הקדמה

החוברת "לוגיקה - קורס שני" מקבילה במידה רבה, לקורס "לוגיקה 2", ומבוססת על הרצאותיו של פרופ' ש' שלח בקורס זה. החוברת נחלקת לשלושה חלקים, אשר במרכזם משפט האי-שלמות של גדל (*Gödel*).

אופן הצגת הדברים מושפע במידה רבה מתחושתנו, כי העבודה עם מכונות חישוב נוחה ואינטואיטיבית יותר מאשר העבודה עם פונקציות חשיבות (רקורסיביות). לפיכך עוסק חלקה הראשון של החוברת במחלקות של פונקציות הניתנות לחישוב על ידי מכונות ובקשר שלה למחלקת הפונקציות החשיבות. בחלק זה של החוברת מתבצעת העבודה הטכנית הנדרשת להצדקת המעברים בין מחלקות אלה. בנוסף, נדמה לנו, כי הכלים הטכנים, שמפותחים בשלב זה מספקים תשתית מוצקה להצדקת התזה של צ'רץ' (*Church*), והחיזוק הנובע ממנה למשפט גדל.

חלקה השני של החוברת מתמקד בהוכחתם של משפט גדל ושל מספר מסקנות חשובות העולות ממנו.

בחלקה השלישי של החוברת אנו מנסים להציג את הדוגמאות הפשוטות ביותר, המצביעות על כך, שעל אף התוצאה השלילית של משפט גדל ניתן להבין במלואן תורות מתמטיות, שעל פניהן אינן פשוטות כלל ועיקר. השלמות בסיסיות בתורת המודלים מקדימות חלק זה של החוברת.

חשוב לציין כי רבים מן הכלים ומן המושגים המתמטים, שפותחו להוכחת משפט גדל שימשו נקודות מוצא להתפתחותם של תחומי מחקר מתמטים חדשים דוגמת חישוביות (או תורת הרקורסיה), סיבוכיות ועוד, אשר אינם נדונים, ואף אינם נזכרים בחוברת זו.

חומר הרקע הנדרש לקריאת שני החלקים הראשונים של החוברת בסיסי ביותר, ואמור להכלל בכל קורס ראשון בלוגיקה מתמטית. המושגים הבסיסים, בלעדיהם לא ניתן יהיה לעקוב אחר החוברת, הם: שפה, מבנה לשפה, תורה בשפה, מודל לתורה, ספיקות ($\models$), מערכת היסק, ויכיחות ($\vdash$). סקירה קצרה של מושגים אלו מופיעה בהקדמה לחלקה השלישי של החוברת (פרק 3.0) .

חלקה האחרון של החוברת אמור גם הוא להיות כמעט בלתי תלוי בידע מוקדם של הקורא (לבד מן הנזכר לעיל), אולם אפשר שהוא אינטואיטיבי פחות וקריאתו מצריכה מעט יותר מאמץ.

1 מכונות ופונקציות חשיבות

1.0 מבוא

בראשית המאה ה- 20 הציב המתמטיקאי הגרמני ד. הילברט (*Hilbert*) שאלה שהפכה לאחד הזרזים החשובים להוכחת משפט גדל. הילברט ביקש לדעת האם קיימת שיטה מכנית שתוכל לקבוע לכל פסוק מתמטי האם הוא נכון או שאינו נכון.

השאלה שהציב הילברט אינה לגמרי מדויקת מבחינה מתמטית שכן היא עושה שימוש במושגים מעורפלים דוגמת "שיטה מכנית" או "פסוק נכון". חלק נכר מן התשובה לשאלתו של הילברט טמון במציאת המושגים המתמטים המדויקים, שיחליפו את המינוח העמום הנ"ל. בחלק זה של החוברת ננסה להבהיר את המושג "שיטה מכנית".

כאמור, אנו מחפשים שיטה מכנית (או בשפה אחרת – מכונה מתמטית), אשר בהנתן פסוק בשפה L סופית תקבע בתוך זמן סופי האם הפסוק נכון או לא. דרישות טבעיות משיטה זו הן שתהיה קובענית (דטרמיניסטית) וחד ערכית. מכאן ששיטה כזו, אם אכן תמצא, תהווה פונקציה מקבוצת הפסוקים בשפה L למספרים הטבעים (או אפילו לקבוצה $\{0,1\}$), ומכיוון שלכל פסוק בשפה סופית ניתן להתאים באופן חח"ע מספר טבעי (למשל, באמצעות קוד *ASCII*) ניתן לחשוב על השיטה שאנו מחפשים כעל פונקציה (חלקית) מהמספרים הטבעיים לעצמם.

בכדי להראות, שהתשובה לשאלתו של הילברט שלילית יספיק להראות שבהנתן שיטה מכנית כלשהי נוכל למצוא פסוק, שעבורו אין ביכולתה של שיטה זו לקבוע האם הוא נכון או לא (כלומר, לכל שיטה מכנית, אשר בהנתן פסוק כלשהו אמורה לקבוע אם הוא נכון או לא, נוכל למצוא פסוק עליו לא תוכל השיטה לומר דבר). כיוון שמן הדיון עד כאן עלה, כי כל שיטה מכנית כזו ניתנת לתאור ע"י פונקציה מן הטבעים לעצמם, הרי אנו מחפשים בעצם תכונה משותפת למשפחת הפונקציות $\mathbf{C}$ המוגדרת ע"י: $f \in \mathbf{C}$ אסם f פונקציה מהטבעיים לטבעיים כך שיש מכונה מתמטית (=מכונת חישוב) המחשבת אותה (לכל טבעי). התכונה המבוקשת אמורה להבטיח לנו קיום של פסוק כנ"ל. אם כן, מצאנו שניתן להעביר את תחום הדיון למשפחה $\mathbf{C}$, אלא שזו עדיין איננה מוגדרת היטב. משום כך, עתה ננסה להבין טוב יותר מתי $f \in \mathbf{C}$ או בלשון אחר מתי פונקציה הינה חשיבה, כלומר ניתנת לחישוב.

בטרם נמשיך בדיון נעיר שתי הערות טכניות לכאורה ביחס למשפחה $\mathbf{C}$: ראשית, אין אנו דורשים, כי הפונקציות המשתייכות למשפחה תהיינה שלמות (כלומר, תיתכנה פונקציות ב-$\mathbf{C}$ שתחומן אינו כל N). שנית, במהלך הדיון נרשה לעצמנו להתייחס גם לפונקציות $f : N^k \to N^m$ כפונקציות במחלקה $\mathbf{C}$. בהמשך נפתח את הכלים הטכנים שיצדיקו זאת.

בבואנו ללמוד את המחלקה $\mathbf{C}$, נשים לב, כי ביסודו של דבר, אם $f \in \mathbf{C}$ יש מכונה המחשבת את f ודי בהצגתה כדי לשכנע שהפונקציה אכן ניתנת לחישוב. לדוגמה, הפונקציה הקבועה $x=0$ בוודאי ניתנת לחישוב, שכן קל להשתכנע בקיומה של מכונה המחזירה על כל קלט תשובה קבועה 0. פונקצית החיבור אף היא מתקבלת על הדעת כפונקציה ניתנת לחישוב - כדי לראות זאת נחשוב על מכונה המקבלת כקלט זוג מספרים טבעיים בהצגה אונרית (כלומר, המספר הטבעי n מיוצג על ידי סדרה באורך n של אחדות) ואשר מחזירה כפלט סדרת אחדות שאורכה כמספר האחדות שקיבלה כקלט. אלא שבהנתן פונקציה כללית $f : N \to N$ (הנתונה, למשל, ע"י סדרת טבעיים אינסופית) אין זה ברור כלל ועיקר כיצד ניתן להראות אפילו שמכונה נתונה כלשהי אכן מחשבת את f, קל וחומר לשכנע שאין בנמצא מכונה המחשבת אותה. גרוע מזה, בחינה מדוקדקת יותר של הטענה לפיה פונקצית החיבור ניתנת לחישוב תדגים לנו תכונה מהותית: פונקצית החיבור הנה פונקציה שלמה על N^2, ולפיכך כל מכונה שאמורה לחשב את פונקצית החיבור צריכה לאפשר חיבור כל זוג מספרים, גדול ככל שיהא, ומכיוון שכך נזקקת לזכרון שאין לו הגבלה סופית - אפילו רק בכדי שתוכל לקבל את הקלט במלואו. מכאן שגם לפונקציות הפשוטות ביותר, אשר בוודאי הינו רוצים לכלול במשפחה $\mathbf{C}$, יתכן שאי אפשר יהיה לבצע את החשוב בפועל (בגלל הגבלות פיזיקליות), כלומר לא נוכל לדרוש שיש מכונה שאכן תוכל לחשבן. קיבלנו, אם כן, שבהנתן פונקציה f כנ"ל, עלינו לדייק בניסוח השאלה "האם קיימת מכונה M המחשבת אותה" ולאמר אולי: "האם קיימת מכונה מתמטית, עיונית (=תיאורטית), המחשבת את f".

נדמה שעל שאלות ממין זה אין המתמטיקאי יכול לקוות לתשובה שתניח את דעתו ללא הגדרה מדויקת של המושג "מכונה עיונית", ומכיוון שבכל הגדרה מתמטית יש מרכיב שרירותי לא נותר אלא להציע הגדרה אשר תקרב ככל האפשר את תפיסתנו האינטואיטיבית (יהא מושג זה אשר יהא) באשר לאופיין של "מכונות חישוב". נעיר, עם זאת שאפשר שתהיינה הגדרות שונות שמתאימות למושג העמום שיש לנו, ואכן בשנות השלושים של המאה ה- 20 הוצעו מספר הגדרות שונות.

בטרם נציע הגדרה פורמלית למושג "פונקציה הניתנת לחישוב ע"י מכונה" נבהיר מספר נקודות הנוגעות למכונות התיאורטיות שהזכרנו לעיל. ראשית, נעיר שהכורח להניח, כי למכונות החישוב זכרון בלתי מוגבל, נבע מרצוננו שלא להגביל מראש את גודל הקלט/הפלט של המכונה או את שטח הזכרון הנדרש לביצוע תהליך החישוב. לפיכך יהיה זה סביר לדרוש שתמיד תעשה המכונה שימוש רק בחלק סופי (אבל לא חסום) של הזכרון (למשל, נוכל להניח שלמכונה מספר סופי של תאי זכרון שבכל אחד מהם ניתן לאחסון מספר טבעי יחיד אך גדול כרצוננו). הגבלה נוספת, הנראית הכרחית, היא שהמכונה תהיה ניתנת לתאור סופי (או בתאור המכני, שהמכונה תהיה מורכבת ממספר סופי של "אטומים" - בנסוח זה נחשוב על הזכרון כולו כעל "אטום" אחד). ללא דרישה זו קשה לראות כיצד נוכל להוציא מן הכלל ל- $f \in {}^N N$ כלשהי את המכונה שתתואר ע"י $\aleph_0$ אטומים באשר האטום ה-n ייתן על הקלט n את הפלט $f(n)$ ועל כל קלט אחר לא יעשה דבר (ובכך נזהה את $\mathbf{C}$ עם ${}^N N$ - תוצאה לא רצויה לכל הדעות). בכדי להשלים את התמונה של

מכונת חישוב עלינו להכניס למערכת את ממד הזמן. נעשה זאת ע״י שנדרוש שלמכונה יהיה מספר סופי של ״פונקציות בסיסיות״ (אשר כל אחת מהן נתונה ע״י ״אטום״), שאינן יכולות להתבצע אלא באופן סדרתי.

התאור הנ״ל של מכונה מותיר את המושגים ״אטום״ ו״פונקציה בסיסית״ של מכונה מעורפלים למדי. נדמה שקשה יהיה לשפוך אור נוסף על מושגים אלה, לבד מן הדרישה שיהיו פשוטים ככל האפשר (למשל, במובן זה שלא ניתן לחלקם למספר רכיבים או פעולות פשוטים יותר).

מן האמור עד כה עולה, שלא ניתן לספק תשובה מתמטית מלאה לשאלתו של הילברט, כפי שזו הוצגה לעיל, כי התשובה תלויה בפרוש המושגים. על מנת לאפשר טיפול מתמטי בשאלה נצטרך לבחור הגדרה למחלקה $\mathbf{C}$, אשר תענה על הדרישות, שתוארו לעיל, ולהוכיח את כל טענותינו ביחס למחלקה זו. מצד שני, כל ההגדרות שהוצעו כממוש של המושג ״פונקציה חשיבה״ הוכחו כשקולות, וזו ראיה כבדת משקל לטבעיות ההגדרה. ליתר דיוק, כאשר אנו מתיחסים לחשוב סופי, אך לא מוגבל, ואיננו מתירים חופש בחירה (למשל אין הטלת מטבעות) אין שום הצעה אחרת. נקודה חשובה נוספת היא שלמרות שהעניין מראש היה בפונקציות שלמות, כלומר שלכל טבעי הן נותנות ערך, אין לנו ברירה אלא לטפל במשפחת הפונקציות החלקיות, כי פונקציה חשיבה נתונה על ידי אלגוריתם או מכונה מתמטית המחשבת אותה, וההבחנה בין הגדרות מסוג זה הנותנות פונקציות שלמות ואלה שאינן נותנות פונקציות שלמות היא קשה (מהותו של קושי זה תתבהר בהמשך).

אחד המודלים המפורסמים והמקובלים ביותר למכונת חישוב הוצע ע״י אלן טיורינג (*A. Turing*), ונקרא על שמו. מכונת טיורינג (שהגדרתה המדויקת תובא בהמשך) מורכבת מסרט אינסופי (הזכרון) ומראש קורא. הסרט מחולק למספר אינסופי של תאים, אשר בכל אחד מהם כתוב תו אחד מתוך א״ב סופי. הראש הקורא יכול לטפל בתא יחיד בכל רגע נתון - לקרוא את תוכנו, ועל פיו לבצע את הפקודה המתאימה מתוך רשימת הפקודות (הסופית) של המכונה (למשל, לשנות את תוכן התא, לזוז תא אחד ימינה או שמאלה).

קל להשתכנע כי מכונת טיורינג היא דוגמה סבירה למכונת חישוב ״תיאורטית״. אכן דווקא בשל פשטותה לא ברור על פניו מדוע לא ניתן יהיה לבנות מכונות מורכבות יותר, בהן ניתן יהיה לחשב פונקציות שמוכנות טיורינג אינן יכולות לחשב. לפיכך, במבט ראשון נראית התזה שלהלן מפתיעה למדי. התזה של צ׳רץ׳ מניחה כי $f \in \mathbf{C}$ אסם יש מכונת טיורינג המחשבת את f מובן שהתזה של צ׳רץ׳ אינה ניתנת להוכחה מתמטית (שכן, כאמור, למושג $f \in \mathbf{C}$ אין הגדרה מתמטית ברורה), אולם כל הראיות שהצטברו עד כה מצביעות על נכונותה. מעתה נניח את התזה של צ׳רץ׳, ובכל פעם שנאמר ״פונקציה הניתנת לחישוב״ נתכוון בעצם לפונקציה הניתנת לחישוב ע״י מכונת טיורינג. אנו מאמינים, כי במבוא הנ״ל בשלוב הכלים הטכניים שיפותחו בהמשך הפרק יש כדי לתת הצדקה סבירה להנחת השערה זו. לקורא המעונין נמליץ לחזור ולקרוא מבוא זה לאחר סיום קריאת חלקה הראשון של החוברת ולבחון מחדש את התזה של צ׳רץ׳ לאורו.

1.1 מכונות טיורינג ומכונות מונים

מכונת טיורינג

בפרק הקודם תארנו באופן סכמתי את המודל של מכונות טיורינג. נציג עתה הגדרה מדויקת למושג זה:

1.1.1 הגדרה: יהיו S א"ב סופי עם תו מיוחד B ו-Q קבוצה סופית של "מצבים פנימים" עם "מצב התחלתי" q_0.

פקודה זו רבעיה $sqxq'$ באשר $s \in S$, $q',q \in Q$ ו- $x \in \{L,R\} \cup S$ (את מושג הפקודה יש להבין באופן הבא: s הוא הנתון שנקרא מן הסרט; q הוא המצב הפנימי של המכונה בעת קריאת הערך s; בהתאם לערך s ולמצב הפנימי q מבצעת המכונה את הפקודה x - תזוזה ימינה/שמאלה או כתיבה על הסרט - ועוברת למצב פנימי חדש q').

מכונת טיורינג זו רביעייה $M = \langle I, S, q_0, Q \rangle$ באשר I סדרת פקודות לא סותרות, כלומר:

$s_i q_i x_i q'_i \in I \wedge (s_1 = s_2 \wedge q_1 = q_2) \rightarrow (x_1 = x_2 \wedge q'_1 = q'_2)$ - במילים אחרות זו פונקציה חלקית מ- $S \times Q$ אל $\{L,R\} \cup S$.

הסבר: כזכור, אנחנו חושבים על מכונת טיורינג כעל ראש קורא/כותב העובר על פני סרט אינסופי המחולק לתאים. S קובע מהם התווים, שיכול הראש הקורא לצפות לקרוא על הסרט, ומהם התווים, שהוא יכול לכתוב עליו. התו המיוחד B ישמש לציין תא ריק. Q הוא אוסף מצבים פנימים, המאפשר לנו לעקוב אחר שלבי הפעולה של המכונה; I היא קבוצת פקודות, הקובעת מה תעשה המכונה בכל צעד בהתאם למצב הפנימי של המכונה ולקלט שנקרא באותו זמן. הדרישה שהפקודות תהינה עקביות היא טבעית ונועדה להבטיח שהמכונה תוכל לבחור בכל שלב את הפקודה המתאימה לבצוע. יש לשים לב, כי הבקרה על פעולות המכונה נעשית ע"י המצבים הפנים בלבד, וכי ל"סדר" הפקודות ב-I אין כל חשיבות.

1.1.2 הגדרה: **מצב M של מכונה T** זו שלשה (n,q,h), באשר $n \in Z$ מציין את מיקום הראש הקורא על הסרט ביחס למיקום ההתחלתי $(n=0)$, $q \in Q$ הוא המצב הפנימי הנוכחי של המכונה ו-h היא פונקציה $h: Z \rightarrow S$ המתארת את מצב הסרט (כלומר $h(m)$ הוא האיבר ה-m-י בסרט).

הערה: ברור של- $0 \in Z$ אין תפקיד מיוחד, וכי להזזה של Z אין כל משמעות.

1.1.3 הגדרה: למצב M נגדיר $M^{(T)}$ **המצב העוקב ל-M** לפי המכונה T:

אם $M = (n,q,h)$ ויש פקודה $sqxq' \in I$ כך ש- $s = h(n)$ אז: $M^{(T)} = (n^*, q^*, h^*)$ כאשר:

(1) n^* מתאר את המיקום החדש של הראש הקורא, ונתון ע"י: $n^* = \begin{cases} n & x \in S \\ n+1 & x = L \\ n+1 & x = R \end{cases}$.

(2) h^* נתון ע"י:

$$h^* = \begin{cases} h(k) & k \neq n \\ h(k) & x \in \{L,R\} \wedge k = n \\ x & x \in S \wedge k = n \end{cases}$$

את h^* יש להבין באופן הבא:

- המכונה יכולה לשנות רק את התא בו נמצא הראש הקורא.
- אם הפקודה היתה לזוז, היא לא שינתה את הכתוב איפה שהיתה.
- אם הפקודה היתה לכתוב על הסרט דבר חדש היא כותבת זאת .

(3) $q^* = q'$ (המצב הפנימי החדש המתאים לפקודה שהתבצעה).

אם אין פקודה מתאימה ב- I $M^{(T)}$ אינו מוגדר. כיוון שב- I אין פקודות סותרות, ברור כי כאשר $M^{(T)}$ מוגדר הוא יחיד.

1.1.4 הגדרה: תהי T מכונת טיורינג. **מסע של T** זו סדרת מצבים $M_0, M_1, M_2 ... M_n ...$ כך ש- $M_{n+1} = M_n^{(T)}$ והסדרה מסיימת ב- M_n אם $M_n^{(T)}$ לא מוגדר. אם הסדרה $\{M_i\}$ אינסופית, נאמר שהמסע של T אינו מסתיים.

1.1.5 טענה: לכל מכונה T ומצב M_0 יש מסע אחד ויחיד של T המתחיל ב- M_0 (תרגיל).

1.1.6 הגדרה: לכל מכונה T ומספר n, נגדיר פונקציה חלקית f_T^n n- מקומית מהטבעיים לטבעיים באופן הבא:

לכל $x_1 ... x_n$ טבעיים נגדיר מצב $M_T^n(x_1 ... x_n)$ אשר בו המכונה עומדת על (התא) 0; מצבה הפנימי q_0; והחל משם וימינה יהיה כתוב: $1^{x_1+1} B 1^{x_2+1} B ... B 1^{x_n+1}$ באופן ציורי:

$$...B\ B\ B\ \overbrace{1\,1...1}^{x_1+1}\ B\ \overbrace{1\,1...1\,1}^{x_2+1}\ B\ 1\,1...1\ \ B\ \overbrace{1\,1...1}^{x_n+1}\ \ B\ \ B...$$

אם המסע של T המתחיל ב- $M_T^n(x_1 ... x_n)$ מסתיים במצב M^*, אזי $f_T^n(x_1 ... x_n)$ יהיה מספר ה- 1 – ים המופיעים על הסרט במצב זה. (זה תמיד מספר סופי כיוון שהמסע סופי והמכונה עברה רק על מספר סופי של תאים). אם המסע אינו מסתיים ערך הפונקציה אינו מוגדר.

