה במסגרתה.

6.8.3 סקירה של הוכחת משפט אי השלמות הראשון

יש מספר דרכים להציג את האופן שבו מוכיחים את משפט אי השלמות הראשון. אולי הפופולריות ביותר היא לומר שבמסגרת הוכחת המשפט, בונים פסוק G שאומר "אין לי הוכחה מתוך Φ". זוהי מעין וריאציה מתמטית על פרדוקס השקרן (שבו איש כרתים אומר ש"כל אנשי כרתים הם שקרנים ואי אפשר להאמין לאף מילה שלהם"). ברור כי G חייב להיות נכון, כי אם G אינו נכון, אז קיימת לו הוכחה מתוך Φ, אבל מכיוון ש־Φ עקבית ומערכת ההוכחה שלנו נאותה עולה מכך ש־G גם הוא נכון.

דרך ההצגה הזו מלווה בלא מעט נפנוף ידיים, בפרט מכיוון שלא ברורה המשמעות של זה ש־G אומר ש"אין לו הוכחה", וגם לא ברור מה פירוש "נכון" כאן; הרי אנחנו רגילים לחשוב על פסוקים כ"נכונים" אם הם נובעים לוגית מ־Φ, אבל ממשפט השלמות של גדל כל מה שנובע לוגית מ־Φ הוא גם יכיח ממנה. לכן ברור שבדרך ההצגה הפשטנית הזו (שהיא מה שרוב ספרי המדע הפופולרי מסתפקים בה) יש בעיה.

הניסוח המדויק יותר של הטענה שלעיל הוא זה: במודל הספציפי של המספרים הטבעיים $\mathbb{N}$, הפסוק G מצליח בדרך מחוכמת מאוד לומר שאין לו הוכחה מתוך Φ. במילים אחרות, אם G נכון **במודל הספציפי** $\mathbb{N}$, אז לא קיימת לו הוכחה מ־Φ. כעת אנו מסיקים ש־G חייב להיות נכון ב־$\mathbb{N}$ כי אחרת היה נובע מכך שקיימת לו הוכחה ב־Φ, מה שמוביל אותנו לסתירה (כי אם קיימת ל־G הוכחה ב־Φ אז Φ נכון ב**כל** מודל של Φ ובפרט ב־$\mathbb{N}$, וכבר אמרנו שהמשמעות של נכונות ב־$\mathbb{N}$ היא שלא קיימת הוכחה ל־G ב־Φ).

שימו לב למה שמשתמע מכך: G הוא נכון ב־$\mathbb{N}$, אבל בהכרח קיים מודל אחר של Φ שבו G **אינו נכון** (ובנוסף, האופן שבו G מתפרש במודל הזה לא אומר כלום על שאלת היכיחות של G מ־Φ). לכן הניסוח הפופולרי של משפט גדל לפיו "קיים תמיד משפט שהוא נכון אך אינו יכיח" הוא בעייתי; צריך להבהיר שהנכונות היא תמיד במודל הספציפי של המספרים הטבעיים (מה שמצריך היכרות קודמת עם המושג של מודל לתורה).

האתגר המהותי בהוכחת משפט אי השלמות היא בניית G כזה, שמצליח איכשהו באמצעות טענה **על המספרים הטבעיים** לטעון טענה **על מערכות הוכחה** ובפרט כזו שמערבת את עצמו. כדי להשיג את האפקט הזה גדל השתמש בכמה תעלולים מחוכמים למדי.

מספור גדל השלב הראשון בהוכחה של גדל הוא להמיר טענות על פסוקים והוכחות לטענות על מספרים. לצורך כך יש להמיר פסוקים והוכחות למספרים. הרעיון נראה פשוט למדי כיום, שכן אנחנו משתמשים ללא הרף באמצעי קידוד ־ כל קובץ טקסט מקודד במחשב בסופו של דבר למספר. בזמנו של גדל הרעיון היה חדשני למדי.