1.1.7 הגדרה: **פונקציה f ניתנת לחישוב ע"י מכונת טיורינג** אם יש מכונה T כך ש- $f = f_T^n$ (ז"א ש- f מוגדרת אם"ם f_T^n מוגדרת ולכל $\bar{x}$ בתחום מתקיים $f(\bar{x}) = f_T^n(\bar{x})$).

דוגמאות:

(1) מכונת החיבור של $x + y$

(1) $1\ \ q_0\ \ B\ \ q_1$ הרעיון הוא שעל מנת לחבר x ו-y עלינו למחוק שתי

(2) $B\ \ q_1\ \ R\ \ q_1$ אחדות מעל הסרט ואז יישארו לנו $x + y$ אחדות

(3) $1\ \ q_1\ \ B\ \ q_2$

הסבר התוכנית:

המכונה נמצאת במצב q_0 ועומדת על תא שבו כתוב 1, היא מוחקת אותו, כותבת במקומו B ועוברת למצב פנימי q_1 (פקודה (1)).

אם המכונה במצב פנימי q_1 ורואה B, היא עוברת ימינה ונשארת במצב פנימי q_1.

אם המכונה במצב פנימי q_1 ורואה 1 היא כותבת B במקומו ועוברת למצב פנימי q_2 (אם היתה רואה B אז היתה חוזרת על הפקודה (2)).

(2) מכונת חישוב $\left[\frac{x}{2}\right]$.

$1\ q_0\ B\ q_0$	(1)	רעיון:
$B\ q_0\ R\ q_1$	(2)	מוחקים את ה- 1 המיותר ואח"כ מוחקים את
$1\ q_1\ B\ q_2$	(3)	האחדות לסרוגין (כלומר מוחקים אחד
$B\ q_2\ R\ q_3$	(4)	ומותירים אחד – חלוקה ב- 2)
$1\ q_3\ R\ q_1$	(5)	

הסבר התוכנית:

פקודה (1): המכונה נמצאת במצב פנימי q_0 ורואה 1 $(1q_0)$ מוחקת אותו, כותבת B במקומו ונשאר במצב פנימי q_0 (Bq_0).

פקודה (2): המכונה נמצאת במצב פנימי q_0 רואה B (Bq_0) הולכת ימינה ועוברת למצב פנימי q_1.

פקודה (3): אם המכונה רואה 1 כשהיא במצב q_1 $(1q_1)$ מוחקת אותו, כותבת B במקומו ועוברת למצב q_2 (Bq_2).

פקודה (4): המכונה נמצאת במצב פנימי q_2 רואה B (Bq_2), הולכת ימינה וניצבת במצב פנימי q_3 (Bq_3).

פקודה (5): המכונה נמצאת במצב פנימי q_3 ורואה 1 $(1q_3)$, הולכת ימינה ומקבלת מצב q_1. (אם במצב q_3 המכונה רואה B סימן שזהו B שני ברציפות ולכן נגמר הקלט והחישוב הסתיים).

<u>1.1.8 טענה</u>: לכל מכונה T יש מכונה T^* כך ש:

i. לכל n: $f_T^n = f_{T^*}^n$.

ii. לכל מסע מסתיים של T^* האותיות S (F) מופיעות בתחילת (בסוף) השטח בו בוצע החישוב, כלומר הסרט נראה כך:

$$\underline{\ldots BBB\overbrace{S \qquad\qquad F}^{\text{המכונה לא יצאה מהתחום הזה}}BBB\ldots}$$

iii. S,F אינן מופיעות באמצע (מניחים כי $S,F \notin S$ אחרת נשנה שמות (אבל $S,F \in S^*$ כאשר S^* האלף בית של המכונה T^*).

<u>הוכחה</u>:

"נבנה" את T^* ע"י כך שנתאר את הפקודות שלה.

<u>שלב 1</u>: הרעיון הוא שאנו רוצים לכתוב S,F בסוף הקלט ובתחילתו בהתאמה. בהתחלה הראש הקורא עומד על ה- 1 הראשון – נזוז שמאלה, נכתוב S ונתחיל לחפש את סוף הקלט ע"י זה שנחפש שני B –ים רצופים. כשנגיע לסוף הקלט נכתוב שם F ונחזור להתחלה.

(1)	$1\ q_0\ L\ q_1$	המכונה עומדת על ה- 1 הראשון וזזה שמאלה.
(2)	$B\ q_1\ S\ q_2$	המכונה כותבת S משמאל ל- 1 הראשון.
(3)	$S\ q_2\ R\ q_2$	המכונה מתחילה את החיפוש של סוף הקלט.
(4)	$1\ q_2\ R\ q_2$	כל עוד המכונה רואה 1 היא ממשיכה לנוע.
(5)	$B\ q_2\ R\ q_3$	המכונה מוצאת B ראשון.
(6)	$1\ q_3\ R\ q_2$	אם אחרי ה- B הקודם יש 1, ממשיכים בחיפוש.
(7)	$B\ q_3\ F\ q_4$	אם אחרי ה- B הקודם יש B – החיפוש הסתיים.
(8)	$F\ q_4\ L\ q_4$	
(9)	$B\ q_4\ L\ q_4$	
(10)	$1\ q_4\ L\ q_4$	
(11)	$S\ q_4\ R\ q_0^*$	

הפקודות (8,11) מחזירות את המכונה שמאלה עד ל- 1 הראשון ואז המכונה עוברת למצב פנימי q_0^* (המתאים למצב הפנימי q_0 של T).

כל מה שעשינו עד עכשיו הוא שרשמנו S בהתחלת הקלט ו- F בסופו, כך שהסרט נראה:

$S1^{x_1+1}B1^{x_2+1}B...B1^{x_n+1}BF$ הראש הקורא נמצא מימין ל- S.

<u>שלב 2</u>: לכל פקודה $y\ q_\ell xq_m \in I$ של T נתאים פקודה $y\ q_\ell^* xq_m \in I^*$ ב- T^*.

<u>שלב 3</u>: נותר להגדיר ל- T^* מה לעשות כאשר היא נתקלת ב- F או ב- S. הרעיון הוא שאם נתקלים ב-S (בכל מצב פנימי שהוא) מזיזים אותו משבצת אחת שמאלה ואם נתקלים ב-F משבצת אחת ימינה.

לפיכך לכל $0 \le \ell \le |Q|$ נתאים את סדרת הפקודות:

המכונה במצב q_ℓ^* נתקלה ב-S .	(1)	$S\ q_\ell^*\ B\ q_\ell^1$
המכונה כותבת במקומו B וזזה שמאלה.	(2)	$B\ q_\ell^1\ L\ q_\ell^2$
המכונה כותבת S במקום זה שנמחק.	(3)	$B\ q_\ell^2\ S\ q_\ell^3$
המכונה זזה ימינה.	(4)	$q_\ell^3\ S\ R\ q_\ell^*$

עתה המכונה תוכל להמשיך בריצה בהתאם לפקודות שהוספנו בשלב 2.

באופן דומה מטפלים במקרה ש- T^* רואה F .

בשלב זה נותיר לקורא להוכיח שהמכונה T^*, שתוארה לעיל אכן מקיימת $f^n_{T^*} = f^n_T$

וכי בכל שלב של ריצתה S, F מסמנים את התחום בסרט שממנו לא חרגה המכונה

עד לאותו שלב. ■

מעתה נניח שכל מכונת טיורינג מתנהגת כמו המכונה המובטחת בטענה 1.1.8.

<u>1.1.9 משפט:</u>

(1) לכל מכונת טיורינג T קיימת מכונת טיורינג T' כך שלכל $f^n_{T'} = f^n_T$ ול-T' התכונה הבאה:

בסוף כל מסע מצב הסרט הוא `$...BBB\overbrace{S\ 1\ 1\ 1...\qquad ...1\ 1\ 1\ F}^{p^+}BBB...$ (כלומר, רצף של אחדות, שאינו מופרע ע"י B –ים) כאשר S תופס את מקומו של ה-1 הראשון בקלט ובמשך המסע המכונה לא היתה אף פעם משמאל ל-S זה.

(2) לכל מכונת טיורינג T קיימת מכונת טיורינג T' כך שלכל n $f^n_{T'} = f^n_T$ ול-T' תכונות הבאות:

i. הא"ב של T' הוא $\{B,1\}$.

ii. T' לא זזה אף פעם שמאלה מן ה-1 הראשון של הקלט ומצבה הסופי הוא $....BB1\ 1\ 1...\ ...\ 1\ 1\ 1BB...$

<u>הוכחה</u>:

נוכיח ראשית את חלקו הראשון של המשפט.

שלב ראשון: נניח בה"כ כי S,F אינם בא"ב של T. עתה נבנה מכונה $T1$, המזיזה את כל הקלט של T במשבצת אחת ימינה, וכותבת S מימין לאחד הראשון ו-F בסוף הקלט.

נסמן ב- q_i מצבים פנימיים של T וב- q^i מצבים פנימיים חדשים, שאנו מוסיפים ל-$T1$. נתאר עתה את המכונה $T1$:

המכונה $T1$ מתחילה במצב q_0	(1) $1\ q_0\ S\ q_1$
המכונה כתבה S ועתה זזה ימינה	(2) $S\ q_1\ R\ q_1$
המכונה מעתיקה את הקלט	(3) $1\ q_1\ R\ q_1$
במצב q_1 יש צורך לפצות על ה-1 שמחקנו	(4) $B\ q_1\ 1\ q_2$
המכונה ממשיכה במסע ימינה	(5) $1\ q_2\ R\ q_3$
אם המכונה מצאה B במצב q_3 - הגענו לסוף הקלט	(6) $B\ q_3\ F\ q_4$
במצב q_3 צריך לפצות על ה-B שמחקנו	(7) $1\ q_3\ B\ q_2$
שוב מצב q_2 משמש לתזוזה כאשר "חייבים" 1 שמחקנו	(8) $B\ q_2\ R\ q_1$

פקודות אלו מטפלות בהזזת הקלט ימינה ובכתיבת S,F בקצוות. עתה נחזיר את הראש הקורא להתחלה:

$F \;\; q^4 \;\; L \; q^4 \quad (9)$

$1 \;\; q^4 \;\; L \;\; q^4 \quad (10)$

$B \;\; q^4 \;\; L \;\; q^4 \quad (11)$

$S \;\; q^4 \;\; R \;\; q_0 \quad (12)$

כשאנו מגיעים ל-S אנו זזים בחזרה ל-1 הראשון ועוברים למצב q_0, שהוא כזכור, המצב ההתחלתי של המכונה T.

שלב שני: לאחר השלמת השלב הראשון (שתמיד מסתיים) נרצה שהמכונה $T1$ תמשיך בריצה כאילו הייתה T, אלא שלשם כך נצטרך להוסיף פקודות שיאמרו ל-T מה לעשות כאשר היא קוראת S או F.

הטיפול ב-F זהה לחלוטין לזה שבטענה 1.1.8. הטיפול ב-S יהיה מעט שונה, שכן עלינו להבטיח שהמכונה לא תזוז משמאל ל-S.

נניח, אם כן כי q_j הם המצבים הפנימיים של T. לכל j נוסיף סדרה של מצבים פנימיים q_j^i כך שכשהמכונה תגיע ל-S במצב פנימי q_j היא תעבור למצב פנימי q_j^0, אשר מתחיל סדרת פקודות אשר מעתיקה את כל הסרט משבצת אחת ימינה, חוזרת ל-S, כותבת במשבצת מימינו B, וחוזרת למצב פנימי q_j.

את כתיבת המכונה, שתבצע זאת, נותיר כתרגיל (השתמשו ברעיונות המופיעים בשלב הראשון).

שלב שלישי: עתה נניח כי נתונה לנו המכונה $T1$, שהוגדרה בשלבים הקודמים. עתה נוסיף למכונה פקודות כך שאם המכונה T עוצרת המכונה החדשה תצמצם את ה-B-ים ותחזור לעמוד מימין ל-S. (תרגיל).

נפנה עתה להוכחת חלקו השני של המשפט. נוכל להניח בה"כ שהמכונה T הנתונה היא כמובטח ב-(1). יהי $S_1,\ldots S_n$ האי"ב של T. נסמן $s_i = 1^i B^{n-i}$ (כלומר, אנו מקודדים כל אות מן האי"ב של T ע"י "בלוק" של n תווים - כזכור, n הוא גודל האי"ב של T). מטרתנו היא שהמכונה T' תזהה את s_i ותפעל עליהם כמו ש-T פועלת על S_i. נתאר את המכונה T', אך לא נכלול את רשימת הפקודות המלאה.

כבחלקה הראשון של ההוכחה נסמן ב-q_j את המצבים הפנימיים של המכונה T הנתונה וב-q^i מצבים פנימיים חדשים, שהוספנו ל-T'.

שלב ראשון: נכין את המכונה $T1$ לריצה שתחקה את ריצת T ע"י שנחליף את הקלט ב"א המתאים בעזרת הצופן שתואר לעיל ונחזיר את הראש הקורא מימין ל-S. כדי לעשות זאת המכונה

תעבור על הקלט ובכל מקום שנראה S_i נחליף אותו ב- s_i (נשתמש באלגוריתם ההזה ימינה שתיארנו בחלק (1) אלא שבמקום הזזה ימינה במשבצת אחת נבצע הזזה של $n-1$ משבצות. כשנגיע לסוף הקלט (לאות F) נחזיר את הראש הקורא שמאלה עד לתחילת הקלט (האות S).

שלב שני: זיהוי האותיות המוצפנות. נשים לב שבכדי לדמות את פעולת T יהיה על המכונה $T1$ "להבין" n-יות של תווים (ולא רק תווים בודדים). כדי לעשות זאת נוסיף לכל $1 \le j \le n$ מצבים פנימיים q_j^i, ה"אומרים" שהמכונה הגיעה לתחילתה של n-יה במצב פנימי q_i וזיהתה n-יה זו כמצפינה את S_j (כלומר המצב הפנימי q_j^i במכונה $T1$ מתאים לזוג $S_j\ q_i$ במכונה T). סדרת הפקודות של $T1$, המחקה קריאת תו בודד ב-T, תראה כך:

המכונה הגיעה לתחילת n-יה במצב פנימי q_i (1) $1\ q_i\ \ R\,q_i^{1,1}$

לאחר ה-1 הראשון קראה המכונה עוד 1 - יש עדיין אינפורמציה ב-n-יה. (2) $1\ q_i^{1,1}\ R\ q_i^{2,2}$

לאחר ה –1 הראשון המכונה קראה B - ה-n-יה מקודדת S_1. (3) $B\ q_i^{1,1}\ R\,q_i^{1,2}$

$\vdots$

המכונה קראה k אחדות לפני שנתקלה ב- B הראשון - ה-n-יה מקודדת S_k. $q_i^{k,n-1}$ אומר שהמכונה כבר קראה $n-1$ תווים מן ה-n-יה הנוכחית, ולכן עוברת למצב הסופי q_i^k. (4) $B\ q_i^{k,n-1}\ R\,q_i^k$

$\vdots$

הטיפול בקידוד של S_n מיוחד, שכן אין בסופו B. (5) $1\ q_i^{n-1,n-1}\ R\,q_i^n$

בשלב זה נקבע (שרירותית) שבתום קריאת n-יה של קלט המכונה $T1$ נשארת על התו האחרון של n-יה זו.

שלב שלישי: בצוע הפקודות. עלינו לתרגם את פקודות T לפקודות, שיתאימו לשפה החדשה.

אם ב-T יש פקודה מהצורה $S_i\ q_j\ R\,q_k$ נוסיף ל-T' את הפקודות הבאות:

(אנו מניחים, שהמכונה השלימה את קריאת ה-n-יה, כמתואר בשלב השני)

(1) $*\ q_i^j\ R\,q_k$

(כזכור הנחנו שבתום קריאת ה-n-יה המכונה נמצאת בקצה הימיני)

התו * בפקודה (1) מציין 1 או B.

אילו הפקודה הייתה $S_i\ q_j\ L\,q_k$ ההבדל היחיד הוא שהיה עלינו להזיז את הראש הקורא $2n-1$ צעדים שמאלה (כדי שיעמוד בקצה הימני של ה-n-יה שמשמאל לזו שנקראה).

אם ב-T יש פקודה מהצורה $S_i\ q_j\ S_j\ q_k$ נוסיף ל-$T1$ את הפקודות שיאמרו לה לזוז $n-1$ צעדים שמאלה (לתחילת ה-n-יה הנוכחית) ולכתוב עליה את ה-n-יה המתאימה ל- S_j.

כל שנותר לעשות עתה הוא לוודא שהמכונה $T1$ אכן מקיימת את הדרישות (נותיר זאת כתרגיל).

■

<u>1.1.10 הגדרה:</u> למכונת טיורינג המובטחת מטענה 1.1.9 (2) נקרא **מכונת טיורינג תקנית** (סטנדרטית) ולפלט של מכונה זו נקרא פלט תקני.

מעתה נניח כי כל מכונת טיורינג בה נעסוק הנה תקנית.

מכונת מונים

עד כה טיפלנו במשפחת הפונקציות הניתנות לחישוב ע"י מכונות טיורינג. נבחן עתה משפחה נוספת של מכונות, ונתחיל בברור הקשר שבין משפחה זו למשפחת הפונקציות שהכרנו בפרק הקודם.

במקום הסרט של מכונת טיורינג, שהוא אינסופי , בכל מכונת מונים יש מספר סופי של מונים (אבל לכל מספר טבעי n יש מכונת מונים בעלת n מונים). מונה הוא תא שבו יכול להיות כתוב מספר טבעי אחד. במהלך החישוב אפשר יהיה להגדיל או להקטין את המספר הטבעי הכתוב במונה ב-1.

1.1.11 הגדרה: **מכונת מונים** היא סדרת פקודות מהצורות הבאות:

$X_7 \leftarrow X_7 + 1$	פירושו הוסף למונה המסומן ע"י X_7 אחד. (במקום X_7 יכול להיות כמובן כל מונה אחר).
$X_7 \leftarrow X_7 \div 1$	במקום המספר הטבעי המופיע במונה X_7 רשום מספר הקטן ממנו ב-1, ואם ב-X_7 רשום 0 אל תעשה דבר.
$If\ X_7 \neq 0\ GOTO\ g$	לכל פקודה של המכונה מתאים מספר טבעי ע"פ מקום הופעתה ברשימת הפקודות. פירוש הפקודה מימין הוא: אם במונה X_7 כתוב 0, בצע את הפקודה העוקבת לפקודה הנוכחית, אחרת בצע את הפקודה שמספרה הסידורי הוא g.
$HALT$	עצור

מוני המכונה הם כל המונים המופיעים באחת מפקודות המכונה. מכונה R תסומן ב-$P_0, P_1, ..., P_{k-1}$ כאשר כל P_i הוא פקודה.

הערה: בחרנו דווקא את הפקודה $X \neq 0$ ולא את הפקודה $X = 0$, כי אם איננו מניחים שיש מונים בהם כתוב אפס, קשה יהיה לתכנת את המכונה.

דוגמאות של מכונות מונים:

(1) מכונה לחישוב $x + y$:

לשם נוחות משתנים יהיו ב- X_1, X_2 והתוצאה ב- X_0, דבר שיסומן ע"י $X_1 + X_2 \to X_0$.

$X_3 = X_3 + 1$	(0)	פקודה זו מבטיחה ש- $x_3 \neq 0$.
$X_0 = X_0 \div 1$	(1)	שלוש הפקודות הראשונות מאפסות את X_0.
$If\ X_0 \neq 0\ GOTO\ 1$	(2)	
$If\ X_1 \neq 0\ GOTO\ 6$	(3)	

(4) $If\ X_2 \neq 0\ GOTO\ 9$

(5) $HALT$ אם גם $x_1 = 0$ - גמרנו.

(6) $X_1 = X_1 \div 1$ על פקודות 6 ו- 7 אנו חוזרים עד אשר התנאי $x_1 \neq 0$ לא

(7) $X_0 = X_0 + 1$ מתקיים.

(8) $If\ X_3 \neq 0\ GOTO\ 3$ כזכור $x_3 \neq 0$ תמיד.

(9) $X_2 = X_2 \div 1$ על הפקודות 8 ו- 9 אנו חוזרים עד אשר התנאי $x_2 \neq 0$ לא

(10) $X_0 = X_0 = X_0 + 1$ מתקיים.

(11) $If\ X_3 \neq 0\ GOTO\ 3$

האלגוריתם הזה עלול להיות בעייתי, כי הוא מוחק (מעלים) מה שהיה במונים X_1, X_2 ולפעמים אנו מעוניינים לשמור על נתונים אלו. לכן נוסיף קטע בו נדאג להעביר את $X_6 \leftarrow X_1$ בלי לשנות את X_1 :

(0) $X_6 = X_6 \div 1$

(1) $If\ X_6 \neq 0\ GOTO\ 0$

(2) $If\ X_1 \neq 0\ GOTO\ 4$

(3) $HALT$ אם מלכתחילה $X_1 = 0$ - גמרנו.

(4) $X_1 = X_1 \div 1$

(5) $X_6 = X_6 + 1$

(6) $X_7 = X_7 + 1$ זה מונה סרק בו נשתמש בהמשך.

(7) $If\ X_1 \neq 0\ GOTO\ 4$

(8) $X_1 = X_1 + 1$ אם הגענו לכאן העתקת הנתונים ל- X_6 הסתיימה ועתה נחזיר

(9) $X_7 = X_7 \div 1$ את הנתונים ל- X_1.

(10) $If\ X_7 \neq 0\ GOTO\ 8$

באותו אופן נעתיק את $X_7 \leftarrow X_2$ ואחר גמר ריצת החלק העיקרי של התוכנהית נחזיר את $X_1 \leftarrow X_6$ ואת $X_2 \leftarrow X_7$.

(2) מכונה לחישוב $x \cdot y$:

(0) $X_3 = X_3 + 1$ כמקודם, 3 הפקודות הראשונות

(1) $X_0 = X_0 \div 1$ מאפסות את X_0.

(2) $If\ X_0 \neq 0\ GOTO\ 1$

(3) $If\ X_2 \neq 0\ GOTO\ 5$ אם $X_2 = 0$ אין יותר מה לעשות.

(4) $HALT$

(5) $X_2 = X_2 \div 1$ הרעיון הוא לחבר את X_1 לעצמו X_2 פעמים.

(6) $X_0 + X_1 \to X_0$ משמעות הסימון הוא שאנו מוסיפים את הערך שכתוב במונה X_1 לזה שב- X_0 מבלי למחוק את הנתונים (כפי שעשינו בדוגמה 1).

(7) $If\ X_3 \neq 0\ GOTO\ 3$

1.1.12 הגדרה: אם R מכונת מונים אז **מצב של המכונה R** הוא זוג סדור $\langle f,n \rangle$ כאשר f פונקציה ממוני המכונה R אל קבוצת המספרים הטבעיים (f מספרת מה כתוב בכל אחד מן המונים), ו- n מסמן שהמכונה עומדת לבצע את הפקודה ה- n -ית. אם מספר הפקודות ב-R הוא k ואם $n > k$ פירושו שהמכונה עצרה או בפקודה $HALT$ או בסוף סדרת הפקודות, או שאמרו לה ללכת לפקודה בעלת מספר סידורי הגדול ממספר הפקודות במכונה.

תהי $f : N^m \to N$. נרצה להגדיר מתי מכונת מונים R מחשבת את f. לשם כך נצטרך מעט הכנות:

1.1.13 הגדרה: תהי $p_0,...,p_k$ המכונה R. יהי $r = \langle f,n \rangle$ מצב של מכונה R. **המצב העוקב של המכונה** מסומן r^R ומוגדר כדלהלן:

$$r^R = \begin{cases} < f^{+[x_i]}, n+1 > & X_i + 1 \to X_i \text{ מהצורה } P_n - \text{ו } k \geq n \\ < f^{-[x_i]}, n+1 > & X_i \div 1 \to X_i \text{ מהצורה } P_n - \text{ו } k \geq n \\ < f, n+1 > & f(X) = 0 - \text{ו } If\ X \neq 0\ GOTO\ l \text{ מהצורה } P_n - \text{ו } k \geq n \\ < f, l > & f(X) \neq 0 - \text{ו } If\ X \neq 0\ GOTO\ l \text{ מהצורה } P_n - \text{ו } k \geq n \\ \text{לא מוגדר} & n > k \\ < f, k+1 > & P_n = HALT \end{cases}$$

כאשר $(f^{+[x_i]})(x_j) = f(x_j)$ לכל מונה x שונה מ- x_i ו- $f^{+[x_i]}(x) = f(x) + 1$ כאשר $x = x_i$ (באופן דומה מוגדרת גם $f^{-[x_i]}$).

1.1.14 הגדרה:

(1) **ריצה (או מסע) של R** זו סדרה של מצבים $r_0, r_1, r_2 ...$ כך שלכל ℓ אם r_ℓ^R מוגדר אז גם $r_{\ell+1}$ מוגדר, ו- $r_l^R = r_{l+1}$.

(2) **החישוב** (או הריצה) של $f_R^n(x_1,...,x_n)$ כאשר n טבעי, $x_1,...,x_n$ טבעיים ו- R מכונת מונים, זו הריצה של R המתחילה במצב $\langle f_{\bar{x}},0\rangle$ כאשר $f_{\bar{x}}(i)=\begin{cases} x_i & 1\le i\le n \\ 0 & \text{אחרת}\end{cases}$.

(3) עתה ההגדרה של **פונקציה הניתנת לחישוב ע"י מכונת מונים** דומה לזו של פונקציה הניתנת לחישוב ע"י מכונת טיורינג, כלומר: לכל מכונה R וטבעי m נגדיר פונקציה f_R^m m-מקומית מ- N ל- N כך ש- $f_R^m(x_1,...,x_m)$ מוגדרת אסם הריצה של R על $(x_1,...,x_m)$ מסתיימת ובמקרה זה הערך של f_R^m יהיה הערך הכתוב במונה x_0 של R. לבסוף $f:N^m\leftarrow N$ ניתנת לחישוב ע"י מכונת מונים, אם יש מכונת מונים R כך ש- $f=f_R^m$.

כעת נוכיח שכל מה שמסוגלת מכונת מונים לחשב אף מכונת טיורינג יכולה לחשב.

<u>1.1.15 משפט</u>: לכל m טבעי ומכונת מונים R יש מכונת טיורינג T כך ש: $f_T^m=f_R^m$.

<u>הוכחה</u>: תהי R מכונת מונים שמוניה הם $X_1,...,X_m$ ויהיו $P_1,...,P_k$ פקודותיה.

נבנה מכונת טיורינג T שתכיל אותם נתונים (כלומר על הסרט יהיו הנתונים שבמונים) שתחקה את פעולת R.

שלב ראשון: לכל מונה X_i מתאימים C_i 1 –ים על הסרט כאשר C_i הערך של X_i, ומפרידים ביניהם ע"י S_i. למשל למונה X_7 נתאים על הסרט את הקטע $S_6\underbrace{11...1}_{(C_7)}S_7$ ונחזור להתחלה. נעשה זאת בעזרת התוכנית הבאה:

(1)	1	q_0	L	q_1
(2)	B	q_1	S_0	q_1
(3)	S_0	q_1	R	q_2
(4)	1	q_2	R	q_2
(5)	B	q_2	S_1	q_2
(6)	S_1	q_2	R	q_3
(7)	1	q_3	R	q_3
(8)	B	q_3	S_2	q_3
(9)	S_2	q_3	R	q_4
(10)	$\begin{cases} 1 & q_{m+1} & R & q_{m+1} \\ B & q_{m+1} & S_m & q^* \end{cases}$			

הסבר: הראש הקורא נמצא על ה- 1 הראשון. הוא הולך שמאלה, מוצא B ומוחק אותו, כותב במקומו S_0 ומקבל מצב פנימי q_1. (שורות 1-2)

המכונה רואה S_0 במצב q_1 זזה ימינה ומקבלת מצב q_2 שפוסח על כל ה- 1 – ים עד שיגיע ל- B, ימחק אותו, ויכתוב במקומו. S_1 (שורות 3-5).

עושים זאת עד שמגיעים למצב פנימי q_{m+1}, לאחר שהמכונה ראתה B, וכתבה במקומו S_m.

אז עוברים למצב פנימי q^* שיחזיר את הראש הקורא להתחלה (S_0) (שורות 6-10). אז תקבל המכונה מצב פנימי P_1^0, שהוא המצב הפנימי הראשוני (ז"א המתאים לפקודה הראשונה של המכונה R).

שלב שני: לכל פקודה P_i נתאים תת תוכנית של T שתאפשר ל-T לבצע את הפעולה האנלוגית. נניח ש-P_i מהצורה $X_i = X_i + 1$ ונניח שהראש הקורא עומד על S_0 (אפשר להניח שכל פקודה מסתיימת בהחזרת הראש קורא לתחילת הסרט), והמצב הפנימי של המכונה הוא q_i.

בסעיף הקודם ראינו שקיימת מכונת טיורינג, נסמנה T_0, שמסיטה את כל הקלט משבצת אחת ימינה. נשתמש, אם כן במכונה זו, ונניח בה"כ, שקבוצת המצבים הפנימים של T_0 זרה לקבוצת המצבים הפניים, בהם עשינו שימוש עד כה. התוכנית תהיה, אם כן:

$S_j\, q_i^0\, R\, q_i^0$ (0) T מחפשת את S_i. לכל $j < i$ תהיה פקודה כמו (0).

$1\ \ q_i^0\, R\, q_i^0$ (1)

$S_i\, q_i^0\, R\, q_*$ (2) המצב q_* "אומר" למכונה "להפעיל" את T_0.

$\vdots$

$S_i\, q_*^K\, R\, q_i^1$ (3) אפשר להניח שזו הפקודה המסיימת את ריצת T_0, כלומר, הראש הקורא על S_i, והמכונה במצב q_i^1. בנוסף, מובטח לנו שמימן ל-S_i כתוב B.

$B\, q_i^1\, S_i\, q_i^2$ (4) מזיזים את S_i ימינה.

$S_i\, q_i^2\, L\, q_i^3$ (5)

$S_i\, q_i^3\, 1\, q$ (6) במקום שהיה S_i כותבים 1, ובכך מגדילים את C_i ב-1.

אם P_j היא פקודה מהצורה $X_i \to X_i \div 1$ התהליך כמעט זהה לבד משני הבדלים: ראשית, לאחר שמצאנו את S_i עלינו לבדוק אם התו שלפניו הוא S_{i-1}. אם כן, $X_i = 0$ ואין לנו מה לעשות - נחזיר את הראש הקורא להתחלה וגמרנו. אם לא, במקום להפעיל את T_0 נפעיל את T_0', המסיטה את כל הקלט במשבצת אחת שמאלה (במקום ימינה).

את הטיפול בפקודות "$IF\ \ x_i \neq 0\ \ GOTO$" ו-$HALT$ נשאיר כתרגיל. ■

תרגילים - מכונות חישוב:

1. כתבו מכונת מונים המחשבת את $2n$. כתבו מכונת מונים המחשבת את $\lceil \log_2(n) \rceil$ (הערך השלם של $\log_2(n)$).

2. כתבו מכונת מונים המקבלת כקלט זוג מספרים (n,d), ומחזירה כפלט את הספרה ה-d מימין בפיתוח העשרוני של n.

3. יהי $f(x)$ פולינום מעל הטבעיים.

   א. מצאו מכונת מונים המחשבת את $f(x)$.

   ב. מצאו מכונת מונים המחשבת את ה-n הקטן ביותר עבורו $n|f(n)$.

   שימו לב: בשני המקרים הפולינום f קבוע ונתון מראש.

   ג. *האם תוכלו למצוא מכונת מונים המקבלת כקלט פולינום חד-מקומי כלשהו f ומספר טבעי x ומחשבת את $f(x)$ (זכרו שלמכונת מונים נתונה מספר קבוע של מונים).

4. הראו שלכל מכונת מונים R n-מקומית (כלומר עם n מוני קלט) קיימת מכונת מונים R' חד-מקומית השקולה לה (כלומר לכל k טבעי ריצת R על k מסתיימת אסם ריצת R' על k מסתיימת ובמקרה זה תוצאות הריצה זהות).

5. הוכיחו שכל פונקציה חשיבה במכונת טיורינג חשיבה גם במכונת מונים.

6. מצאו פונקציה $f : N \to N$ המקיימת:

   א. f ניתנת לחישוב במכונת מונים.

   ב. לכל $n \in N$ הקבוצה $f^{-1}(n) = \{m : f(m) = n\}$ היא אינסופית.

7. הראו שקיימות פונקציות $f \in {}^N N$, שאינן ניתנות לחישוב במכונת טיורינג.

8. הוכיחו שמשפחת הפונקציות הניתנות לחישוב ע"י מכונת מונים (מכונת טיורינג) סגורה תחת הגדרה באינדוקציה, כלומר, אם $f(\bar{x}, y)$ הפונקציה המוגדרת ע"י $f(\bar{x},0) = g(\bar{x});\ f(\bar{x}, y+1) = h(\bar{x}, y, f(\bar{x}, y))$ והפונקציות g,h ניתנות לחישוב ע"י מכונת מונים (טיורינג) אזי גם הפונקציה f ניתנת לחישוב ע"י מכונת מונים (טיורינג).

9.

   א. הרחיבו את ההגדרה של מכונת טיורינג כך שלמכונה מספר כלשהו, n , של סרטים ומספר מתאים של ראשים קוראים. שימו לב, עליכם למצוא הגדרה שתרחיב את המושג של מכונת טיורינג, כלומר המכונה שתקבלו תוכל בפרט לחשב כל פונקציה שניתנת לחישוב ע"י מכונת טיורינג. עוד וודאו שהרחבת ההגדרה אינה מנוונת, כלומר עליכם להבטיח שהמכונה עושה שימוש אמיתי בסרטים ובראשים הקוראים הנוספים.

   ב. הראו שלכל מכונה העונה להגדרה שמצאתם בסעיף א' קיימת מכונת טיורינג סטנדרטית השקולה לה.

ג. האם ניתן להרחיב את ההגדרה באופן סביר (למשל כך שהטענה המקבילה לזו שבשאלה 7 לעיל תמשיך להתקיים) למכונה בעלת מספר אינסופי של סרטים וראשים קוראים.

10. הוכיחו שכל פונקציה הניתנת לחישוב במכונת טיורינג ניתנת לחישוב במכונת מונים.

11. נתונה מכונת מונים R שתחומה לא ריק. מצאו מכונת מונים חסרת קלט (אך התלויה ב-R) אשר הפלט שלה הוא איבר בתחום של R. במילים אחרות, בהנתן מכונת מונים R עליכם לתאר מכונת מונים R', אשר מוצאת איבר כלשהו עבורו R מוגדרת.

12. נתונה פונקציה חשיבה במכונת טיורינג $f : N \to N$.

א. הראו שניתן למצוא f' מלאה שהיא חשיבה ע"י מכונת טיורינג וכך ש- $\mathrm{Im}(f) = \mathrm{Im}(f)$.

ב. הראו שאם $\mathrm{Im}(f)$ אינסופית ניתן למצוא f כבסעיף ב' שהיא חח"ע.

ג. מצאו תנאי מספיק על $\mathrm{Im}(f)$ על מנת להבטיח שניתן יהיה למצוא f' כבסעיף ב' מונוטונית עולה ממש.

1.2 פונקציות חשיבות (רקורסיביות)

כפי שציינו במבוא, הפונקציות הקבועות ופונקצית החיבור, למשל, בוודאי צריכות להיכלל בכל הגדרה סבירה של פונקציות הניתנות לחישוב. בפרק זה נבחן משפחה של פונקציות נוספות אשר, גם הן, צריכות להיכלל בכל הגדרה של פונקציות ניתנות לחישוב. מטבע הדברים, נקרא למשפחה זו משפחת הפונקציות החשיבות.

1.2.1 הגדרה: **משפחת הפונקציות החשיבות** זו הקבוצה המזערית G של פונקציות חלקיות מהטבעיים לטבעיים בעלת התכונות הבאות:

(1) $\{C_<(x,y);\ \Pi_i^n;\ x\cdot y;\ x+y;\ c_0,c_1\}\subseteq G$.

באשר:

i. Π_i^n זו פונקצית ההיטל, כלומר $\Pi_i^n(x_1,...,x_n)=x_i$.

ii. c_0,c_1 הם הקבועים האישיים 0,1 (או לחילופין פונקציות חד מקומיות $c_0(x)=0$, $c_1(x)=1$).

iii. $C_<(x,y)=\begin{cases}1 & x<y\\ 0 & \text{אחרת}\end{cases}$.

(2) G סגורה תחת הרכבות: אם הפונקציות $g_1(\bar{x}),...g_m(\bar{x}),f(x_1,...,x_m)$ שייכות ל- G (כאשר $\bar{x}$ מהצורה $\langle x_1,...,x_n\rangle$) אז $h(x_i...x_m)=f(g_1(\bar{x}),...,g_m(\bar{x}))$ גם היא ב- G.

(3) G סגורה תחת אופרטור מיזער, μ, המוגדר כדלקמן: אם $g(x_0,x_1,...,x_n)$ פונקציה חלקית מ- N^n ל- N אז $h(x_1,...,x_n)=\mu_{x_0}(g(x_0,x_1,...,x_n))$ מוגדרת באופן הבא:

אם קיים a כך ש- $0=g(a,x_1,x_2,...,x_n)$ ולכל $x<a$ $g(x,x_1,...,x_n)$ מוגדר ושונה מ-0 נגדיר $h(x_1,...,x_n)=a$ אחרת $h(x_1,...,x_n)$ אינה מוגדרת.

דוגמה: נגדיר $f(x)=x-1$ באופן הבא:

$$f(x)=\begin{cases}x-1 & x\geq 1\\ 0 & \text{אחרת}\end{cases}.$$

f חשיבה, כי $f(x)=\mu_y(C_<(y+1,x))$ שהרי $C_<(y+1,x)=0 \Leftrightarrow y+1\geq x$.

תזכורת: נאמר שמכונה T (מונים או טיורינג) מחשבת את $f(x_1,..,x_n)$ כאשר f פונקציה חלקית, אם T עוצרת על הקלט $(x_1...x_n)$ אסם $f(x_1,..,x_n)$ מוגדר, ואזי תוצאת הריצה של T היא $f(x_1,..,x_n)$.

1.2.2 משפט: אם f חשיבה אז היא ניתנת לחישוב ע"י מכונת מונים.

הוכחה: נוכיח שלכל פונקציה חשיבה יש מכונת מונים המחשבת אותה. לשם כך דרושות לנו ארבע טענות העזר הבאות:

1.2.2.0 טענה: לכל מכונת מונים T_0 m-מקומית יש מכונת מונים T_1 כך ש:

(1) $f_{T_1}^m=f_{T_0}^m$ (בפרט $f_{T_0}^m(x_1,...,x_m)$ מוגדרת אסם $f_{T_1}^m(x_1,...x_n)$ מוגדרת).

(2) T_1 אינה מוחקת נתונים, כלומר (אם $r_0,...,r_n$ ריצה של T_1 המחשבת את $f_{T_1}^m(x_1,...,x_m)$ אז $f_{T_1}^{r_0}, f_{T_1}^{r_n}$ שוות על כל המונים הנזכרים במכונה T_0 חוץ אולי מ-X_0).

(3) כאשר ריצה של T לחשוב $f_T^m(x)$ נעצרת , היא נעצרת בפקודה אחרי האחרונה.

(4) תוכן המונים x_0, x_{m+1} אינו חשוב.

1.2.2.1 טענה: הפונקציות הבסיסיות ניתנות לחישוב ע"י מכונת מונים (באופן הנ"ל).

1.2.2.2 טענה: אם $h(x_1,...,x_m) = f(g,(x_1,...,x_m),...,g_k(x_1,...,x_m))$ כאשר g_i, f ניתנות לחישוב ע"י מכונת מונים אזי h ניתנת לחישוב.

1.2.2.3 טענה: אם g ניתנת לחישוב בלי מחיקת הנתונים אזי גם אופרטור המינימום עליה ניתן לחישוב.

הוכחת טענה 1.2.2.0: יהי m^* כך שהמכונה משתמשת רק במונים מבין $X_0,...,X_{m-1}$. בתוכנית T_1 נתחיל בכך שנעתיק את X_i ל- X_{m+i} לכל $m > i$ כשיסתיים החשוב נעתיק את תוכן X_{m+i} ל- X_i כאשר $i = 1,2,...,m$. ■

הוכחת טענה 1.2.2.1: פונקצית ההיטל היא פשוט העברה ממונה למונה. בכל היתר כבר טיפלנו

פרט לפונקציה: $C_<(x,y) = \begin{cases} 1 & x < y \\ 0 & \text{אחרת} \end{cases}$.

הרעיון: מחסירים x מ- y . אם התוצאה גדולה מאפס כותבים $X_0 = 1$ אחרת משאירים את $X_0 = 0$.

$X_3 = X_3 + 1$	(0)	
$X_0 = X_0 \div 1$	(1)	
$If\ X_0 \neq 0\ GOTO\ 1$	(2)	
$If\ X_2 \neq 0\ GOTO\ 6$	(3)	
$X_0 = X_0 + 1$	(4)	אם הגענו לכאן $X_2 \leq X_1$
$HALT$	(5)	
$If\ X_1 \neq 0\ GOTO\ 8$	(6)	
$HALT$	(7)	אם הגענו לכאן $X_1 \leq X_2$
$X_1 = X_1 \div 1$	(8)	נקטין את X_1 .
$X_2 = X_2 \div 1$	(9)	נקטין את X_2 .
$If\ X_3 \neq 0\ GOTO\ 3$	(10)	נחזור על כל התהליך מההתחלה.

■

<u>הוכחת טענה 1.2.2.2</u>: תהיינה $R_1...R_k$ ו-R מכונות המחשבות את $g_1...g_k$ ואת f בהתאמה בלי למחוק את הנתונים ועוצרות רק בפונקציה אחרי האחרונה. בה"כ המונים המשותפים ל-g_i ול-g_j $(i \neq j)$ הם $X_1...X_n$ בלבד, בהם כתובים הנתונים. עוד נניח כי תוצאת החישוב של g_i נכתבת ב-Y_i. (במקום ב-X_0) ו-R משתמשת במונים $X_0, Y_1, ..., Y_m, Y_{m+1}, ...$. בפרט הנתונים הם ב-$Y_1, ..., Y_m$ והפלט הוא ב-$X_0 = Y_0$, כן אפשר להניח שהמונה היחידי המשותף ל-R ול-R_i הוא Y_i.

תהי R^* המכונה המתקבלת משרשור המכונות $R, R_1...R_k$, כלומר, לכל $i = 1,....,k$ כל פקודה של R_i בה יש קפיצה לכתובת g נחליף את g ב-$g + \sum_{j<i} C(R_j)$ באשר $C(R_j)$ מספר בפקודות הכולל במכונה R_j וכנ"ל לגבי R. אז R^* מחשבת את h. ■

<u>הוכחת טענה 1.2.2.3</u>: נניח כי R מחשבת את $g(x_1,...x_n)$ והתוצאה ב-X_0 כאשר הקלט ב-$X_1...X_n$ ותהי $h(x_2...x_n) = \mu_{x_1}(g(x_1...x_n))$.