גדל התאים לכל סימן בשפה מסדר ראשון של Φ מספר ייחודי ־ למשל, $5=|\forall|$, או $17=|+|$, וכדומה. כעת, בהינתן פסוק φ, אפשר להתאים לו מספר $|\varphi|$ באופן הבא: אם $\varphi=\sigma_1\sigma_2\cdots\sigma_k$ כאשר σ_i הם סימנים מתוך השפה, אז $|\varphi|=2^{|\sigma_1|}3^{|\sigma_2|}\cdots p_k^{|\sigma_k|}$ כאשר p_k הוא הראשוני ה־k. בשל העובדה שלכל מספר יש הצגה יחידה כמכפלה של ראשוניים ("המשפט היסודי של האריתמטיקה") זה מבטיח שכל פסוק יזכה לקידוד ייחודי. קיימות, כמובן, שיטות קידוד נוספות, אך זו השיטה שבה השתמש גדל.

כעת אפשר לקודד הוכחות בדרך דומה: הוכחה היא בסך הכל סדרה סופית של פסוקים, $\varphi_1,\varphi_2,\ldots,\varphi_k$ ולכן אפשר לקודד אותה על ידי $2^{|\varphi_1|}3^{|\varphi_2|}\cdots p_k^{|\varphi_k|}$. השלמנו את המעבר לדיבור על מספרים טבעיים: לכל נוסחה ולכל הוכחה יש מספר טבעי ייחודי שמקודד אותה (כמובן, ייתכן שיהיו פסוקים בעלי אותו קידוד כמו הוכחה מסויימת, אבל לא תהיה סיטואציה שבה לא נדע אם להתייחס למספר כאילו הוא מייצג קידוד של הוכחה או של פסוק ספציפי).

פונקציות רקורסיביות

בשלב הבא גדל מגדיר את המושג של **פונקציה רקורסיבית**. פונקציה רקורסיבית מוגדרת באינדוקציית מבנה באופן הבא על אוסף כל הפונקציות $f:\mathbb{N}^n\to\mathbb{N}$ (עבור כל n):

בסיס:

1. $f(x_1,\ldots,x_n)=0$ היא רקורסיבית (הפונקציה הקבועה אפס).
2. $g(x)=x+1$ היא רקורסיבית (פונקצית העוקב).
3. $h_i(x_1,\ldots,x_n)=x_i$ היא רקורסיבית (הטלה על הרכיב ה־i).

צעד:

1. הרכבה: אם $f(x_1,\ldots,x_n)$ היא רקורסיבית ו־$g_1(y_1,\ldots,y_m),\ldots,g_n(y_1,\ldots,y_m)$ הן רקורסיביות, כך גם הפונקציה

$$h(y_1,\ldots,y_m) = f(g_1(y_1,\ldots,y_m),\ldots,g_n(y_1,\ldots,y_m))$$

2. רקורסיה: אם $f(y,z,x_1,\ldots,x_n)$ רקורסיבית ו־$g(x_1,\ldots,x_n)$ רקורסיבית, כך גם הפונקציה $h(y,x_1,\ldots,x_n)$ המוגדרת באופן הבא:

$$\begin{aligned}h(0,x_1,\ldots,x_n) &= g(x_1,\ldots,x_n)\\ h(n+1,x_1,\ldots,x_n) &= f(n,h(n,x_1,\ldots,x_n),x_1,\ldots,x_n)\end{aligned}$$

במילים אחרות, h מוגדרת רקורסיבית על פי המשתנה הראשון שלה, כאשר יתר המשתנים הם "פרמטרים". הפונקציה g משמשת כאן בתור "תנאי ההתחלה" ו־f משמשת בתור הפעלת הרקורסיה.

הסיבה לפיה הפונקציות הרקורסיביות מעניינות היא שהן בבירור ניתנות לחישוב בצורה פשוטה, ומצד שני ניתן לבנות פונקציות רקורסיבות שמבצעות דברים מחוכמים ביותר.

מרגע שהוגדרה פונקציה רקורסיבית אפשר להגדיר גם "יחס רקורסיבי" בתור יחס שהפונקציה המציינת שלו רקורסיבית (הפונקציה המציינת של יחס S היא פונקציה $\chi_S:\mathbb{N}^n\to\{0,1\}$ כך ש־$\chi_S(x_1,\ldots,x_n)=1$ אם ורק אם $(x_1,\ldots,x_n)\in S$).