המכונה הבאה מחשבת את h (כאשר הקלט כתוב ב-$X_2...X_n$ והתוצאה תהיה כתובה ב-X_0):

	$\vdots$	$\vdots$
$(k+1)$	$If\ \ X_0 \neq 0\ GOTO\ 4$	
$(k+2)$	$X_1 \to X_0$	
$(k+3)$	$HALT$	
$(k+4)$	$X_1 = X_1 + 1$	
$(k+5)$	$If\ \ X_0 \neq 0\ GOTO\ 4$	אם התכנית הגיעה לכאן ברור ש-$X_0 \neq 0$

הערות:

(1) ב-k השורות הראשונות (שאינן מופיעות בתכנית) מופיעות פקודות המכונה R.

(2) אנו מניחים שבתחילת הריצה R מאפסת את X_1.

(3) הכוונה היא שכל פקודה בה R אמורה לעצור תביא את המכונה לפקודה $(k+1)$.

(4) בכל פקודה אחרת מבין הפקודות המכונה תבצע את פקודות R כרגיל. ■

עתה נתחיל בבחינת תכונותיהם של יחסים חשיבים.

<u>1.2.3 הגדרה</u>: יהי $A \subseteq N^k$ יחס k - מקומי על הטבעיים. **הפונקציות האופיינית של A**, $\chi_A : N^k \to \{0,1\}$ מוגדרת ע"י: $\chi_A(\bar{x}) = \begin{cases} 1 & \bar{x} \in A \\ 0 & \bar{x} \notin A \end{cases}$.

<u>1.2.4 הגדרה</u>: יחס $A \subseteq N^k$ נקרא **חשיב** אם χ_A פונקציה חשיבה; נשים לב כי χ_A הנה פונקציה מלאה.

1.2.5 טענה: משפחת היחסים החשיבים סגורה תחת פעולות בוליניות, כלומר, אם $A,B \subseteq N^k$ יחסים חשיבים, אזי היחסים: $A \cup B,\ A \cap B,\ \neg A$, הם חשיבים ($\neg A$ הוא היחס $N^k \setminus A$).

הוכחה: נזכור כי $C_<(X,Y)$ היא פונקציה חשיבה דו-מקומית השווה ל-1 אם $x < y$ ול-0 אחרת. עתה קל לבדוק כי $\chi_{\neg A}(\bar{x}) = C_<(\chi_A(\bar{x}),1)$. לכן, אם A יחס חשיב, $\chi_{\neg A}(\bar{x})$ היא הרכבה של הפונקציות החשיבות $1, \chi_A, C_<$; ולכן היא חשיבה.

לגבי חיתוך – קל לראות כי $\chi_{A\cap B} = \chi_A(\bar{X}) \cdot \chi_B(\bar{X})$. לכן, אם B,A חשיבים אזי $\chi_{A\cap B}$ פונקציה חשיבה כהרכבה של χ_B, χ_A וכפל.

לגבי איחוד הטענה נובעת ממה שכבר הוכחנו, שהרי $A \cup B = \neg(\neg A \cap \neg B)$. ■

הערה: נשים לב שהיחסים

$$A_1(x,y) = (x < y) \quad (1)$$
$$A_2(x,y) = (x \le y) \quad (2)$$
$$A_3(x,y) = (x = y) \quad (3)$$

הם חשיבים.

הוכחה: A_1 חשיב כי הפונקציה האופיינית שלו היא $C_<(x,y)$. בעזרת טענה 1.2.5 נוכל להסיק מכאן שגם A_2 ו- A_3 חשיבים, שהרי:

$$A_3(x,y) \equiv \neg A_1(x,y) \wedge \neg A_1(y,x)$$
$$A_2(x,y) \equiv A_1(x,y) \vee A_3(y,x)$$

■

1.2.6 הגדרה: יהי A יחס חשיב k מקומי. נגדיר אופרטור:

$$\mu_{x<z}[A(x,\bar{y})] = \begin{cases} t & t = \mu_x[A(x,\bar{y})] \text{ ו- } t < z \\ z & \text{אחרת} \end{cases}$$

הערות:

- $A(x,\bar{y})$ פירושו $(x,\bar{y}) \in A$.
- כיוון שאנו מחפשים רק $x < z$, זו פונקציה ומלאה.

1.2.7 טענה: אם A יחס חשיב הפונקציה $h(z,\bar{y}) = (\mu_{x<z})(A(x,\bar{y}))$ היא חשיבה.

הוכחה: נשים לב כי $h(z,\bar{y}) = \mu_x[A(x,\bar{y}) \vee x = z]$. כדי לסיים את ההוכחה יש להראות שהביטוי בסוגריים המרובעים הינו יחס חשיב, אך זה ברור, שהרי הוא מתקבל ע"י פעולות בוליניות (איחוד ושלילה) משני יחסים חשיבים $(=, A)$. ■

הערה: הן בהגדרה 1.2.6 והן בהוכחת טענה 1.2.7 יש אי דיוק פורמלי, בכך שאופרטור מיזער μ הוגדר בשעתו לא על יחסים אלא על פונקציות. לכן נתייחס לביטוי $\mu_x[A(x,\bar{y})]$ כאל קיצורו של הביטוי $\mu_x[\chi_{\neg A}(x,\bar{y})]$ וברור מההגדרות, שאם A יחס חשיב אזי הפונקציה $f(y) = \mu_x[A(x,\bar{y})]$ היא חשיבה, ולכן גם הפעלת האופרטור μ על הפונקציה (החשיבה) $\chi_{\neg A}$.

1.2.8 טענה: אם $A \subseteq N^k$ יחס חשיב, היחס $B(z,\bar{y}) = (\exists x < z)[A(x,\bar{y})]$ הוא חשיב.

<u>הוכחה</u>: לפי הגדרת $\mu_{x<z}$ ברור כי $B(z,\bar{y}) \equiv [(\mu_{x<z})(A(x,\bar{y})) \wedge x<z]$.

שקילות זו מוכיחה את הטענה, שהרי הפונקציה $\mu_{x<z}(A(x,\bar{y}))$ ויחס הסדר > הם חשיבים. ■

<u>1.2.9 הערה</u>: ברור שהיות A חשיבה מבטיחה גם את היות היחס $C(x,\bar{y}) = (\exists x \le z)[A(x,\bar{y})]$ חשיב שהרי $(\exists x < z+1)(A(x,\bar{y})) \equiv C(x,\bar{y})$ חשיב. לעומת זאת, היות A חשיבה אינה מבטיחה את היות היחס $D(\bar{y}) = \exists x(A(x,\bar{y}))$ חשיב. (בהמשך נראה לכך מספר דוגמאות).

לסיכום: כמתים חסומים המופיעים לפני יחס חשיב שומרים על תכונה זו, אך כמתים לא חסומים – בדרך כלל לא.

<u>1.2.10 טענה (הגדרה לפי מקרים)</u>: תהינה $f_1,...,f_n$ פונקציות חשיבות k-מקומיות, ויהיו $A_1,...,A_n \in N^k$ יחסים חשיבים זרים כך ש- $\bigcup_{i-1}^{n} A_i = N^k$. אזי הפונקציה

$$h(\bar{x}) = \begin{cases} f_1(\bar{x}) & \text{אם } A_1(\bar{x}): \\ \vdots & \\ f_m(\bar{x}) & \text{אם } A_m(\bar{x}): \end{cases}$$

היא חשיבה. (נזכור כי $A_i(\bar{x})$ פירושו $\bar{x} \in A_i$). כמו כן, אם $f_1,...,f_n$ מלאות אז כך גם h (בעצם מספיק ש- $A_i \subseteq dom(f_i)$, אך על h יש לדרוש שלמות).

<u>הוכחה</u>: קל להיווכח כי $h(\bar{x}) = \chi_{A_i}(\bar{x}) \cdot f_1(x) + ... + \chi_{A_m}(\bar{x}) \cdot f_1(\bar{x})$, ולכן k חשיבה כהרכבת הפונקציות, f_i, χ_{A_i} כפל וחיבור. ■

תרגילים – פונקציות וקבוצות חשיבות:

1. הראו שהפונקציות הבאות חשיבות:
   - א. לכל n הפונקציה x^n.
   - ב. $[n/m]$ (הערך השלם של n/m).
   - ג. לכל n הפונקציות $f(\bar{x}) = \min(x_1,...,x_n)$ ו- $f(\bar{x}) = \max(x_1,...,x_n)$.
   - ד. $[\log_2(n)]^*$ (המוגדרת לכל $n \neq 0$. בהמשך נראה טענות שיקלו על ההוכחה).
2. הראו שהקבוצות הבאות חשיבות:
   - א. כל קבוצה סופית.
   - ב. כל קבוצה שמשלימה סופי.
   - ג. קב' המספרים הראשוניים.
   - ד. n הוא חזקה של ראשוני, הוא יחס חשיב.
   - ה. קבוצת המספרים הפריקים.
   - ו. קבוצת המספרים מהצורה $2^n 3^m$.
   - ז. *קבוצת המספרים מהצורה 2^{2^n}.

3. הראו כי היחסים הבאים חשיבים:

א. $a \mid b$ (a מחלק את b).

4. $(a,b)=1$ כלומר a זר ל- b.

א. המחלק המשותף הקטן ביותר של (a,b) הוא חזקה שלמה של 2.

ב. $\mathrm{Re}\,m(n,m)=k$ כלומר, השארית בחלוקת n ב- m היא k.

ג. תהי $\Pr(x,y)=(x+y)^2+x+1$. נגדיר פונקציה $\Pr_1(n)$ באופן הבא:

$\Pr_1(n)=\begin{cases} a & (\exists a,b) f(a,b)=n \\ 0 & \text{אחרת} \end{cases}$. באופן דומה נגדיר $\Pr_2(n)$. הראו ש- $\Pr_i$ מוגדרות היטב, חשיבות ומלאות. הסיקו שהיחס $n \in \mathrm{Im}(f)$ חשיב.

5. הראו שלכל פונקציה חשיבה דו מקומית f קיימת פונקציה חשיבה חד מקומית f' כך ש- $\mathrm{Im}(f)=\mathrm{Im}(f')$.

6. תהי $g: N^k \to N^2$. ונניח ש- $\Pr \circ g$ ניתנת לחישוב במכונת מונים ($\Pr$ הפונקציה, שהוגדרה בשאלה הקודמת) אזי הפונקציה g ניתנת לחישוב במכונת מונים שלה פלט דו מקומי (כלומר הפלט של המכונה ניתן בתאים X_0, X_1 והקלט ניתן בתאים $X_2 \ldots X_{k+1}$).

7. תהי $A=\{3^n : n \in N\}$ הראו ש- χ_A חשיבה. האם תוכלו להראות שגם הפונקציה $f(n)=3^n$ חשיבה. האם תוכלו להראות ש- $A=\{6^n : n \in N\}$ חשיבה. (בהמשך נוכיח נשפטים, שיקלו על הוכחת טענה זו).

8. הראו ש- A קבוצה חשיבה אינסופית אסם קיימת פונקציה f חשיבה, מונוטונית עולה ממש ומלאה כך ש- $\mathrm{Im}(f)=A$.

1.3 הצפנות והקשר בין פונקציות חשיבות למכונות חישוב

עד כה הכרנו 3 משפחות של פונקציות:

(1) פונקציות ניתנות לחישוב ע"י מכונות טיורינג.

(2) פונקציות ניתנות לחישוב ע"י מכונות מונים.

(3) פונקציות חשיבות.

במשפט 1.1.15 ראינו שכל פונקציה, הניתנת לחישוב ע"י מכונת מונים, ניתנת לחישוב ע"י מכונת טיורינג. במשפט 1.2.2 הוכחנו שכל פונקציה חשיבה ניתנת לחישוב ע"י מכונת מונים. עתה נפנה להוכיח כי כל פונקציה הניתנת לחישוב ע"י מכונת טיורינג היא חשיבה, ובכך נראה כי שלוש משפחות הפונקציות הנ"ל שוות.

הרעיון שבבסיס ההוכחה שנציג אינו מסובך:
ראשית, נראה שקיימת פונקציה חשיבה, המצפינה סדרות סופיות של טבעיים, כלומר, בהנתן סדרה סופית $\bar{x} = \langle x_1,...,x_n \rangle$ של מספרים טבעיים קיים מספר טבעי y (המצפין את $\bar{x}$) ופונקציה חשיבה $\beta(y,i)$ כך ש- $\beta(y,0)$ הוא האורך של $\bar{x}$ ולכל $1 \le i \le \beta(y,0)$ מתקיים $x_i = \beta(y,i)$.
שנית, נזכור כי בכל רגע נתון בריצה של מכונת טיורינג רק קטע סופי מן הסרט מכיל אינפורמציה, ולכן אפשר לתאר את הסרט בכל שלב בריצה ע"י סדרת טבעיים סופית, $\{\bar{x}_n\}$, ולפי מה שאמרנו כבר, ניתן להתאים לה סדרת טבעים $\{y_n\}$ (y_n מצפין את $\bar{x}_n$). לבסוף נראה שאפשר להצפין לא רק מצבים של מכונת טיורינג אלא גם תהליך חישוב של המכונה ונראה, כי הצפנה זו הנה הרכבה של פונקציות חשיבות.

נטפל, אם כן בנושא של הצפנת סדרות סופיות ע"י מספרים טבעיים. אנו נראה שקיימת פונקציה חשיבה $\beta : N^2 \to N$ בעלת התכונה הבאה: לכל סדרה $\langle a_1,...,a_n \rangle$ של מספרים טבעיים, יש מספר טבעי b כך ש- $\beta(b,1) = a_1,...,\beta(b,n) = a_n$. באופן זה מצפינה הפונקציה β כל סדרה סופית של מספרים טבעיים ע"י המספר b המתאים. נרצה להוכיח:

<u>1.3.1 משפט</u>: קיימת פונקציה שלמה וחשיבה $\beta(x,y)$ כך ש:

(1) לכל סדרה סופית $\langle a_1,...,a_n \rangle$ יש b שלכל $1 \le i \le n$ $a_i = \beta(b,i)$ וכן $n = \beta(b,0)$.

(2) לכל x ו- y מתקיים $\beta(x,y) \le x$.

בהמשך יתברר לשם מה דרושה התכונה הנוספת (2). לצורך הוכחת המשפט נביא מספר טענות עזר [1.3.2-1.3.5].

<u>סימון</u>: לכל x ולכל $y \ne 0$, תהי $\mathrm{Re}\,m(x,y)$ השארית בחלוקת x ל- y.

<u>1.3.2 טענה</u>: $\mathrm{Re}\,m(x,y)$ היא פונקציה חשיבה.

<u>הוכחה</u>: קל לראות כי $\mathrm{Re}\,m(x,y)=\mu_z[\exists t(x=t\cdot y+z)]$ זה עדיין לא מוכיח שהפונקציה חשיבה, כי יש כאן כמת לא חסום. אך אם נזכור שהמנה בחילוק מספרים טבעיים לעולם אינה גדולה מהמחולק, נוכל להחליף את $\exists t$ ב-$(\exists t\le x)$ וזה יראה שהפונקציה חשיבה. ■

הגדרה: הפונקציה $P(x,y)=\frac{1}{2}(x+y)^2+\frac{1}{2}(x+y)+x$ נקראת פונקציות הזיווג, והיא מסדרת את איברי N^2 בסדרה לפי שיטת האלכסון של קושי. תכונות פונקצית הזיווג:

(1) חח"ע.

(2) על.

(3) זו פונקציה חשיבה.

(4) לכל $x,y\in N$ מתקיים $P(x,y)\ge x, P(x,y)\ge y$.

התכונות (3) , (4) הן מיידיות מהגדרת הפונקציה, ואילו (1), (2) מיידיות משתי הטענות הבאות:

<u>טענה א'</u>: לכל $z\in N$ קיים n טבעי יחיד כך ש: $\frac{1}{2}n^2+\frac{1}{2}n\le z\le\frac{1}{2}n^2+\frac{1}{2}n+n$ (*)

(n יהיה מספר האלכסון שבו מופיע $P^{-1}(z)$ בהצגה הציורית).

<u>טענה ב'</u>: עבור n,z טבעיים נתונים (*) מטענה א' מתקיים אסם יש $x,y\in N$ כך ש- $x+y=n$ ו- $P(x,y)=z$.

<u>הוכחת טענה א'</u>: יהי $n=\max\{m:\frac{1}{2}m^2+\frac{1}{2}m\le z\}$. ברור ש- n מקיים את האי שוויון השמאלי של (*). לגבי הימני - אם לא אז $\frac{1}{2}n^2+\frac{1}{2}n^2+n<z$ וזה גורר $\frac{1}{2}(n+1)^2+\frac{1}{2}(n+1)<z+1$, מה ששקול לאי שוויון $\frac{1}{2}(n+1)^2+\frac{1}{2}(n+1)\le z$, העומד בסתירה למרביות (= למקסימליות) n.

לגבי היחידות: אם גם n' מקיים את (*) אז $n'\le n$ בגלל מרביות (מקסימליות) n, אך לא יתכן $n>n'$ כי אז $n\ge n'+1$ וזה גורר (מהאי שוויון הימני עבור $n-1$) $\frac{1}{2}n^2+\frac{1}{2}n\ge z+1$ מה ששקול לאי שוויון: $\frac{1}{2}n^2+\frac{1}{2}n>z$ העומד בסתירה לכך, ש- n מקיים את (*).

<u>הוכחת טענה ב'</u>: יהיו n,z המקיימים את (*) ויהיו $y=n-x$, $x=z-\frac{1}{2}n(n+1)$.

$x\ge 0$ בגלל האי שוויון השמאלי של (*) ו- $y\ge 0$ בגלל הימני. לכן x,y טבעיים, וברור כי $P(x,y)=z$.

הכיוון השני: נניח שיש $x,y\in N$ שסכומם n וכן $P(x,y)=z$. אזי

$$\frac{1}{2}n^2+\frac{1}{2}n=\frac{1}{2}(x+y)^2+\frac{1}{2}(x+y)\le p(x,y)\le\frac{1}{2}(x+y)^2+\frac{1}{2}(x+y)+(x+y)=\frac{1}{2}n^2+\frac{1}{2}n+n$$

כלומר, n ו- z מקיימים את (*).

מאחר ש-P חח"ע ועל, לכל $z \in N$ יש זוג יחיד $< a,b > \in N^2$ כך ש- $P(a,b) = z$. נסמן:

$a = P^L(z), b = P^R(z)$. נראה שאלו פונקציות חשיבות.

1.3.3 טענה:

(1) הפונקציות $\left.\begin{array}{l} P^L(z) = \Pi_1^1 P^{-1}(z) \\ P^R(z) = \Pi_1^2 P^{-1}(z) \end{array}\right\}$ הן חשיבות.

(2) לכל $z \in N$, $P^L(z) \le z$.

הוכחה:

(1) קל לראות כי $\left.\begin{array}{l} P^L(z) = \mu_x[\exists y](P(x,y) = z] \\ P^R(z) = \mu_y[\exists x](P(x,y) = z] \end{array}\right\}$. כאמור, P פונקציה חשיבה, ולכן כדי לראות שהפונקציות הנדונות חשיבות די אם נחסום כאן את הכמתים, ואמנם לפי תכונה (4) של פונקצית הזיווג, לכל x ו-y מתקיים $P(x,y) \ge x,\ P(x,y) \ge y$; נוכל איפה להחליף את $\exists x$ ו-$\exists y$ ב- $\exists x \le z$ ו- $\exists y \le z$.

(2) מידי מתכונה (4) של פונקציית הזיווג. ■

1.3.4 טענה (משפט השאריות הסיני): יהיו $d_1,...,d_n$ מספרים טבעיים חיוביים זרים בזוגות (כלומר אין $d > 1$ המחלק שנים מהם). אזי לכל סדרה $\langle a_1,...,a_n \rangle$ של מספרים טבעיים, המקיימת $a_i < d_i$ לכל i, יש b טבעי כך שלכל i מתקיים $\mathrm{Re}m(b,d_i) = a_i$.

הוכחה: לכל $b < \prod_{i-1}^{n} d_i$ נסמן $\bar{b} =< \mathrm{Re}m(b,d_1),...,\mathrm{Re}m(b,d_n) >$, הפונקציה $b \to \bar{b}$ היא העתקה מקבוצת המספרים הקטנים מ- $\prod_{i-1}^{n} d_i$ לקבוצת הסדרות באורך n שבהן האיבר ה- i בסדרה קטן מ- d_i (כי הוא שארית בחלוקה ב- d_i) מספר הסדרות האלה הוא $\prod_{i-1}^{n} d_i$.

ברור שאם נראה שהעתקה זו היא על, משפטנו הוכח. אך זאת העתקה בין 2 קבוצות סופיות בנות אותו מספר איברים ולכן די אם נוכיח שהיא חח"ע. נניח איפוא שיש $b_1,b_2 < \prod_{i-1}^{n} d_i$ כך ש- $\bar{b}_1 = \bar{b}_2$. אזי לכל $1 \le i \le n$, $\mathrm{Re}m(b_1,d_i) = \mathrm{Re}m(b_2,d_i)$, כלומר: $b_2 - b_1$ מתחלק בכל d_i.

בגלל זרות ה- d_i-ים, נובע מכך ש- $b_2 - b_1$ מתחלק ב- $\prod_{i-1}^{n} d_i$ וזו סתירה כי $\prod_{i-1}^{n} d_i > b_2 - b_1$. ■

1.3.5 טענה: לכל n טבעי, הסדרה $< 1+n!, 1+2(n!),...,1+n(n!) >$ היא סדרת מספרים זרים.

הוכחה: יהיו $i \ne j,\ i,j \le n$ כך ש- $1+i(n!)$ אינו זר ל- $1+j(n!)$. כלומר, יש k ראשוני ששניהם מתחלקים בו. לכן גם הפרשם $n!(i-j)$ מתחלק ב-k. בגלל ראשוניות k נובע ש-$n!$ או $(i-j)$ מתחלקים ב-k. כיוון ש- $n > i-j$ בכל מקרה נקבל ש-$n!$ מתחלק ב-k.

מאחר ש-$n!$ מתחלק ב-k, המספר $1+(n!)\cdot i$ אינו מתחלק ב-k, בסתירה להנחה על k. ■

<u>הוכחת משפט 1.3.1</u>: תהי $\gamma(z,y,i)=\mathrm{Re}m(z,1+y(i+1))$. נראה של-$\gamma$ התכונות הבאות:

(1) γ פונקציה חשיבה.

(2) לכל סדרה סופית $\langle a_1,...a_n\rangle$ יש y,z כך שאם $0\le i<n$ אז מתקיים $a_i=\gamma(z,y,i)$.

(3) לכל z,y,i טבעיים, $\gamma(z,y,i)\le z$.

זה יספיק, כי אם נגדיר $\beta(b,i)=\gamma(P^L(b),P^R(b),i)$, נקבל ש-$\beta$ חשיבה לפי (1) וטענה 1.3.3; β מקיימת את הדרישה (1) של משפטנו לפי תכונה (2) תוך שימוש בפונקציית הזיווג; β מקיימת את הדרישה (2) של משפטנו לפי תכונה (3). נותר איפה רק להוכיח את התכונות הנ"ל של הפונקציה γ.

התכונה הראשונה מיידית מטענה 1.3.2 ומהיות פונקצית ההיטל חשיבה.

עתה, אם $\langle a_1,...a_n\rangle$ סדרה סופית של טבעיים נבחר $k>n$ כך שלכל i, $k>a_i$. יהי $y=k!$. לפי טענה 1.3.5 n המספרים $\{1+yi:1\le i\le n\}$ הם זרים, לכן לפי משפט השארית הסיני (טענה 1.3.4) קיים z כנדרש בתכונה השנייה של γ. התכונה השלישית של γ נובעת ישירות מכך שהשארית בחלוקה לעולם אינה גדולה מהמחולק. ■

הפונקציה β שהוגדרה כאן תשמש אותנו לכל אורכה של הוכחת משפט גדל.

לפי המשפט שהוכחנו, נוכל עתה להצפין כל סדרה סופית באופן הבא:

בהינתן $\langle a_1,...a_n\rangle$ נבחר ℓ טבעי כך ש-

$\beta(\ell,0)=n,\ \beta(\ell,1)=a_1,\ \beta(\ell,2)=a_2,...,\beta(\ell,n)=a_n$. כך נצפין ע"י המספר ℓ גם את אורך הסדרה וגם את אבריה. נגדיר איפה:

<u>1.3.6 הגדרה</u>: b נקרא **צופן של הסדרה** $\langle a_1,...a_n\rangle$ אם $n=\beta(b,0)$ ולכל $0\le i\le n$ מתקיים $a_i=\beta(b,i)$.

נשים לב שלפי תכונות הפונקציה β, אם b הוא צופן של $\langle a_1,...a_n\rangle$ אזי $n\le b$ ולכל $1\le i\le n$ מתקיים $a_i\le b$. כמו כן ברור שכל מספר טבעי מצפין סדרה יחידה: פשוט מפעילים את β בהתאם ומקבלים את הסדרה. מאידך לכל סדרה יש צופן, אך לאו דוקא יחיד, שהרי יתכן למצוא c עם $\beta(c,i)=\beta(b,i)$ לכל $1\le n$ אבל $\beta(c,n+1)\ne\beta(b,n+1)$ (הסדרה, כזכור באורך n).

מהגדרה 1.3.6 ומהיות β חשיבה נובע, שהתכונה "b הוא צופן של $\langle a_1,...a_n\rangle$" היא יחס חשיב.

ולכן נקבל:

<u>1.3.7 מסקנה</u>: לכל k טבעי קיימת פונקציה חשיבות $Seq_k:N^k\to N$ כך ש- $Seq_k(\langle a_1,...,a_k\rangle)$ הוא צופן של הסדרה $\langle a_1,...a_n\rangle$.

<u>הוכחה</u>: נגדיר $Seq_k(\langle a_1,...,a_k\rangle):=\mu_b[\langle a_1,...,a_k\rangle$ *צופן עבור* $b]$. מאחר שהיחס בסוגריים המרובעים הוא חשיב, שוויון זה מוכיח את היות Seq_k חשיבה. ■

לפעמים נסמן $\langle a_1,...a_n \rangle$ במקום $Seq_k(\langle a_1,...,a_k \rangle)$. למשל, במקום "X צופן של $\langle a_1,...a_n \rangle$" נכתוב בקיצור (אך בחוסר דיוק): $X = \langle a_1,...,a_n \rangle$.

נוכיח עתה שאפשר להצפין לא רק סדרות אלא גם מצבים (קונפיגורציות) ומסעים של מכונות טיורינג. הצפנה זו תאפשר לנו להפוך את תהליך החישוב של המכונה להצגת הפונקציה המחושבת כהרכבת פונקציות חשיבות, ובכך יוכח שבמכונות טיורינג אפשר לחשב רק פונקציות חשיבות.
יהי S האי"ב של המכונה ותהי Q קבוצת המצבים הפנימיים. נניח בה"כ ש- $S \cap Q = \phi$. כדי להצפין מצב עלינו להצפין (1) את הכתוב על הסרט; (2) את המצב הפנימי של המכונה; (3) את מקום הראש הקורא בסרט.
החישוב של פונקציה בעזרת המכונה מתבצע כך שבכל שלב של החישוב יש בסרט תחום סופי שמחוצה לו כתובים רק B-ים. בתיאור הסרט, נוכל איפה להסתפק בטיפול בתחום סופי זה. נניח עתה שבמצב מסויים בתחום הנ"ל כתוב על הסרט $S_1,...,S_j,...,S_n$; מצבה הפנימי של המכונה הוא q; והראש הקורא נמצא על S_j . נתאר מצב זה ע"י הסדרה:

$\langle S_1,...,S_j,q,S_{j+1},...,S_n \rangle$ (את המצב הפנימי q כותבים מימין לאות שעליה נמצא הראש הקורא).

כלומר כל מצב מוצפן ע"י סדרה סופית של איברי $S \cup Q$ שבה מופיע איבר של Q בדיוק פעם אחת, אך לא בתחילת הסדרה.

(בעצם צריכים לדקדק בהצפנת מצב, ולתת גם את המספר השלם אשר "בו מתחיל הסרט" כלומר את מספר התא שבו מתחיל התחום הסופי שרק אותו אנו מצפינים. אך זה לא משנה מבחינה מהותית – אפשר להזיז הכל על פני השלמים ולא ישתנה דבר מבחינת החישוב במכונה).

כעת תהי T מכונת טיורינג קבועה עד סוף הדיון. האי"ב S_T וקבוצת המצבים הפנימיים Q_T הן קבוצות סופיות, ולכן יש k,l טבעיים כך ש- $|S_T| = k, |Q_T| = \ell$. נניח איפוא בה"כ, כי $S_T = \{0,...,k-1\}; Q_T\{k,...,k+\ell-1\}$. לכן, בה"כ כל מצב ניתן להצגה כסדרה של מספרים טבעיים שכולם קטנים מ- $k+\ell$, ואחד מהם (אך לא הראשון) גדול מ- $k-1$. ניתן איפה להצפין מצב ע"י מספר – צופן של סדרה זו. מספר המצפין מצב M נקרה מספר גדל של המצב ומסומן ע"י M^{GN} [$Godel\ Number\ of\ M$] . כלומר, בסימונים דלעיל, $M^{GN} = \langle S_1,...,S_j,q,S_{j+1},...,S_n \rangle$
נשים לב, שמספר גדל של מצב הוא לעולם לפחות 2. שהרי לפי הגדרת מכונת טיורינג, תמיד $1, B \in S_T$ ולכן $k = |S_T| \geq 2$, אך כל סדרה המתארת מצב מכילה איבר של Q_T, כלומר מספר n כך ש- $n \geq k \geq z$. ומאחר שמספר שמצפין סדרה הוא גדול מכל איבריה, נובעת מכאן טענתנו [נשתמש בכך באחד המשפטים הבאים].

<u>הערות</u>:

(1) תכונות חשיבות: כשאנו אומרים שתכונה $\varphi(\bar{x})$ הוא חשיבה, הכוונה היא שהיחס $\{\bar{x} \in N^k : \varphi(\bar{x})\}$ הוא חשיב.

(2) להגדרת הצפנה של סדרות: הגדרנו מתי x נקרא צופן של הסדרה $\langle a_1,...,a_n \rangle$ הגדרה 1.3.6). כפי שכבר הערנו, הצופן של סדרה לפי הגדרה זו אינו יחיד וזה לא נוח. לכן נשנה כאן את ההגדרה: הצופן של סדרה סופית יהיה המספר המזערי (=המינימלי) שהוא צופן שלה לפי ההגדרה הקודמת. יש לשים לב שמכאן נובע שלא כל מספר הוא צופן של סדרה סופית, אם נסמן ע"י $\vartheta(\bar{x})$ את התכונה "x הוא צופן של סדרה סופית", $\vartheta(\bar{x})$ היא תכונה חשיבה בגלל השקילות $\vartheta(x) \equiv \neg(\exists y < x)(\forall i \le \beta(x,0))[\beta(x,i) = \beta(y,i)]$, כלומר, x מצפין סדרה (לפי ההגדרה החדשה) אם לא קיים $y < x$ אשר מצפין (לפי ההגדרה הקודמת) אותה סדרה כמו x.

(3) יחסים חשיבים: הוכחנו שמשפחת יחסים החשיבים סגורה תחת חיתוך ושלילה (טענה 1.2.5). נשים לב שנובע מכאן, שאם $\varphi(x) \equiv [\varphi_1(x) \to \varphi_2(x)]$ אזי אם $\varphi_2(x)$ ו- $\varphi_1(x)$ חשיבות אז φ חשיבה, שהרי $[p \to q] \equiv [\neg(p \wedge \neg q)]$.

נזכור שאנו עוסקים עדיין במכונה T קבועה שעבורה הנחנו $S_T = \{0,...,k-1\}$; $Q_T = \{k,...,k+\ell+1\}$. לשם נוחות נניח שתמיד המספרים $k,1,0$ עומדים במקום $q_0,1,B$ בהתאמה (q_0 - המצב ההתחלתי של T).

<u>1.3.8 טענה</u>: תהי $\varphi(x)$ התכונה "x מצפין מצב של T" אזי $\varphi(x)$ חשיבה.

<u>הוכחה</u>: לפי האמור לעיל, x מצפין מצב אסם הוא מצפין סדרה סופית שבה איבר אחד שייך ל- Q_T אך לא הראשון, וכל שאר האיברים שייכים ל- S_T. תהי $\varphi_1(j,x)$ התכונה: "x מצפין סדרה; $j > 1$, האיבר ה- j בסדרה הוא מ- Q_T, ושאר איבריה מ- S_T". לפי האמור לעיל, $\varphi(x) \equiv (\exists j \le \beta(x,0))(\varphi_1(j,x))$ (כאשר, נזכור ש- $\beta(x,0)$ הוא אורך הסדרה המתאימה ל-x). לכן די אם נראה ש- $\varphi_1(x,j)$ תכונה חשיבה, וזה נובע מהשקילות:

$$\varphi_1(x,j) \equiv \vartheta(x) \wedge j > 1 \wedge k \le \beta(x,j) \le k+\ell \wedge [\forall i \le \beta(x,0)(i \ne j \to \beta(x,i) \le k]$$

כאשר:

- $\vartheta(\bar{x})$ הנוסחה האומרת ש- x מצפין של סדרה סופית.
- האיבר ה- j בסדרה (הנתון ע"י $\beta(x,j)$) שייך ל- Q_T.
- כל איברי הסדרה האחרים (הנתונים ע"י $\beta(x,i)$ ל- $i \ne j$) הם מ- S_T. ■

<u>1.3.9 טענה</u>: תהי $\psi(x,y)$ התכונה "x מצפין מצב של T ו- y מצפין מצב עוקב לו" אזי ψ חשיבה.

<u>הוכחה</u>: תהי $\varphi_1(j,x)$ התכונה שהוגדרה בהוכחת הטענה הקודמת. לכל פקודה P של המכונה T תהי $\chi_P(x,y,j)$ התכונה: "P פקודה רלוונטית למצב ש-x מצפין ו- y המצב המתקבל ממנו לפי P". (הפרמטר j הוא מקומו של המצב הפנימי בסדרה ש-x מצפין בדומה למצב בהוכחת הטענה הקודמת). קל להיווכח כי:

$$\psi(x,y) \equiv \exists j \le \beta(x,0)((\varphi_1(x,j) \wedge \bigvee_P \chi_P(x,y,j))$$

(האיחוד הוא על כל הפקודות P של T, והוא סופי בגלל סופיות מספר הפקודות). לכן כדי להוכיח כי ψ חשיבה, די אם נראה שלכל פקודה P χ_P תכונה חשיבה.

קיימים 3 סוגי פקודות: (1) פקודות שצורתן $sqLq'$; (2) פקודות שצורתן $sqRq'$; (3) פקודות שצורתן $sqs'q'$.

נוכיח את הדרוש רק לגבי (1) ולגבי השאר ההוכחה דומה. נניח איפוא כי P היא הפקודה $sqLq'$.

לשם קיצור, לכל i טבעי נסמן $x_i = \beta(x,i)$, $y_i = \beta(y,i)$ (לפי סימון זה, אורכי הסדרות ש- y,x מצפינים הם x_0, y_0). נניח ש-x מצפין את הסדרה: $\langle x_1,\dots,x_{n+1}\rangle = \langle s_1,\dots,s_{j-1},s_j,q,s_{j+1},\dots,s_n\rangle$

כלומר, את מצב המכונה בו על הסרט כתובים $s_1,\dots,s_n$, המכונה במצב פנימי q והראש הקורא במקום j (לשם הנוחות נניח ש-x אינו מצפין אינפורמציה מיותרת, כלומר אינו מצפין סדרה המתחילה או מסתיימת ברצף של B-ים. ברור שאין כל קושי לעבור באופן חשיב מ-x כלשהו ל-x' המצפין אותה אינפורמציה וללא רצפי ה-B-ים המיותרים. ראו גם טענה 2.1.1). עתה עלינו לומר כי:

(1) P רלוונטית למצב ש-x מצפין: נבטא זאת ע"י הנוסחה $\gamma_P(x,j) = [s = x_j \wedge q = x_{j+1}]$.

(2) y מצפין סדרה סופית: $\vartheta(y)$ כמקודם.

(3) הסדרה ש- y מצפין זהה בקטעים הרלוונטיים לזו ש-x מצפין פרט לכך ש-$\langle s_j,q\rangle$ הוחלף ב-$\langle q',s_j\rangle$:

$$y_0 \ge x_0 \wedge (\exists i \le y_o - x_0)(\forall n \le y_0)[0 < n < i \to y_n = 0 \wedge n > i + x_0 \to y_n = 0 \wedge$$
$$i \le n < i + j - 1 \to y_n = x_{n-i} \wedge y_{i+j-1} = q' \wedge y_{i+j} = x_j]$$

כאשר שני התנאים הראשונים מבטיחים שמחוץ לקטע הרלוונטי ל- x y מצפין רק B-ים. ועתה, קל לראות כי $\chi_P(x,y,j)$` היא החיתוך של שלוש התכונות הנ"ל, ולכן חשיבה. ■

<u>1.3.10 טענה</u>: הפונקציה $F_0(x)$ המוגדרת ע"י

$$F_0(x) = \begin{cases} y & \text{x מצפין מצב של T שיש לו עוקב ו – y מצפין עוקב זה} \\ 0 & \text{אחרת} \end{cases}$$

הינה חשיבה.

<u>הוכחה</u>: תהי $\psi(x,y)$ כבהוכחת טענה 1.3.9. ברור כי

$$F_0(x) = \begin{cases} \mu_y[\psi(x,y)] & \exists y[\psi(x,y)] \\ 0 & \text{אחרת} \end{cases}$$

ולכן כדי להוכיח כי F_0 חשיבה, די אם נראה שהתכונה $\gamma(x) = \exists y[\psi(x,y)]$ היא חשיבה. וזה נובע ממה שכבר עשינו בטענה 1.3.9. ■

עתה נתקדם צעד נוסף, וכשם שהצפנו מצב, נצפין גם מסע:

1.3.11 הגדרה: נאמר שמספר x **מצפין סדרת מצבים** $M_0,...,M_n$ של T אם $x=\langle M_0^{GN},...,M_n^{GN}\rangle$ (כלומר, x הוא הצופן של $\langle M_0^{GN},...,M_n^{GN}\rangle$).

1.3.12 טענה: התכונות הבאות חשיבות:

(1) $x''=\psi_1(x)$ מצפין סדרת מצבים של T".

(2) $x''=\psi_2(x)$ מצפין מצב התחלתי של T".

(3) $x''=\psi_3(x)$ מצפין מצב סופי של T".

(4) $x''=\psi_4(x)$ מצפין סדרת מצבים של T שהיא מסע אשר הסתיים".

(5) $x''=\psi_5(x,y)$ מצפין מצב התחלתי של T, ו- y מצפין מסע שהסתיים של T המתחיל במצב ש- x מצפין".

הוכחה: נמשיך להשתמש בקיצור $x_i=\beta(x,0)$ לכל i, $\vartheta(x)$ אומר ש- x מצפין סדרה סופית ו- $\varphi(x)$ אומר ש- x מצפין מצב של T.

(1) ψ_1 חשיבה, כי $\psi_1(x)\equiv\vartheta(x)\wedge x_0>0\wedge(\forall i\le x_0)(i>0\to\varphi(x_i))$.

(2) מצב התחלתי של T הוא מצב בו המכונה במצב פנימי q_0, משמאל לראש הקורא יש רק סימני B וכך גם אחרי הקלט האחרון. לכן:

$$\psi_2(x)=\vartheta(x)\wedge(\exists i\le x_0)(\exists j\le x_0)[(\forall n<i)(\overset{(i)}{x_n=0})\wedge(x_i=k\wedge\overset{(ii)}{x_{i+1}=1})\wedge$$
$$(\forall n\le x_0)(n>i\to\overset{(iii)}{x_n=0}\vee x_n=1)\wedge(\forall n<j)(n>i\wedge\overset{(iv)}{x_n=0}\to x_{n+1}=1)\wedge$$
$$(\forall n\le x_0)(n>j\overset{(v)}{\to}x_n=0)]$$

(i) אומר שעד למקום ה- i בסדרה ש- x מצפין יש רק B.

(ii) אומר שבמקום ה- i עומד הראש הקורא, וששם אכן מתחיל הקלט.

(iii) אומר שאחרי המקום ה- i אין בסדרה אברים מ- Q_T.

(iv) אומר שאחרי כל B בסדרה מתחיל קלט חדש.

(v) אומר שאחרי המקום ה- j בסדרה נגמר הקלט.

לכן גם ψ_2 חשיבה.

(3) תהי F_0 הפונקציה מטענה 1.3.10 נראה כי: $\psi_3(x)=[\varphi(x)\wedge F_0(x)\ne 0]$ (ובזה נסיים).

ואמנם: ברור שאם ל- x יש עוקב, $F_0(x)$ הוא מספר גדל של עוקב, וכפי שהערנו כבר מספר כזה הוא לפחות 2, ולכן $\ne 0$.

(4) תהי $\psi(x,y)$ התכונה "x מצפין מצב ו- y מצפין מצב עוקב לו" אז ψ חשיבה לפי טענה 1.3.9. יהי $n=x_0$ אורך הסדרה ש- x מצפין. אזי רקורסיביות ψ_4 נובעת מהשקילות:

$$\psi_4(x)\equiv\psi_1(x)\wedge\psi_2(x_1)\wedge(\forall i\le n)[(i\ge 2\to\psi(x_{i-1},x_i))]\wedge\psi_3(x_n).$$

(5) ψ_5 חשיבה משום ש: $\psi_5(x,y)=\psi_4(y)\wedge x=y_1$. ■

1.3.13 טענה: הפונקציות F_3,F_2,F_1 המוגדרות להלן הן חשיבות:

$$F_1(x)=\begin{cases} x \text{ מצפין סדרה לא ריקה האיבר האחרון בסדרה ש}-x \text{ מצפין} \\ 0 \quad \text{אחרת} \end{cases}$$

$$F_2(x)=\begin{cases} n & x \text{ מצפין מצב סופי תקני} \\ 0 & \text{אחרת} \end{cases}$$

כאשר מצב סופי תקני (סטנדרטי) הוא מצב סופי של המכונה בו הראש הקורא משמאל לפלט והפלט נתון בצורה של n-יה רצופה של 1-ים (ראו הגדרה 1.1.10) .

לבסוף, אם T מחשבת את הפונקציה $f(x_1,...,x_n)$ אז $F_3(x_1,...,x_n)$ יהיה הצופן של המצב ההתחלתי בחישוב $f(x_1,...,x_n)$.

בשלב זה נשאיר הוכחת טענה זו לקורא.

1.3.14 משפט: כל פונקציה שניתנת לחישוב ע"י מכונת טיורינג, היא חשיבה.

הוכחה: תהי $f(x_1,...,x_n)$ פונקציה המחושבת ע"י המכונה T. לפי חלק (2) במשפט 1.1.9, בכל מסע שמסתיים המצב הסופי הוא, בלי הגבלת הכלליות, מצב סופי תקני (סטנדרטי). נגדיר:

$F_4(x_1,...,x_4)=\mu_y\left[\psi_5(F_3(x_1,...,x_4),y)\right]$.