גדל בונה בהדרגה אוסף הולך וגדל של יחסים רקורסיביים: הוא מראה שפעולות החשבון הן רקורסיביות, שהיחס "x מחלק את y" הוא רקורסיבי, שהיחס "x הוא ראשוני" הוא רקורסיבי, שפונקציית העצרת היא רקורסיבית וכן הלאה. הוא מראה כיצד יחסים רקורסיביים מסוגלים "לפענח" את שיטת הקידוד שלו ולזהות את המחרוזת המקורית שמקודדת בתוך מספר, ולבסוף הוא מראה כיצד יחסים רקורסיביים מסוגלים לבדוק שהוכחה מתוך Φ, שמקודדת על ידי מספר נתון, היא תקפה. זהו שלב טכני ארוך של המאמר, וגדל מגדיר לא פחות מ־45 יחסים לפני שהוא מגיע ליעד של יחס $B\subseteq\mathbb{N}^2$ שמשמעותו היא זו: $(x,y)\in B$ אם ורק אם x מקודד **הוכחה** עבור **הנוסחה** ש־y מקודד.

מבחינה רעיונית אין דבר מפתיע כאן - כל מתכנת מתחיל יכול לכתוב תוכנית מחשב שמפענחת את הקידוד של גדל ומבצעת את אותה בדיקה בדיוק, אבל גדל עושה זאת באמצעות יחסים רקורסיביים שאותם הוא מגדיר מדברים בסיסיים ביותר - הוא "מתכנת באסמבלי של המתמטיקה".

6.8.4 סיום ההוכחה

גדל מראה כעת כי במערכת שעליה הוא מדבר במאמר ניתן לייצג את הפונקציות הרקורסיביות באמצעות השפה הקיימת (שכוללת, כזכור, את פעולות החיבור והכפל). לצורך כך הוא נזקק לכמה תעלולים מתמטיים מתורת המספרים שחורגים מהיקף החומר שנוכל לתאר כאן ולכן לא ניכנס לפרטים. מעתה ואילך ניתן להניח ש־$B(x,y)$ שתיארנו הוא יחס שניתן להשתמש בו בתוך נוסחאות בשפה שלנו, ובמודל של $\mathbb{N}$ המשמעות של B היא המשמעות המקורית שלו (כלומר, הנוסחה האטומית $B(x,y)$ מקבל T במודל $\mathbb{N}$ אם x מוכיח את y).

כעת האינטואיציה היא שניתן להגדיר את הפסוק G ("לא קיימת לי הוכחה ב־Φ") כך:

$$G = \neg\exists x\,(B(x,|G|))$$

(כאן $|G|$ הוא קבוע מספרי כלשהו שניתן לתאר בתור $S(S(S(\cdots S(0))))$ עבור מספר גדול מאוד של הפעלות של S).

לרוע המזל, אי אפשר לבנות פסוק בצורה הזו באופן ישיר, כי כל עוד לא סיימנו את כתיבת הפסוק G איננו יודעים כלל מה יהיה המספר שלו; ויותר מכך, כל תו שאנחנו מוסיפים ל־G משנה את המספר שלו, ומצריך אותנו לשנות את התווים הקיימים של G, ולכן שוב לשנות את המספר שלו וחוזר חלילה. זהו אותו הקושי שבכתיבת תוכנית מחשב הפולטת את הקוד שלה עצמה.

אלא שאת הבעיה הזו ניתן לעקוף (כמו גם את הבעיה של תוכנית מחשב שכותבת את הקוד של עצמה) וגדל עושה זאת בצורה ערמומית למדי.

ראשית, בהינתן נוסחה $\varphi(x)$ עם משתנה חופשי יחיד x, ניתן להציב בתוך φ, בכל מקום שבו מופיע x, את שם העצם $|\varphi|$ (שמייצג את מספר גדל של הקידוד של φ) ולקבל את הפסוק $\varphi(|\varphi|)$. שימו לב שלפסוק זה מספר גדול **שונה** משל φ והוא באופן כללי שונה מ־φ (שהרי φ היא נוסחה עם משתנה חופשי ואילו $\varphi(|\varphi|)$ הוא פסוק). ל־$\varphi(|\varphi|)$ נקרא **הלכסון** של φ.