נסביר את משמעותה של F_4: נזכור כי $F_3(x_1,...,x_n)$ הוא צופן של המצב ההתחלתי במסע לחישוב $f(x_1,...,x_n)$ ואילו $\psi_5(x,y)$ מטענה 1.3.12 היא התכונה: "y מצפין מסע מסתיים המתחיל במצב ש-x מצפין". לכן F_4 היא פונקציה (חלקית) הנותנת את הצופן של המסע לחישוב $f(x_1,...,x_n)$ אם יש מסע מסתיים כזה, ואחרת אינה מוגדרת. F_4 פונקציה חשיבה, כי הוכחנו ש-F_3 ו-ψ_5 חשיבות.

עתה אם $f(x_1,...,x_n)$ מוגדר, כלומר, אם קיים מסע מסתיים המחשב את $f(x_1,...,x_n)$ אז $f(x_1,...,x_n)=F_2(F_1(F_4(x_1,...,x_n)))$ כלומר: $f(x_1,...,x_n)$ היא מספר ה-1-ים במצב הסופי של המסע של T לחישוב f.

לעומת זאת, אם $f(x_1,...,x_n)$ אינו מוגדר, כלומר, לא קיים מסע מסתיים המחשב אותו, אזי F_4 אינה מוגדרת ולכן גם אגף ימין בשויון למעלה אינו מוגדר. בסיכום, אגף ימין מוגדר אסם שמאל מוגדר, וכששניהם מוגדרים הם שווים. לכן השוויון למעלה מראה שהפונקציה f היא למעשה הרכבה של הפונקציות F_2,F_1,F_4, ולכן היא חשיבה. ■

עתה סגרנו את המעגל, ויש לנו שלוש הגדרות שקולות עבור הפונקציות החשיבות. לכן בהמשך הדיון בחשיבויות נוכל להשתמש לסירוגין בכל אחת מהן, לפי הנוחות.

תרגילים - מכונות חישוב ופונקציות חשיבות:

1. תהי $A \subseteq N$ קבוצה חשיבה הראו שגם הקבוצות הבאות חשיבות:

א. אוסף כל הטבעיים שהם חזקות של אברי A.

ב. אוסף כל הטבעיים שניתן להביעם כסכום של איברים ב-A.

2. נציע וריאציה להוכחת הצפנת סדרות סופיות. נגדיר $\Pr(x,y) = (x+y)^2 + x + 1$.

בתרגיל קודם הראתם ש- Pr חח"ע, ושהפונקציות ההפוכות $\Pr_i$ חשיבות. עתה נגדיר:

$\beta(n,i) = \mu_{x<n\div 1}(\exists y,z<n)(n = \Pr(y,z) \wedge (1+(\Pr(x,i)+1)z) \mid y)$.

א. שתמשו בטענה 1.3.3 כדי להוכיח שלכל סדרה סופית $a_0 \ldots a_n$ יש b טבעי המקיים $\beta(b,i) = a_i$ לכל $i \le n$.

ב. הראו ש- β מקיימת את התכונות הנדרשות מפונקצית ההצפנה.

3.

א. הוכיחו שהפונקציה $\gamma(b,i) = \Pr_1^i(b)$, כלומר, הפונקציה $\Pr_1$ מופעלת i פעמים על b, היא פונקצית הצפנה חשיבה.

ב. מדוע לא יכולנו להשתמש בפונקציה γ, שהוגדרה בסעיף הקודם (או אפילו בפונקצית הצפנה פשוטה יותר דוגמת $\delta(b,i) = \max_n\{p_i^n \mid b\}$ באשר p_i הראשוני ה-i), והשתמשנו בפונקציה המורכבת יותר שהוגדרה במשפט 1.3.1 או בזו שבסעיף א'.

4. הראו שקיים $n \in N$ כך שלכל מכונת מונים R יש מכונת מונים R' בעלת פחות מ-n מונים השקולה לה (כלומר, לכל x ריצת R' על x מסתיימת אם ריצת R על x מסתיימת ובמקרה זה תוצאת הריצה של שתי המכונות זהה).

5. הוכיחו ישירות, מבלי להשתמש במשפט על השקילות של מכונות מונים ופונקציות חשיבות, שמשפחת הפונקציות החשיבות סגורה תחת הגדרה באינדוקציה. כלומר, אם $H(x)$ ו-$G(x,y,z)$ חשיבות אזי הפונקציה

$$F(x,y) = \begin{cases} H(x) & y = 0 \\ G(x,z,F(x,z)) & y = z+1 \end{cases}$$ חשיבה.

6. לכל $l \in N$ נגדיר פונקציה $b_l \in N$ באופן הבא:

$$b_0(n) = 2n$$

$$b_{l+1}(n) = \underbrace{b_l(b_l(b_l \ldots (1) \ldots)))}_{n+1 \text{ פעמים}}.$$

א. מהם $b_1(n), b_2(n), b_3(n)$.

ב. הראו ש- b_l חשיבה לכל $l \in N$. הסיקו שהפונקציה $A(l) = b_l(l)$ חשיבה.

7. הגדרה: נאמר שפונקציה f היא חשיבה פרימיטיבית אם היא בסגור של הפונקציות $f(n) = n+1,\ I_n^m f(n) = n \div 1$ (ההיטל על הקואורדינטה ה-m מבין n) תחת הפעולות:

הגדרה ע"פ מקרים: $f(n)=\begin{cases} g_0(n) & h(n)=0 \\ g_1(n) & \text{אחרת} \end{cases}$ באשר h, g_1, g_2 ח"פ.

הרכבה: $f(n)=G(h_1(n)\ldots h_k(n))$, G, h_i ח"פ.

הגדרה באינדוקציה פרימיטיבית (ראו הגדרה בשאלה קודמת).

הראו כי הפונקציה A, שהוגדרה בשאלה הקודמת אינה ח"פ. רמז: הראו באינדוקציה על בניית f שכל פונקציה ח"פ חסומה ע"י הפונקציה b_l לאיזה l מספיק גדול.

8.

א. הוכיחו שהאופרטור מזער (μ) אינה ח"פ, כלומר, תיתכן $F(\overline{X}, y)$ ח"פ אבל $\mu_y F(\overline{X}, y)$ אינה ח"פ.

ב. מהי השגיאה בנימוק הבא:

$\mu_x f(y_1 \ldots y_n, x) = z \Leftrightarrow (\forall i < z)(\beta(b,i) > 0) \wedge \beta(b,z) = 0$, באשר b מצפין את הסדרה $f(y_1 \ldots y_n, 0) \ldots f(y_1 \ldots y_n, z)$. (שימו לב שמשאלה 2 נובע שניתן להגדיר פונקצית הצפנה שהיא ח"פ).

2 משפט גדל ומסקנותיו

עתה, משבררנו את הסוגיה של "משפחת הפונקציות החשיבות" נפנה לטיפול במשפט גדל. בטרם נציג את ניסוחו המדויק של המשפט, נפתח עוד את הכלים שהכרנו עד כה, ואשר ישמשו אותנו בהמשך.

2.1 קבוצות נל"ח ותכונותיהן הבסיסיות

2.1.1 טענה:

(1) הגדרה באינדוקציה שומרת על היות פונקציה חשיבה. כלומר: אם הפונקציות $G(\bar{x}),\ H(\bar{x},y,z)$ הן חשיבות, אזי הפונקציה $F(\bar{x},y)$ המוגדרת ע"י:

$F(\bar{x},0)=G(\bar{x});\ F(\bar{x},y+1)=H(\bar{x},y,F(\bar{x},y))$ היא חשיבה.

(2) שרשור סדרות הוא פונקציה חשיבה. כלומר, הפונקציה F הנתונה ע"י:

$F(x_1,\cdots,x_n)=\begin{cases} c(x_1,\cdots,x_n) & \text{לכל } i \text{ מתקיים } \vartheta(x_i) \\ 0 & \text{אחרת} \end{cases}$ באשר $c(x_1,\cdots,x_n)$ הצופן של הסדרה

שהיא שרשור הסדרות המוצפנות ע"י x_i וכמקודם $\vartheta(x)$ אסם x מצפין סדרה סופית.

(3) צמצום סדרות הוא פונקציה חשיבה: אם x מצפין סדרה סופית $\langle x_1,\ldots,x_n\rangle$

הצמצום $x|_{[y,z]}$ מוגדר ע"י $x|_{[y,z]}=\begin{cases} \langle x_y,x_{y+1},\ldots,x_z\rangle & 1\le y<z\le n \\ \text{הסדרה הריקה} & \text{אחרת:} \end{cases}$

הוכחה:

(1) תהי $x_0(\bar{x},y,z)$ התכונה "z מצפין סדרה באורך $y+1$", האיבר הראשון בה הוא $G(\bar{x})$ ולכל $i\le y$ אם האיבר ה-i הוא a אז האיבר ה-$i+1$ הוא $H(\bar{x},i,a)$". כמו בהוכחות קודמות קל להראות ש-x_0 חשיבה, ולכן גם הפונקציה $F'(\bar{x},y)=\mu_z[x_0(\bar{x},y,z)]$ היא חשיבה, ועתה $\bar{F}(\bar{x},y)=F_1(F'(\bar{x},y))$ ולכן סיימנו (הגדרת F_1 ראו בטענה 1.3.13).

(2) ו-(3) קל בעזרת מכונת מונים, תוך שימוש בכך שהפונקציה היא חשיבה אסם קיימת מכונת מונים המחשבת אותה. ■

כשם שהצפנו מסעים, אפשר גם להצפין מכונות. לשם הנוחות של הצפנה זו, נניח כי הא"ב מורכב ממספרים טבעיים זוגיים >2 והמצבים הפנימיים הם מספרים טבעיים אי זוגיים, ותמיד מצב ההתחלה יסומן ע"י 1. במקום הסימנים R,L בפקודות (= לך שמאלה, לך ימינה) נשים את המספרים 2,0. באופן זה, כל פקודה היא סדרה באורך 4 של מספרים טבעיים ונוכל להצפינה באופן חשיב ע"י מספר. עתה נרשום בסדר עולה את הצפנים של כל הפקודות, ואת הסדרה המתקבלת נצפין שוב ע"י מספר. כפי שכבר הערנו, קבוצת הפקודות קובעת את המכונה לחלוטין. ולכן בזאת הצפנו את המכונה ע"י מספר.

2.1.2 טענה: תהי $T_n(e,x_1,\ldots,x_n,\ell,y)$ התכונה "קיים מסע באורך l של מכונת טיורינג שמספרה e הפועלת על הנתונים $x_1,\ldots,x_n$ והתוצאה היא y". אזי T_n חשיבה.

יש לציין, שבניגוד לכך, נראה בהמשך שהתכונה "קיים מסע של מכונת טיורינג שמספרה e הפועלת על $x_1,...,x_n$ והתוצאה y" אינה חשיבה. כמו כן מעניינת הטענה הבאה:

2.1.3 משפט: יש מכונת טיורינג כוללת (אוניברסלית), כלומר: יש מכונת טיורינג T_u כך שלכל מכונת טיורינג T שמספרה e $f^2_{T_u}(e,x) = f^1_T(x)$. במלים אחרות, אם נותנים ל-T_u את המספר e של המכונה T המחשבת פונקציה מסויימת היא יכולה למצוא מהי תוצאת החישוב של T עבור כל קלט x. (לשם פשטות הסתפקנו בפונקציה חד מקומיות, אך הטענה נכונה עבור פונקציות n-מקומיות לכל n).

הוכחת הטענות 2.1.2 ו- 2.1.3 היא מייגעת, אך אין בה כל קושי עקרוני. ניתן כאן רק סקירה של ההוכחה: עבור טענה 2.1.2 מראים כי T_n חשיבה בשיטה דומה למה שכבר עשינו פעמיים רבות: T_n שקול לכך ש-e מצפין סדרה סופית שכל איבריה מצפינים רביעיות, ורביעיות אלו בנויות כפקודות לא סותרות של מכונה, וקיימת סדרה באורך l של מצבים של מכונה זו שבה המצב הראשון הוא התחלתי לחישוב עבור $x_1,...,x_n$; כל מצב אחריו הוא עוקב לו; והמצב הסופי הוא y אחדות רצופות. עבור טענה 2.1.3 מתארים מכונת טיורינג, אשר משחזרת מתוך e את הסדרה שהוא מצפין, וממנה את פקודות המכונה T, ואז פועלת בהתאם למה ש- T הייתה עושה ל-x.

2.1.4 משפט: תהי A קבוצה לא ריקה של מספרים טבעיים. הטענות הבאות שקולות:

(1) יש פונקציה שלמה חשיבה f כך ש-$A = Rang(f)$.

(2) יש פונקציה חלקית חשיבה f כך ש- $A = Rang(f)$.

(3) יש פונקציה חלקית חשיבה f כך ש- $A = Dom(f)$.

(4) יש יחס חשיב $\varphi(x,\bar{y})$ כך ש-$A = \{x : \exists y \varphi(x,y)\}$.

(5) יש יחס חשיב $\varphi(x,\bar{y})$ כך ש-$A = \{x : \exists \bar{y} \varphi(x,y)\}$.

הערה: אם A ריקה קל לראות שהיא מספקת את 2 עד 5 אך לא את 1. ואמנם בהוכחת המשפט, המקום היחידי שבו נסתמך על כך ש-$A \neq \phi$ יהיה בהוכחה ש-$1 \Leftarrow 5$.

2.1.5 הגדרה: קבוצה $A \subseteq N$ נקראת **ניתנת למניה חשיבה** (נל"ח), אם $A \neq \phi$ או ש-A מקיימת את הטענות (השקולות) של משפט 2.1.4.

לפני שנוכיח את המשפט, כדאי להתעכב על המשמעות האינטואיטיבית של נל"ח. אנו יודעים שקבוצה חשיבה A היא קבוצה, עבורה קיימת מכונת טיורינג שלכל x מחשבת אם $x \in A$ או לא. לעומת זאת, קבוצה B היא נל"ח אם היא קבוצה, שקיימת מכונת טיורינג הפולטת את איבריה של B בזה אחר זה (שהרי: לפי 1 במשפט 2.1.4, יש f שלמה רקורסיבית שהטווח שלה B; ובעזרת מכונה T המחשבת את f אפשר לחשב את $b(0), b(1),...$ ואלה הם כל איברי B). זאת דרישה חלשה יותר מחשוביות: כל קבוצת חשיבה היא בהכרח נל"ח: לפי חלק 4 של משפט 2.1.4 אפשר לקחת עבור $\varphi(x,y)$ המבוקש את היחס $x \in A$. אולם יש קבוצות נל"ח שאינן חשיבות.

במילים אחרות, הקבוצות הנל"ח הן הקבוצות עבורן יש עדות סופית לשייכות, אך לאי שייכות לאו דווקא.

<u>הוכחת משפט 2.1.4</u>: ראשית נוכיח כי $3 \Leftrightarrow 4 \Leftrightarrow 5$.

$5 \Leftarrow 3$: נניח $A = Dom(f)$, f חלקית וחשיבה. יהי e המספר של מכונת טיורינג T המחשבת את f נגדיר $\varphi(x,\ell,y) = T_1(e,x,\ell,y)$ לפי טענה 2.1.2 φ יחס חשיב. ועתה:

$A = Dom(f) = \{x : \exists y[f(x) = y]\} = \{x : \exists \ell \exists y[T_1(e,x,\ell,y)]\} = \{x : \exists \ell \exists y(\varphi(x,\ell,y)\}$.

$4 \Leftarrow 5$: נניח $A = \{x : \exists y_1,...,y_n[\varphi(x,y_1,...,y_n)]\}$, φ חשיב. נגדיר:

$\varphi'(x,y) = \varphi(x,\beta(y,1),...,\beta(y,n))$. φ' יחס חשיב כי φ ו- β פונקציות חשיבות. לפי תכונות β, לכל $\langle y_1,...,y_n\rangle$ יש y כך ש- $\langle y_1,...,y_n\rangle = \langle \beta(y,1),...,\beta(y,n)\rangle$ ולכן $A = \{x : \exists y[\varphi(x,y)]\}$.

$3 \Leftarrow 4$: נניח $A = \{x : \exists y[\varphi(x,y)]\}$, φ חשיב. יהי e מספרה של מכונת טיורינג T המחשבת את χ_φ (הפונקציה האופיינית של φ).

נגדיר: $f(x) = \mu_y T_2(e,x,\beta(y,1),\beta(y,2),1)$. עתה, f חשיבה כי T_2 חשיבה (לפי טענה 2.1.2) וכך גם הפונקציה β. עתה:

$$A = \{x : \exists y \varphi(x,y)\} = \{x : \exists y[\chi_\varphi(x,y) = 1] =$$
$$= \{x : (\exists x,y)[T_2(e,x,\beta(y,1),\beta(y,2),1]\} = \{x : \exists z[z = f(x)\} = Dom(f)$$

הוכחנו איפה כי $(3) \Leftrightarrow (4) \Leftrightarrow (5)$. נוכיח עתה כי $(1) \Leftrightarrow (2) \Leftrightarrow (5)$, ובזאת נסיים.

$2 \Leftarrow 1$: מיידי, שהרי כל פונקציה שלמה היא גם פונקציה חלקית.

$5 \Leftarrow 2$: נניח $A = Rang(f)$, f חלקית חשיבה. יהי e מספרה של המכונה המחשבת את f. היחס $\varphi(x,\ell,y) = T_1(e,y,\ell,x)$ הוא חשיב לפי 2.1.2 והוא היחס המבוקש.

$1 \Leftarrow 5$: מאחר שהוכחנו $5 \Leftarrow 4$, נוכל להניח כי $A = \{x : \exists y[\varphi(x,y)]\}$, φ חשיב. נניח כי χ_φ מחושבת ע"י מכונה שמספרה e. ומאחר ש- $A \neq \phi$, נוכל לבחור $a_0 \in A$ ולהגדיר:

$$f(v) = \begin{cases} \beta(v,1) & \text{אם } T_2(e,\beta(v,1),\beta(v,2),(\beta,3),1) \\ a_0 & \text{אחרת} \end{cases}.$$

f פונקציה שלמה, ולפי הטענה על הגדרה לפי מקרים, (1.2.10), היא גם חשיבה.

נראה עתה כי $A = Rang(f)$:

ראשית נוכיח ש- $A \subseteq Rang(f)$

$$x \in A \Rightarrow \exists y[\varphi(x,y)] \Rightarrow$$
$$\Rightarrow \exists y[\chi_\varphi(x,y) = 1] \Rightarrow \exists \ell, y[T_2(e,x,y,\ell,1)] \Rightarrow$$
$$\Rightarrow \exists v[\beta(v,1) = x] \wedge T_2(e,\beta(v,1),\beta(v,2),\beta(v,3),1] \Rightarrow$$
$$\Rightarrow \exists v[f(v) = x] \Rightarrow x \in Rang(f)$$

והכלה הפוכה: נניח $x \in Rang(f)$. כלומר יש v כך ש- $f(v) = x$. ועתה, אם

$T_2(e,\beta(v,1),\beta(v,2),\beta(v,3),1)$ אז לפי הגדרת f , $f(v)=\beta(v,1)$ וע"י הפיכת הגרירות למעלה נסיק: $x\in A$.

אחרת, $x=f(v)=a_0\in A$. ובכל מקרה: $x\in A$ וסיימנו. ■

לשם פשטות הוגדר המושג נל"ח רק עבור קבוצות של טבעיים, אך ניתן להרחיב את ההגדרה ליחסים על הטבעיים: יחס $A\subseteq N^k$ יקרא נל"ח אם הקבוצה של כל המספרים המצפינים את איברי A היא נל"ח. בהמשך נדון במושג נל"ח גם עבור יחסים k-מקומיים. לשם כך יש לוודא שלא נוצרה סתירה בהגדרת מושג זה עבור יחסים חד מקומיים. כלומר, יש להוכיח, כי $A\subseteq N$ היא נל"ח אסם הקבוצה של המספרים המצפינים את איבריה, היא נל"ח. זוהי מסקנה מיידית של המשפט הבא:

<u>2.1.6 טענה</u>: יהי $A\subseteq N^k$ יחס על הטבעיים. הטענות הבאות שקולות:

(1) A יחס נל"ח (קבוצת הצפנים של איברי A היא נל"ח).

(2) יש יחס חשיב $\varphi(\bar{x},y)$ כך ש-$A=\{\bar{x}:\exists y\varphi(\bar{x},y)\}$.

(3) יש יחס חשיב $\varphi(\bar{x},\bar{y})$ כך ש- $A=\{\bar{x}:\exists\bar{y}\varphi(\bar{x},\bar{y})\}$.

<u>הוכחה</u>:

$2\Leftarrow 1$ הצופן של סדרה $\bar{x}\in N^k$ יסומן ע"י $seq_k(x)$. אם B היא קבוצה הצפנים של איברי A אז יש יחס חשיב $\psi(x,y)$ כך ש-$B=\{x:\exists y\psi(x,y)\}$. נסמן $\varphi(\bar{x},y)=\psi(seq_k(x),y)$. φ חשיב בגלל שהפונקציה seq_k חשיבה ואילו $A=\{\bar{x}:seq_k(\bar{x})\in B\}=\{\bar{x}:\exists y\varphi(\bar{x},y)\}$.

$3\Leftarrow 2$ מיידי.

$1\Leftarrow 3$ תהי $\vartheta_k(x)$ התכונה "x מצפין סדרה סופית באורך k", ותהי $\alpha(x)$ הסדרה ש-x מצפין. התכונה $\psi(x,\bar{y})=[\vartheta_k(x)\wedge\varphi(\alpha(x),\bar{y})]$ היא חשיבה כי התכונה ϑ והפונקציה α הן חשיבות, ואילו B, קבוצת הצפנים של אברי A מקיימת:

$B=\{x:\vartheta_k(x)\wedge\alpha(x)\in A\}=\{x:\vartheta_k(x)\wedge\exists\bar{y}\varphi(\alpha(x),\bar{y})\}=\{x:\exists\bar{y}\psi(x,\bar{y})\}]$ לכן B קבוצה נל"ח, כלומר A יחס נל"ח. ■

נראה עתה עוד מספר תכונות יסודיות של יחסים נל"ח.

<u>2.1.7 משפט</u>:

(1) משפחת היחסים שהם נל"ח סגורה תחת כמת ישי. כלומר, אם $\varphi(\bar{x},\bar{y})$ יחס נל"ח, אז גם $\exists\bar{y}\varphi(\bar{x},\bar{y})$ יחס נל"ח.

(2) משפחת היחסים הנל"ח סגורה תחת הוספת כמת כולל חסום כלומר: אם $\varphi(\bar{x},y,y_0)$ יחס נל"ח, אז גם $(\forall y<y_0)\varphi(\bar{x},y,y_0)$ יחס נל"ח.

(3) משפחת היחסים שהם נל"ח סגורה תחת הטלה, הוספת אינדקסי סרק והחלפת הסדר. כלומר: אם $A\subseteq N^k$ יחס נל"ח, אז גם היחס $B=\{\langle a_1,\dots,a_n\rangle:\langle a_{\ell_1}\dots a_{\ell_r}\rangle\in A\}$ הוא נל"ח.

(4) אם היחסים $\varphi(x)$ ו- $\neg\varphi(x)$ הם נל"ח, אזי הם גם חשיבים.

(5) משפחת היחסים הנל"ח סגורה תחת איחוד וחיתוך אך לא תחת השלמה).

<u>הוכחה</u>: בהוכחת כל הסעיפים נשתמש בטענה הקודמת (2.1.5) בכך שבמקום להשתמש בהגדרה של יחס נל"ח (עפ"י הצפנות), נשתמש בהגדרה השקולה של קיום תכונות 2,3 במשפט הנ"ל.

(1) יש להראות כי $\psi(\bar{x}) = \exists\bar{y}\varphi(\bar{x},\bar{y})$ הוא נל"ח. לפי הנל"חיות של $\varphi(\bar{x},\bar{y})$ יש יחס חשיב $\chi(\bar{x},\bar{y},z)$ כך ש- $\varphi(\bar{x},\bar{y}) \equiv \exists z(\bar{x},\bar{y},z)$ ולכן, $\psi(\bar{x}) \equiv \exists\bar{y}\exists z\chi(\bar{x},\bar{y},z)$ מה שמוכיח את נל"חיות ψ.

(2) יש להראות כי $(\forall y < y_0)\varphi(\bar{x},y,y_0)$ הוא נל"ח. לפי נל"חיות $\varphi(\bar{x},y,y_0)$ יש $\chi(\bar{x},y,y_0,z)$ חשיב כך ש- $\varphi(x,y,y_0) \equiv \exists z(\chi(\bar{x},y,y_0,z)$. ועתה:

$$\psi = (\forall y < y_0)(\exists z)(\chi(x,y,y_0,z)) \equiv (\exists z)[\vartheta(z) \wedge (z_0 = y_0) \wedge$$
$$\wedge (\forall i < y_0)(i \neq 0 \to \chi(x,i,y_0,z_i)]$$

לכן לפי 1 ψ נל"ח.

(3) אם $A \subseteq N^k$ נל"ח, יש $\varphi(x_1,...,x_k,y)$ חשיב כך ש- $A = \{\bar{x} \in N^k : \exists y\varphi(\bar{x},y)\}$ נגדיר יחס $n+1$ מקומי ψ ע"י $\psi(a_1,...,a_n,y) = \varphi(a_{\ell_1},...,a_{\ell_r},y)$ ψ חשיב. ועתה:

$$B = \{\langle a_1,\ldots,a_n\rangle : \langle a_{\ell_1},...,a_{\ell_r}\rangle \in A\} = \{\langle a_1,\ldots,a_n\rangle : \exists y\varphi(a_{\ell_1},...,a_{\ell_r},y)\} =$$
$$= \{\langle a_1,\ldots,a_n\rangle : \exists y\psi(a_1,\ldots,a_n,y)\}$$

ולכן B נל"ח.

(4) לשם פשטות נניח כי $\varphi(x)$ חד מקומי (ההרחבה ל- $\varphi(x)$ כלשהו היא קלה). יהיו f,g חשיבות שלמות כך ש- $\varphi(x) \equiv x \in Rang(f), \neg\varphi(x) \equiv x \in Rang(g)$. משקילויות אלו נובע מיידית כי $Rang(f) \cup Rang(g) = N$. לכן הפונקציה $h(x) = \mu_y[f(y) = x \vee g(y) = x]$ היא שלמה.

כמו כן היא חשיבה כי f חשיבה וקל לראות כי $\neg\varphi(x) \equiv [g(h(x)) = x]$ ו- $\varphi(x) \equiv [g(h(x)) = x]$ לכן φ ו- $\neg\varphi$ חשיבים.

(5) יהיו $A,B \subseteq N^k$ יחסים נל"ח, יהיו f_1,g_1 פונקציות שלמות חשיבות שטווחן A,B בהתאמה. (ליתר דיוק, טווחן הקבוצות המצפינות את A,B). תהי $k_1(n) = \begin{cases} f_1(n) & x = 2n+1 \\ g_1(n) & x = 2n \end{cases}$.

k_1 חשיבה (הגדרה לפי מקרים), טווחה הוא $A \cup B$ ולכן זו קבוצה נל"ח.

עתה, יהיו f_2,g_2 פונקציות חלקיות חשיבות שתחומן A,B בהתאמה. נגדיר פונקציה חלקית k_2: תחומה יהיה $A \cap B$, ולכל $x \in A \cap B$, $k_2(x) = f_2(x) + g_2(x)$ אזי k_2 חשיבה, ולכן $A \cap B$ נל"ח. ■

נסיים סעיף זה בדוגמה ראשונה של קבוצה נל"ח שאינה חשיבה.

2.1.8 משפט (אי כריעות בעיית העצירה): לכל $e \in N$, אם e מצפין מכונת טיורינג, נסמן ב- $T_e(n)$ את הפעלת המכונה ש- e מצפין על הקלט n, אזי הקבוצה $\{\langle e,n\rangle : T_e(n) \text{ עוצרת}\}$ נל"ח אך לא חשיבה.

הוכחה: נגדיר פונקציה חשיבה $f_{e*}(e,x)$ באופן הבא (ראו גם משפט 2.1.3):

$$f_{e*}(e,x) = \begin{cases} T_e(x) & \text{אם } e \text{ מספר גדל של מכונת טיורינג} \\ 0 & \text{אחרת} \end{cases}.$$

עתה, נגדיר פונקציה $g(x)$ ע"י:

$$g(x) = \begin{cases} T_x(x)+1 & x \text{ מספר גדל של מכונת טיורינג שעוצרת על קלט } x \\ 0 & \text{אחרת} \end{cases}$$

יוצא שאם בעיית העצירה כריעה אז g שלמה וחשיבה (לפי הטענה עלההגדרה לפי מקרים, כי מהנחתנו התנאי הראשון בהגדרת $g(x)$ חשיב) לכן יש מכונת טיורינג T_{e_1} המחשבת את g , ז"א שלכל x $T_{e_1}(x)$ מוגדר ומתקיים $g(x) = T_{e_1}(x)$. מהגדרת $g(x)$ נקבל $g(e_1) = T_{e_1}(e_1)+1$, אבל מצד שני מבחירת T_{e_1} נקבל $T_{e_1}(e_1) = g(e_1)$ בסתירה. מכאן שבעיית העצירה אינה כריעה.

מאידך היחס "e מספר גדל של מכונת טיורינג" חשיב ולכן הקבוצה $\{\langle e,n\rangle : T_e(n) \text{ עוצרת}\}$ נל"ח, כי יש נוסחה מהצורה $\exists z\varphi(e,n,z)$ המגדירה אותה.

(הנוסחה φ תגיד שהמכונה T_e עצרה על הקלט n אחרי פחות מ-z צעדים). ■

תרגילים - קבוצות נל"ח ותכונותיהן

1. תהי A קבוצה נל"ח אינסופית הוכיחו שקיימת $B \subseteq A$ אינסופית וחשיבה.
2. ניתן עוד דוגמאות לקבוצות נל"ח שאינן חשיבות:

   א. תהי $U_1(x,y)$ חשיבה כוללת. הוכיחו כי הפונקציה

   $$g(y) = \begin{cases} U_1(e,x) & y = \lceil (e,x) \rceil \\ \text{לא מוגדר} & \text{אחרת} \end{cases}$$

   היא חשיבה, באשר $\lceil (e,x) \rceil$ הוא מספר גדל של הזוג (e,x).

   ב. לכל e נסמן $W_e \overset{d}{=} \{x : U_1(e,x) \text{ מוגדר}\}$. תהי Y נל"ח. הראו ש- $Y = W_e$ לאיזה e מתאים.

   ג. נגדיר $U = dom(g)$. הראו ש- U נל"ח כוללת, כלומר:

   i) U נל"ח.

   ii) לכל Y נל"ח יש f חשיבה מלאה עבורה לכל n טבעי $n \in Y \Leftrightarrow f(n) \in U$.

   ד. נגדיר $K \overset{d}{=} \{e : e \notin W_e\}$. הראו ש-$K$ אינה נל"ח, אבל $\overline{K} = N \setminus K$ נל"ח. הסיקו ש- $\overline{K}$ אינה חשיבה.

   ה. הוכיחו שם X נל"ח כוללת אז X אינה חשיבה.

3. תהי $L = \langle +,\cdot,< \rangle$.

א. לכל נוסחה $\varphi(x)$ נסמן $\varphi^N \overset{d}{=} \{n \in N : N \models \varphi(n)\}$. הוכיחו שאם כל הכמתים ב- φ חסומים אז φ^N חשיבה. נוסחה המקיימת תנאי זה תקרא נוסחת $\sum_0$.

ב. נוסחה $\varphi \in L$ תקרא נוסחת $\sum_1$ אם היא שקולה לנוסחה מהצורה $(\exists x)\psi(x,y)$, באשר $\psi(x,y) \in \sum_0$. הראו שאם $\varphi \in \sum_1$ אז φ^N נל"ח. הסיקו שמשפחת הנוסחאות $\sum_1$ סגורה תחת הוספת כמתים חסומים. כלומר,

$\varphi(x,y) \in \sum_1 \Rightarrow (\forall x < n)\varphi(x,y) \in \sum_1$ (וכך גם לכמת ישי חסום, כמובן).

ג. באופן דומה נאמר שנוסחה היא $\prod_1$ אם היא שקולה לנוסחה מהצורה $(\forall x)\varphi(x,y)$ לאיזו φ ב- $\sum_0$. הוכיחו שקבוצה $A \subseteq N$ היא קו-נל"ח (כלומר משלימתה היא נל"ח) אסם היא גדירה ע"י נוסחת $\prod_1$, כלומר, $A = \varphi^N$ לאיזו נוסחת $\varphi \in \prod_1$.

ד. הסיקו שקבוצה $A \subseteq N$ חשיבה אסם היא גדירה ב-L הן ע"י נוסחת $\sum_1$ הן ע"י נוסחת $\prod_1$.

4. בסימונים של השאלה הקודמת נגדיר $Th_{\Pi_1}(\boldsymbol{N}) \overset{d}{=} \{\varphi \in L : \varphi \in \prod_1, \boldsymbol{N} \models \varphi\}$.

5. תהי $A \subseteq N$ גדירה ע"י נוסחת $\prod_1$. הראו שלו הייתה הקבוצה $\{n : n = \ulcorner\varphi\urcorner, \varphi \in Th_{\Pi_1}(N)\}$ נל"ח אז גם A הייתה נל"ח. הערה: אמנם, עד כה לא דנו בהצפנת פסוקים, כפי שזו מופיעה לעיל, אולם לאחר שהצפנו מכונות אין בכך כל קושי. לטיפול כללי יותר ופורמלי לגמרי בנושא ראו בפרק הבא.

6. הסיקו כי $\{n : n = \ulcorner\varphi\urcorner, \varphi \in Th_{\Pi_1}(N)\}$ אינה נל"ח.

7. *הסיקו של-$Th(N)$ (=אוסף הפסוקים ב-L שאמיתים ב-N) אין מערכת אקסיומות חשיבה.

2.2 בעיית ההכרעה ומשפט גדל

הבעיה שבה נטפל, בניסוחו המקורי של הילברט, היא האם יש שיטה מכנית לבדיקה אם משפט מתמטי כלשהו נכון או לא. בחלקה הראשון של החוברת הסברנו מדוע המושג של "שיטה מכנית" אינו מדוייק דיו מבחינה מתמטית והצענו מספר הגדרות (שקולות) שבהן נוכל לטפל. כעת אפשר לטעון כי גם נכונות אינה דרישה מתאימה מאחר והיא מאד תלויה בנימוקים סוביקטיביים ומתוך כך מתקרבת יותר לתחום של "דעה ואמונה" שאיננו תחום התעניינותנו (בלוגיקה).

בחכמה שלאחר מעשה אנו יודעים שהאכסיומות של תורת הקבוצות, שמכסות את כל מתמטיקה, אינן מכריעות כל משפט לחיוב או לשלילה. לכן סביר להחליף המושג של "נכונות" במושג של יכיחות.

בניסוח זה התשובה לשאלתנו היא שלילית - אין תמיד שיטות הכרעה שמאפשרות לנו לדעת אם פסוק כלשהו יכיח או לא. יתר על כן, לגבי נכונות התוצאות השליליות חזקות אף יותר. הניסוח המדוייק של הבעיה הוא: בהנתן התורה T בשפה L, האם קיימת מכונת טיורינג שעבור קלט ψ שהוא סדרת סימנים ב-L למכונה יש חישוב מסתיים (המתחיל בקלט זה) שבסופו היא מודיעה לנו אם המלה בקלט היא פסוק יכיח מ-T או לא. כאמור, התשובה לשאלה זו שלילית. בתרגילים נוכיח תוצאה חזקה אף יותר: אין חישוב שיפריד בין הפסוקים שאפשר להוכיחם לבין פסוקים שאפשר לסותרם (=להוכיח את שלילתם).

נפתח עתה ניסוח שקול לבעיה, אשר בו יהיה לנו נוח יותר לטפל:

תהי T תורה בשפה סופית L, נגדיר מספור גדל g שהוא פונקציה המתאימה לכל נוסחה ולכל שם עצם בשפה מספר טבעי. (אפשר פשוט לראות בשם עצם ובנוסחה סדרות של אותיות מאלף בית סופי). באופן מדויק יותר:

<u>2.2.1 הגדרה</u>: g היא **פונקצית השם התקנית** לשפה L (או פונקצית גדל ל-L) אם:

$R_1, R_2, \ldots$ סימני היחס ו- $F_1, F_2, \ldots$ סימני הפונקציה של L (אם בשפה יש שוויון נחליט כי R_1 הוא השוויון).

יהיו $p_0, p_1, \ldots, p_n \ldots$ המספרים הראשוניים ($p_0 = 2$, $p_1 = 3$ וכו').

נגדיר:

$$g(X_i) = 2^i$$

$$g(F_j(t_1, \ldots t_n)) = 2^5 \cdot 3^{5^j} \cdot 5^{g(t_1)} \ldots p_{n+1}^{g(t_n)}$$

$$g(R_i(t_1, \ldots t_n)) = 2^4 \cdot 3^{3^i} \cdot 5^{g(t_1)} \ldots p_{n+1}^{g(t_n)}$$

$$g[(\exists x_i)\varphi] = 2^1 \cdot 3^{2^i} \cdot 5^{g(\varphi)}$$

$$g(\varphi \to \psi) = 2^2 \cdot 5^{g(\varphi)} \cdot 7^{g(\psi)}$$

$$g(\neg \psi) = 2^3 \cdot 5^{g(\psi)}$$

הסבר:

(1) חזקת 2 מסבירה באיזה סוג נוסחה אנו מטפלים, למשל 2^4 מתאים לנוסחה מהצורה $R_i(t_1,...,t_n)$; 2^3 לנוסחה מהצורה $\neg\psi$ וכו'.

(2) חזקות 3 נועדו לטפל בנוסחאות שאינן נוצרות ישירות ע"י קשר לוגי. למשל לנוסחה מהצורה $\exists x_i$ תתאים החזקה 3^{2^i} (האומרת שהכימות הוא על המשתנה האישי המקודד ע"י 2^i, כלומר x_i - זכרו שחזקת 2^i כבר אומרת לנו שאנו מקודדים נוסחה המתחילה בכמת ישי).

(3) עתה, אם הנוסחה נוצרה מיידית ע"י קשר לוגי או ע"י כמת ישי חזקות 5 (ו- 7) נועדו להצפנת הנוסחה (או נוסחאות) שברמה הקודמת בבנית הנוסחה. אם הנוסחה הייתה מהצורה $R_i(t_1,...,t_n)$ או $F_i(t_1,...,t_n)$ ישמשו החזקות של הראשוניים הבאים לקידוד שמות העצם $t_1,...,t_n$.

<u>דוגמה</u>:

את $x_1 = F_1(x_2)$ (*) נציג ע"י: $2^4 \cdot 3^3 \cdot 5^{g(x_1)} \cdot 7^{g(F_1(x_2))}$ (כזכור את הנוסחה הזו יש לרשום כ- $(R_1(x_1, F_1(x_2))$.

באשר: $g(F_1(x_2)) = 2^5 \cdot 3^{5^1} \cdot 5^{2^2}$.

ולכן מספר גדל של (*) הוא $2^4 \cdot 3^{3^1} \cdot 5^{2^1} \cdot 7^{2^5 \cdot 3^{5^1} \cdot 5^{2^2}}$.

נותיר זאת כתרגיל קל לקורא להוכיח:

<u>2.2.2 טענה</u>:

(1) הצפנת גדל היא חד-חד ערכית וחשיבה.

(2) הפונקציה הבאה חשיבה: $f(n)$ היא 0 אם $n \notin Rang(g)$, 1 אם φ אטומית וכו'.

(3) f פונקציה מלאה.

רמז: השתמשו בטענה 2.1.1 סעיף 1.

<u>2.2.3 הגדרה</u>: תהי T תורה בשפה סופית בשפה L, נאמר כי **T כריעה** אם הקבוצה:

$A = \{g(\varphi) : T \vdash \varphi$ ו- φ פסוק ב- $L\}$ חשיבה.

<u>הערות</u>:

(1) למעשה יש לדבר על הזוג $\langle T, L \rangle$ כי הרחבת L מגדילה את קבוצת הפסוקים היכיחים מ-T ולכן יכולה לקלקל את כריעות T).

(2) כיוון שציינו כבר ש- g פונקציה חח"ע וחשיבה, היות A חשיבה תבטיח לנו בדיוק, שבהנתן פסוק φ נוכל לחשב בזמן סופי את $g(\varphi)$ ולהכריע אם $g(\varphi) \in A$, כלומר האם $T \vdash \varphi$.

קיבלנו, איפה, שבהנתן תורה T בשפה סופית L, השאלה האם T כריעה שקולה לשאלתו של הילברט בניסוח שהוצג בתחילת סעיף זה.

השאלות הבאות הן טבעיות:

(1) האם התורה הריקה ($T = \phi$) בשפה סופית המכילה סימן יחס דו מקומי כריעה.

תהי T קבוצת כל הפסוקים הנכונים ב- $\langle \omega, 0, S, + \rangle$ כאשר S פונקצית העוקב, האם T כריעה.

(3) אם P תורת פיאנו (ראו להלן), האם P כריעה.

בהמשך נראה שהתשובה לשלושת השאלות היא שלילית.

תורת פיאנו P היא קבוצת הפסוקים הבאה $L\{0,+,\cdot,S\}$:

(1) $\forall x(Sx \neq 0)$

(2) $\forall x \forall y(Sx = Sy \to x = y)$

(3) $\forall x(x + 0 = x)$

(4) $\forall x \forall y(x + Sy = S(x + y)$

(5) $\forall x(x \cdot 0 = 0)$

(6) $\forall x \forall y(x \cdot Sy = x \cdot y + x)$

(7) סכימה של אכסיומת האינדוקציה: $\forall x[\varphi(\bar{x},0) \wedge \forall y(\varphi(x,y) \to \varphi(\bar{x},Sy) \to \forall y \varphi(\bar{x},y)]$.

הסבר: (1) אומר ש- 0 אינו עוקב; (2) אומר שפעולת העוקב חח"ע; (3) ו- (4) מגדירים את החיבור; (5) ו-(6) הגדרת הכפל; (7) סכימת האינדוקציה עבור $\varphi(\bar{x},y)$ (כאשר $\bar{x} = (x_1,\ldots,x_n)$).

(נשים לב ש-P קבוצת פסוקים אינסופית).

<u>2.2.4 הגדרה</u>: תהי T תורה בשפה L . נסמן ב- $F(L)$ את קבוצת הנוסחות בשפה L , ונניח שנתונה פונקצית "השם של φ", : שנסמנה $'\varphi'$ כך ש: {שמות העצם הקבועים של $F(L) \to L$ } : ' ' .

תהי : $f : F(L) \to F(L)$ פונקציה חלקית.

(1) נאמר ש- f **מיוצגת** ע"י הנוסחה $\varphi(x,y)$ ב-T , אם לכל נוסחה ψ בתחום של f מתקיים:

$T \vdash \forall y(\varphi('\psi',y) \leftrightarrow y = 'f(\psi)')$. כלומר, אם c הוא השם של ψ אז $\varphi(c,y)$ אומר ש- y הוא השם של $f(\psi)$ ו- φ נוסחה "שמקשרת" בין השם של ψ לשם של $f(\psi)$.