כעת ניתן להגדיר את הפונקציה הבאה: $\mathrm{diag}(|\varphi|) = |\varphi(|\varphi|)|$. במילים אחרות, $\mathrm{diag}(x) = y$ אם y הוא מספר גדל של הלכסון של הנוסחה שמספר גדל שלה הוא x. ניתן להוכיח כי גם diag היא פונקציה רקורסיבית ולכן ניתנת לייצוג בתורה שלנו.

השלב הלפני אחרון בבניה הוא זה: נגדיר נוסחה $U(y) = \neg\exists x(B(x, \mathrm{diag}(y)))$. כלומר, U היא נוסחה שמקבלת את מספר גדל של פסוק כלשהו y, ואומרת (בפרשנות שלה במודל $\mathbb{N}$) ש"לא קיימת הוכחה ל־$\mathrm{diag}(y)$".

וכעת הגענו לשלב האחרון: נגדיר $G = \mathrm{diag}(U) = U(|U|)$. כלומר, G אומרת "לא קיימת הוכחה ל־$\mathrm{diag}(U)$", אבל $\mathrm{diag}(U)$ הוא G עצמה! על כן, G אומרת בדיוק ש"לא קיימת ל־G הוכחה מתוך Φ", מה שמסיים את הוכחת משפט אי השלמות של גדל.

6.9 משפט אי השלמות השני של גדל

אחת המסקנות שנובעות ממשפט אי השלמות הראשון היא שתורות מסויימות ־ בפרט אריתמטיקת פיאנו ־ אינן מסוגלות להוכיח את העקביות שלהן עצמן. לא נציג כעת את האופן שבו המשפט השני נובע מהראשון, אלא נסתפק בדיון קצר על המסקנה.

בעוד שמשפט אי השלמות הראשון של גדל מנחית מהלומה על תקוותו של הילברט למצוא מערכת אקסיומות אחת שניתן יהיה להסיק ממנה את כל המתמטיקה, המשפט השני מטיל צל גדול גם על התקווה לפתור את הבעיה ששורשיה כבר בבעיה אותה הציג כבר בקונגרס המתמטי של 1900 ־ להוכיח שאקסיומות האריתמטיקה הן עקביות מבלי להסתמך על בניית מודל מפורש.

כדאי להעיר שהבעיה אינה בכך שלא ניתן להוכיח את עקביות האריתמטיקה מתוך האריתמטיקה, שהרי על הוכחה שכזו לא ניתן לסמוך ממילא (שהרי אם האריתמטיקה **אינה** עקבית אז אפשר "להוכיח" ממנה הכל, ובפרט את עקביות האריתמטיקה). העניין הוא בכך שאם אפילו האריתמטיקה אינה יכולה להוכיח את העקביות של עצמה, בוודאי שכל מערכת **חלשה** ממנה לא תוכל לעשות זאת. לכן, על מנת להוכיח את עקביות האריתמטיקה, יש הכרח להשתמש באקסיומות שנכונותן גם היא תהיה מוטלת בספק מסויים. כך קרה בשנת 1936 כאשר גרהרד גנצן, אחד מהסטודנטים הרבים של הילברט, הוכיח את עקביות האריתמטיקה בהתבסס על הנחות טכניות מסויימות שלא נציג כאן, אך הן כוללות מרכיב "אינסופי" כלשהו.

נחדד נקודה זו, שספרי מדע פופולרי רבים כושלים בה: **קיימות** הוכחות לעקביות האריתמטיקה; הן בהכרח מתבססות על עקרונות אחרים שאפשר לפקפק בהם, ואינן פשוטות כפי שהילברט קיווה שיהיו, אך גדל לא הוכיח שהוכחות כאלו לא יכולות להתקיים כלל, אלא רק שהן לא יכולות להתקיים אם מסתפקים בכלים הבסיסיים של האריתמטיקה עצמה.

6.10 כמה תפיסות שגויות של משפטי גדל

נציג כעת כמה ציטוטים שנשמעים לעתים בהקשר למשפטי גדל ונעמוד על השגיאות שבהם.

- "משפט גדל מראה שקיים משפט נכון שלא ניתן להוכיח" ־ זהו כשל של "היפוך סדר הכמתים" ־ מה שמשפט גדל מראה הוא ש**לכל** תורה Φ (אפקטיבית, אריתמטית ועקבית) יהיה **קיים** פסוק שהוא נכון ב־$\mathbb{N}$ אך אינו יכיח מ־Φ; הניסוח הפופולרי אומר דבר חזק בהרבה: **שקיים** פסוק שהוא נכון ב־$\mathbb{N}$ אך **לכל** תורה Φ הוא אינו יכיח. טענה חזקה זו היא בבירור שגויה, שכן אם φ אינו יכיח מ־Φ אז $\Phi \cup \{\varphi\}$ היא עקבית, אריתמטית ואפקטיבית וניתן להוכיח ממנה את φ (אך יהיה פסוק אחר שאינו יכיח ממנה).

- "לפני משפטי גדל חשבו שכל דבר שהוא אמת אפשר להוכיח, עכשיו יודעים שזה לא נכון" ־ יש לזכור כי גדל עצמו הוכיח שלכל תורה Φ בלוגיקה מסדר ראשון, אם יש פסוק φ שהוא אמת **בכל המודלים** של Φ, דהיינו הוא נובע לוגית מ־Φ, אז **קיימת** לו הוכחה. הבעיה היא שלעתים איננו מתעניינים בתור Φ אלא מנסים להבין את התכונות של מודל ספציפי דוגמת $\mathbb{N}$, אך זה לא תמיד המצב (כך למשל בתורת החבורות אנחנו כן מתעניינים במשפטים שהם אמת בכל המודלים; כמו כן בבירור תורת החבורות אינה שלמה כי $\forall x \forall y(x \cdot y \approx y \cdot x)$ אינו ניתן להוכחה או להפרכה ממנה, והדבר אינו מפריע לנו).

- "משפטי גדל הרסו את המתמטיקה" - לא כדאי להגזים. לכל היותר נהרסה תוכנית הילברט, בהיקף השאפתני המקורי שלה. מתמטיקאים באופן כללי מודעים לכך שמערכת האקסיומות שלהם לא בהכרח מסוגלת להוכיח כל דבר, אבל המחוייבות של רוב המתמטיקאים למערכת אקסיומות ספציפית היא רופפת למדי - מעטים המתמטיקאים שעובדים ישירות עם מערכת אקסיומות ספציפית ומונעים מעצמם בכוח לחרוג ממנה. כמובן, אם תמצא הוכחה לבעיה קשה ייתכן שיתברר לאחר מכן שחלק מההוכחה מתבסס על אקסיומות "חדשות" ושהטענה המקורית כלל אינה ניתנת להוכחה מ־ZFC (או מערכת אקסיומות סטנדרטית אחרת). יש להעיר כי זה בערך המצב עבור טענות מתמטיות שמשתמשות באקסיומת הבחירה להוכחתן - הן עשויות להיות בלתי תלויות ב־ZF לבדה, אבל זה לא מנע מהמתמטיקאים להוכיח אותן בתוך מערכת אקסיומות רחבה יותר.

- "משפט גדל מוכיח שקיים אלוהים/משפט גדל מוכיח שאלוהים לא קיים" - באופן כללי, כל נסיון להשתמש במשפט כדי לטעון טענה על משהו שאיננו תורה (אריתמטית, אפקטיבית, עקבית) מתמטית הוא שקר גס או חוסר הבנה מוחלט של המשפט. למשפט גדל, כמו לכל משפט מתמטי אחר, יש תנאי מאוד דקדקניים. הוא אינו תקף אפילו עבור מחלקה גדולה מאוד של תורות מתמטיות; קל וחומר שאינו תקף עבור דברים שאינם מתמטיים.

- "משפטי אי השלמות של גודל" - בגרמנית שמו של גדל הוא Gödel, כאשר ה־ö לא נהגה כ"ו".

6.11 אחרית דבר - לידתה של תורת החישוביות

גם אחרי משפטי גדל נותרה עדיין פתוחה שאלת ה־Entscheidungsproblem - "בעיית ההכרעה" של הילברט. גדל הראה שלא יהיה ניתן לתת את הפתרון הטריוויאלי לבעיה, אך הדבר לא שלל את האפשרות שיהיה לה פתרון אחר. עם זאת, הסבירות לכך שהבעיה ניתנת לפתרון בכלל הייתה נמוכה, וכאן צץ קושי אחר - איך אפשר להראות ש**לא** קיים אלגוריתם שעושה את מה שהילברט רצה, אם אין אפילו הגדרה פורמלית ל"אלגוריתם"?

לאחר משפטי גדל החלו מספר נסיונות לתת משמעות פורמלית למושג של פונקציה **ניתנת לחישוב**. הרעיון הבסיסי נמצא במאמר של גדל עצמו - הפונקציות הרקורסיביות שלו נראות כמו כיוון מבטיח, אך פונקציה שנקראת **פונקצית אקרמן**, על שם סטודנט נוסף של הילברט, מראה שזה לא כך - זוהי פונקציה שהיא בבירור ניתנת לחישוב אך גדלה "מהר מדי" מכדי שתוכל להיות רקורסיבית.

פתרון אחד לבעיה היה הרחבה של אוסף הפונקציות הרקורסיביות של גדל על ידי הוספת כלל בניה נוסף, שלא נציג כאן. גישה אחרת למושג הפונקציות הניתנות לחישוב הייתה תחשיב הלמדא של אלונזו צ'רץ'. עם זאת, הגישה הטובה ביותר וזו שהשתרשה בסופו של דבר בעולם המתמטי הייתה שלו של המתמטיקאי הבריטי אלן טיורינג, שבחר בגישה שונה למושג החישוב. בעוד שגדל ושאר החוקרים הגדירו **מחלקות של פונקציות** שנבנו באמצעות כללי בניה מסויימים, טיורינג הגדיר **מכונה** דמיונית שמבצעת חישובים באופן כמעט מכני, ובחר להגדיר את הפונקציות הניתנות לחישוב בתור הפונקציות שאותן המכונה שלו מסוגלת לחשב. המכונה נקראה ברבות הימים על שמו, **מכונת טיורינג**, והתברר כי הפונקציות שהיא מסוגלת לחשב הן **בדיוק** הפונקציות הרקורסיביות של גדל (עם ההרחבה ההכרחית שלהן) ו**בדיוק** הפונקציות שניתנות לחישוב בתחשיב הלמדא של צ'רץ'. במילים אחרות, הוצעו (באופן בלתי תלוי!) מספר מודלים שונים מאוד באופיים שניסו לתפוס את מושג הפונקציות הניתנות לחישוב, וכולם התבררו כשקולים. זה מחזק את ההשערה (שאין דרך של ממש להוכיח מכיוון שאין ולא תהיה הגדרה מדויקת למושג "אלגוריתם") שמכונות טיורינג מסוגלות לחשב **כל דבר שניתן לחישוב**. השערה זו מכונה "התזה של צ'רץ' וטיורינג".

טיורינג וצ'רץ' הוכיחו באופן בלתי תלוי, כל אחד עבור המודל שלו, כי קיימות פונקציות שאינן ניתנות לחישוב, ובפרט שה־Entscheidungsproblem אינה ניתנת לפתרון. אצל טיורינג הדבר בוצע על ידי ההוכחה שלא ניתן להכריע, בהינתן קידוד של מכונה וקלט מסויים עבורה, האם היא עוצרת על הקלט הזה או לא (בעיה זו מכונה "בעיית העצירה"). אופי ההוכחה של טיורינג מזכיר את ההוכחה של גדל (טיורינג מציין אותו במפורש בתור מקור השראה) אך היא פשוטה משמעותית יותר מאשר הוכחתו של גדל.

המודל של טיורינג והוכחת אי הכריעות של בעיית העצירה היו הצעד הראשון בפיתוח תורה מתמטית שעוסקת בחישובים - **תורת החישוביות**, שברבות השנים (בד בבד להמצאת המחשב ופיתוח תורת האלגוריתמים) התרחבה והפכה ל**תורת הסיבוכיות**, שהיא ענף המחקר המרכזי בתיאוריה של מדעי המחשב גם בימינו.