(2) ל- $A \subseteq F(L)$ נאמר ש-A **מיוצג** ע"י $\varphi(x)$ ב-T אם לכל $\psi \in F(L)$ מתקיים:

$T \vdash \varphi('\psi')$ אם $\psi \in A$.

$T \vdash \neg\varphi('\psi')$ אם $\psi \notin A$.

<u>הערה</u>:

(1) נשים לב כי ב-(1) לא נדרש מאום לגבי נוסחה שאינה בתחום f .

(2) תהי $L = \langle 0,+,S,\cdot \rangle$. כל פונקציה חשיבה $f : N \to N$ מגדירה באופן טבעי פונקציה מקבוצת שמות העצם הקבועים של L אל עצמה. משום כך יש משמעות לשאלה האם תורה T בשפה L מייצגת פונקציה חשיבה.

<u>2.2.5 הגדרה</u>: תהי L שפה ו –' ' פונקציה כנ"ל. נגדיר פונקציה חלקית D מ- $F(L)$ אל $F(L)$, **פונקצית האלכסון** כדלקמן:

{ב- φ לכל היותר משנה חופשי יחיד x_0 : $dom(D)=\{\varphi\in F(L)$ (שימו לב שיתכן $\varphi\in dom(D)$ ו- φ ללא משתנים חופשיים). עתה נגדיר $D(\varphi(x_0))=\varphi('\varphi')$ כלומר הפונקציה D פועלת על פסוקים או נוסחאות בעלות המשתנה x_0 בלבד, ופעולתה היא החלפת x_0 (כשהוא מופיע) בשם של φ.

2.2.6 משפט האמת של *Tarski*:

תהי T תורה עקבית (ז"א חסרה סתירה) בשפה L ו- $'\ '$ פונקצית שם. נניח כי פונקצית האלכסון ניתנת לייצוג ע"י נוסחה ב-T אזי:

(1) הקבוצה $A=\{\varphi : T\vdash\varphi$ - φ פסוק ב- L } איננה יציגה.

(2) לכל נוסחה $\varphi(x)$ קיים פסוק ψ כך ש: $T\vdash\varphi('\psi')\leftrightarrow\neg\psi$.

הוכחה:

נראה ראשית כי (2) $\Leftarrow$ (1). נניח כי $\varphi(x)$ מייצגת את A, ויהי ψ פסוק כמובטח ב-(2). נתון כי $T\vdash\varphi('\psi')\leftrightarrow\neg\psi$ לכן אם $\psi\in A$, אז מהגדרת A $T\vdash\psi$ ויחד עם הידוע מבחירת ψ יוצא $T\vdash\psi\rightarrow\neg\varphi('\psi')$. לכן $T\vdash\neg\varphi('\psi')$. כיוון ש-$T$ עקבית T לא מוכיחה את $\varphi('\psi')$ וזאת סתירה להנחה ש- ψ מייצגת את A.

לעומת זאת אם $\psi\notin A$, כלומר T לא מוכיחה את ψ, אזי $T\vdash\neg\varphi('\psi')$. כיוון שבנוסף $T\vdash\neg\varphi('\psi')\rightarrow\psi$ נקבל ש- $T\vdash\psi$ בסתירה.

עתה נוכיח את (2): תהי $\delta(u,v)$ מייצגת את פונקצית האלכסון. נרשום

$$(i)\ \ \chi(x_0)=\neg\forall y(\delta(x_0,y)\rightarrow\varphi(y))$$

$$(ii)\ \ \psi=D(\chi)=\neg\forall y(\delta('\chi',y)\rightarrow\varphi(y))$$

למשל, במקרה הפשוט שבו D מיוצג ע"י שם עצם τ פירוש נוסחה (i) הוא $\neg\varphi(\varphi(x_0))$ וביחס ל- (2) פירוש ψ הוא $\neg\varphi(\tau(\chi))$. כלומר, ψ אומר: שלילת φ של השם של ψ.

הערה: בפועל אין יצוג ע"י שמות עצם, ודוגמה זו לא נועדה אלא להבהרת ההגדרה.

נראה כי: $T\cup\{\psi\}\vdash\neg\varphi('\psi')$.

ואמנם: $T\cup\{\psi\}\vdash\exists y(\delta('\chi',y)\wedge\neg\varphi(y))$, שכן הפסוק שמימין שקול ל- ψ. נסמנו α.

מכיוון ש- δ מייצגת את D, $T\vdash(\forall y)[\delta('\chi',y)\leftrightarrow y='D(\chi)']$. נסמן את הפסוק מימין ב- β.

מ- α נובע שקיים y כך ש- $\delta('\chi',y)$ וכן $\neg\varphi(y)$. מ- β נקבל שזה גורר $y='D(\chi)'$, ולכן $\alpha,\beta\vdash\neg\varphi('D(\chi)')$, ומהגדרת ψ נקבל $\neg\varphi('\psi')$ יכיח. עתה, ממשפט השלמות נקבל ש- $\neg\varphi('\psi')$ יכיח מ- α,β גורר ש- $T\cup\psi\vdash\neg\varphi('\psi')$.

נראה עתה שגם $T\cup\{\neg\psi\}\vdash\varphi('\psi')$, ובכך נשלים את ההוכחה.

עלינו להראות: $T\cup\{\forall y(\delta('\chi',y)\rightarrow\varphi(y))\}\vdash\varphi('\psi')$ ואמנם: $T\vdash\delta('\chi','D(\chi)')$ כי δ

מייצגת את פונקצית האלכסון ולכן $T \cup \{\neg\psi\} \vdash \delta('\chi','D(\chi)') \to \varphi('D(\chi)')$ ומכיוון ש- $\psi = 'D(\chi)'$ נקבל בעזרת כלל הניתוק ש- $T \cup \{\neg\psi\} \vdash \varphi('\psi')$. ■

הערה: חלק (2) של המשפט נקרא גם **משפט נקודת השבת**, והוכח לראשונה ע"י גדל.

<u>סימון</u>: תהי L שפה סופית המכילה את $\cdot,+,S,0$.

נגדיר את הפונקציה "_" באופן הבא: $\_ : \omega \to \{$ קבוצת שמות העצם הקבועים ב- $L \}$ נתונה ע"י $\underline{n} = \underbrace{SS...S}_{n\text{ פעמים}}0$.

<u>2.2.7 משפט</u>: כל פונקציה חשיבה ניתנת לייצוג בתורת פאנו, כל קבוצת חשיבה ניתנת לייצוג בתורת פאנו (הפונקציה "_", שהוגדרה לעיל, תמלא את תפקיד פונקצית השם, שהופיעה בהגדרת היצוג). יתר על כן אפשר להסתפק בתורה N סופית החלקית לתורת פיאנו (ראו הערה להגדרה 2.2.4).

<u>הוכחה</u>:

תהי N קבוצת הפסוקים הבאה ב- L :

$$(N1)\ \forall x(Sx \neq 0)$$
$$(N2)\ \forall x\forall y(Sx = Sy \to x = y)$$
$$(N3)\ \forall x(x + 0 = x)$$
$$(N4)\ \forall x\forall y(x + Sy = S(x + y)$$
$$(N5)\ \forall x(x \cdot 0 = 0)$$
$$(N6)\ \forall x\forall y(x \cdot Sy = x \cdot y + x)$$
$$(N7)\ (\forall x)\neg(x < 0)$$
$$(N8)\ \forall x\forall y(x < Sy \leftrightarrow x < y \vee x = y)$$
$$(N9)\ \forall x\forall y(x < y \vee x = y \vee y < x)$$

כאשר $x < y$ מוגדר ע"י הנוסחה $(\exists z)(z \neq 0 \wedge x + z = y)$.

<u>הערה</u>: יתרונה של קבוצת פסוקים זו הוא שהיא סופית, בניגוד ל P שיש בה סכמה (ראו בצמוד להגדרה 2.2.3) ולכן ניתן להציגה כפסוק אחד (חיתוך כל האקסיומות) . התורה N (אקסיומות $(N1)-(N9)$) היא הרבה פחות מאקסיומות פאנו, למשל, אי אפשר להוכיח בתורה שהחיבור קומוטטיבי או אסוציאטיבי. גם לא ניתן להוכיח כי "<" מגדיר סדר וכו'.

בהמשך נשתמש בסימון N^* המוגדר ע"י הוספת הסימן < לשפה.

נוכיח משפט עזר:

<u>2.2.7.0</u> <u>משפט עזר</u>: $P \vdash N$.

ממשפט העזר נסיק שבכדי להוכיח את משפט 2.2.7 מספיק להוכיח שכל פונקציה (וקבוצה) חשיבה יציגה ב-N .

<u>הוכחת משפט העזר 2.2.7.0</u>: $N1$ עד $N6$ מופיעות במפורש בתורת פיאנו.

$N7$ שקול ל: $(\forall x)\underbrace{(\neg\exists z)z \neq 0 \wedge x+z=0}_{x<0}$.

או: $\forall x \forall z(x+z=0 \to z=0)$

נוכיח באינדוקציה על z כי $x+sz=s(x+z)\neq 0$. ל- $z=0$ אין מה להוכיח. ל- $z=sz^*$

$x+sz^*=s(x+z^*)\neq 0$ ולכן הגרירה מתקיימת. את $N8$ ו- $N9$ מוכיחים באופן דומה. ■

<u>הוכחת משפט 2.2.7</u>:

עתה נוכיח שכל פונקציה (קבוצה) חשיבה ניתנת ליצוג ב- N. מעתה נוכל להחליף את N ב- N^* בלי שום שינוי אחר. כדי לראות זאת, נעיר שאם M מודל של N^*, אפשר לשכן בו את הטבעיים באופן טבעי:

$$g(0)=0^{N*}$$
$$g(n+1)\to S(g(n))$$

שיכון זה שומר על כל הפעולות, אך מחוץ לשכון זה החיבור יכול להתנהג בצורה שונה. עלינו להראות תחילה כי כמה פונקציות ניתנות לייצוג:

(1) פונקצית ההיטל $P_i^n(x_1,...,x_n)=x_i$, תיוצג ע"י הנוסחה $\varphi(x_1,...,x_n,y)=(y=x_i)$. עלינו להוכיח כי לכל $k_1,...,k_n$ טבעיים:

$N\vdash(\forall y)\varphi(\underline{k}_1,\underline{k}_2,...,\underline{k}_n,y)\equiv\left[y=P_i^n(\underline{k}_1,...,\underline{k}_n)\right]$: (כזכור $\underline{n}=S^n(0)$). נציב ונקבל:

$N\vdash\forall y\left[(y=\underline{k}_i)\equiv(y=\underline{k}_i)\right]$ וזה ברור (גם בלי N).

(2) הפונקציה הקבועה, $C_0(x)=0$, תיוצג ע"י $\varphi(x,y)=(y=0)$.

צ"ל: $N\vdash\forall y\left[\varphi(\underline{k},y)\equiv[y=c_0(\underline{k})\right]$: או $N\vdash(\forall y)\left[(y=0)\equiv(y=0)\right]$ וזה ברור.

(3) פונקצית החיבור, $x+y=z$, תיוצג ע"י: $\varphi(x,y,z)=(x+y=z)$.

צ"ל: $N\vdash(\forall z)(\varphi(\underline{n},\underline{m},z)\equiv(z=\underline{m+n}))$.

יספיק להוכיח $N\vdash\underline{n}+\underline{m}=\underline{n+m}$. נראה זאת באינדוקציה על m.

עבור $m=0$ $\quad N\vdash\underline{n}+\underline{0}=\underline{n+0}$.

עבור $m+1$ $\quad N\vdash\underline{n}+\underline{m+1}=\underline{n}+s(\underline{m})=s(\underline{m}+\underline{n})=s(\underline{m+n})=\underline{m+n+1}$

(4) פונקציה הכפל, $x\cdot y=z$, תיוצג ע"י $\varphi(x,y,z)=(x\cdot y=z)$ וההוכחה דומה.

(5) הפונקציה האופיינית של הסדר, $c_<(x,y)=\begin{cases}1 & x<y\\ 0 & \text{אחרת}\end{cases}$, תיוצג ע"י ($z$ = ערך הפונקציה)

$\varphi(x,y,z)=(x<y\wedge z=1)\vee(\neg(x<y)\wedge z=0)$.

צ"ל: $N\vdash(\forall z)[(\underline{n}<\underline{m}\wedge z=1)\vee\neg(\underline{n}<\underline{m})\wedge z=0]\equiv(z=c_<(n,m))$

ראשית, מ- $N7$ מקבלים שעבור $m=0$ $N\vdash \neg(\underline{n}<\underline{m})$. עתה באינדוקציה נקבל שאם $n<m$ $N\vdash \underline{n}<\underline{m}$ ואם $\neg(n<m)$ אז $N\vdash \neg(\underline{n}<\underline{m})$ (ההוכחה קלה בעזרת $N8$), ומכאן הטענה נובעת.

(6) הרכבה: נניח כי $F_\ell(x_1,...,x_n)$ $\ell=1,...,k$; $G(x_1,...x_k)$ מיוצגות ו-

$H(x_1,...x_n)=G(F_1(x_1,...,x_n),F_2(x_1,...x_n),...,F_k(x_1,...x_n))$ אזי H ניתנת להצגה.

הוכחה: נניח כי $\varphi_\ell(x_1,...,x_n,y)$ מייצגות את F_ℓ ו- $\psi(x_1,...,x_k y)$ מייצגת את G אזי:

$\vartheta(x_1,...,x_n,y)=(\exists y_1,...,y_k)(\bigwedge_{\ell-1}^{k}(x_1,...,x_n y_\ell)\wedge\psi(y_1,...,y_k,y))$ מייצגת את H.

נראה זאת: נניח כי $q_\ell=F_\ell(p_1,...,p_n)$ ו- $r=H(q_1,...,q_k)$; (r,q_i,p_i טבעיים) עלינו להראות: $N\vdash(\forall y)(\vartheta(\underline{p}_1,...,\underline{p}_n,y))\Leftrightarrow(y=\underline{r})$.

מאחר ש-y לא מופיע ב-N מספיק להוכיח בלי $\forall y$, ולכן מספיק להוכיח כל גרירה.

הכיוון "$\Leftarrow$": לפי הגדרת ייצוג, $N\vdash\bigwedge_\ell\varphi_\ell(\underline{p}_1,...,\underline{p}_n,q_\ell)\wedge\psi(q_1,...,q_k,r)$. לכן

$N\cup\{y=r\}\vdash\bigwedge_\ell\varphi_\ell(\underline{p}_1,...,\underline{q}_\ell)\wedge\psi(q_1,...,q_k,y)$, לכן

$N\cup\{y=r\}\vdash(\exists y_1,...,y_k)[\bigwedge_\ell\varphi_\ell(\underline{p}_1,...,\underline{p}_n,y_\ell)\wedge\psi(y_1,...,y_k,y)]$.

הכיוון "$\Rightarrow$": צ"ל $N\cup\vartheta(\underline{p}_1,...,p_n,y)\vdash y=\underline{r}$ וזה שקול ל:

$N\cup\{\bigwedge\varphi_\ell(\underline{p}_1,...,p_n,y_\ell)\wedge\psi(y_1,...,y_k,y)\vdash y=\underline{r}$ כיוון ש-φ_ℓ מייצגת את F_ℓ,

$N\vdash y_\ell=q_\ell$, לכן $N\vdash\psi(q_1,...,q_n,y)$, אך ψ מייצגת את G, ולכן:

$N\cup\{\psi(q_1,...,q_n,y)\}\vdash y=\underline{r}$.

(7) מזער (מינימום): נניח ש- $F(x_1,...,x_n,y)$ מיוצגת ע"י $\varphi(x_1,...,x_n,y,z)$ ותהי

$G(x_1,...,x_n)=\mu_y F(x_1,...,x_n,g)$ (כזכור הגדרת μ היתה שעבור ערך מסוים F מתאפסת ולכל ערך קטן יותר F מוגדרת ושונה מ-0). נראה ש-G תיוצג ע"י:

$\psi(x_1,...,x_n,v)=\varphi(x_1,...,x_n,v,\underline{0})\wedge(\forall u<v)(\neg\varphi(x_1,...,x_n,u,\underline{0}))$. נניח שנתונים לנו

$k_1,...,k_n$ ונניח כי $q_\ell=F(k_1,...,k_n,\ell);\ G(k_1,...,k_n)=r$. נשים לב כי

$N\vdash(x<\underline{p})\equiv(x=\underline{0}\vee x=\underline{1},...\vee x=\underline{p-1})$.

ההוכחה באינד' על p. עבור $p=0$ לפי $N7$ צד שמאל שקרי וצד ימין הוא איחוד ריק, ולכן שקר לפי ההגדרה. עבור $p+1$ לפי $N8$, $N\vdash(x<p+1)\Leftrightarrow[(x<p)\vee x=p-1)$ והטענה נובעת מהנחת האינדוקציה.

עתה נוכיח:
$$N\vdash \psi(\underline{k}_0,\dots,\underline{k}_n,z)\to z=\underline{r} \quad (1)$$
$$N\vdash z=\underline{r}\to \psi(\underline{k}_0,\dots,\underline{k}_n,z) \quad (2)$$

הוכחה: נראה ראשית את (2). די להוכיח ש- $N\vdash \psi(\underline{k}_0,\dots,\underline{k}_n,\underline{r})$, אך ψ חיתוך של שני פסוקים, לכן די להוכיח כל אחד מהם בנפרד.

2(א): עלינו להוכיח $N\vdash \varphi(\underline{k}_0,\dots,\underline{k}_n,\underline{r},0)$ אך $F(k_0,\dots,k_n,r)=0$ לפי הגדרת G ו- r; מכיוון ש- φ מייצגת את F $N\vdash \varphi(\underline{k}_0,\dots,\underline{k}_n,\underline{r},\underline{0})$ כנדרש.

2(ב): באופן דומה לכל $p<r$ $N\vdash \neg\varphi(\underline{k}_0,\dots,\underline{k}_n,\underline{p},0)$ אך כיוון ש:

$N\vdash (x<r)\equiv (x=0)\vee\dots\vee(x=r-1)$ לפי האקסיומות הלוגיות (ואפשר דרך משפט השלמות) נקבל: $N\vdash (\forall x)[x\le \underline{r}\to\neg\varphi(k_0,\dots,k_n,x,0)]$.

בזאת הוכחנו את (2).

עתה נוכיח את (1). די להוכיח $N\cup\{\psi(k_0,\dots,k_n,z)\}\vdash z=r$, אבל $N\cup\{\psi(\underline{k}_0,\dots,\underline{k}_n,z)\}\cup\{\underline{p}<z\}\vdash\neg\varphi(\underline{k}_0,\dots,\underline{k}_n,\underline{p},0)$ ואם נניח $p=r$ נקבל סתירה, כי $N\vdash\varphi(\underline{k}_0,\dots,\underline{k}_n,r,0)$, כי $F(k_0,\dots,k_n,r)=0$. לכן $N\cup\psi(\underline{k}_0,\dots,\underline{k}_n,z)\vdash\neg(\underline{r}<z)$ (*). עתה, אם $p<r$ אזי $N\cup\{\psi(k_0,\dots,k_n,z)\}\cup\{\underline{p}=z\}\vdash\varphi(\underline{k}_0,\dots,\underline{k}_n,\underline{p},0)$ אך $F(k_0,\dots,k_n,p)$ מוגדר ושונה מאפס ולכן $N\vdash\neg\varphi(k_0,\dots,k_n,p,0)$ בסתירה. לכן (עבור $p<r$) $N\cup\psi(\underline{k}_0,\dots,\underline{k}_n,z)\vdash\neg(z=\underline{p})$ (**). לפי (*) ו- (**) נקבל $N\vdash z=r$.

בזאת סיימנו את הוכחת המשפט: כל פונקציה חשיבה היא יציגה ב- N. ■

<u>מסקנות</u>:

(1) קל לוודא כי הפונקציה $t\leftarrow$ (מספר גדל של t) היא פונקצית שם. בנוסף, פונקציה זו חשיבה (טענה 2.2.2) ולכן קל לבדוק שגם פונקצית האלכסון חשיבה. מכאן נסיק בעזרת המשפט האחרון שהוכחנו, שפונקצית האלכסון מיוצגת ב- N לכן לפי משפט האמת של *Tarski* ל- N תורה לא כריעה. מכאן שגם P (האריתמטיקה של פיאנו) אינה כריעה.

הוכחה נוספת לאי כריעות N ניתן לקבל בעזרת אי כריעות בעיית העצירה (משפט 2.1.8) תהי $\varphi(e,z,n)$ הנוסחה האומרת שמכונת טיורינג T_n עצרה על הקלט n לאחר z צעדים לכל היותר. היחס $\varphi(e,z,n)$ חשיב ולכן מיוצג ב- N לכן אם $T_e(n)$ לא עוצרת $N\vdash\neg\varphi(e,n,z)$ לכל z. מצד שני, אם $T_e(n)$ עוצרת יש איזה z עבורו $N\vdash\varphi(e,n,z)$, ולכן $N\vdash\exists z\,\varphi(e,n,z)$. יוצא ש- $N\vdash\exists z\,\varphi(e,n,z)$ אסם $T_e(n)$ עוצרת. אילו הייתה N כריעה היינו יכולים להכריע לכל $\langle e,n\rangle$ אם $N\vdash\exists z\,\varphi(e,n,z)$ ובכך מכריעים את בעיות העצירה.

שיקולים אלו אפשר בעצם לקבל קצת יותר: אילו לכל $\langle e,n\rangle$ כך ש- $T_e\ (n)$ אינה עוצרת היה מתקיים $N\vdash(\forall z)\neg\varphi(e,n,z)$ היינו יכולים להכריע את בעיית העצירה: בהנתן $\langle e,n\rangle$ היינו עוברים באופן חשיב על כל ההוכחות ב- N עד שהיינו נתקלים בהוכחה ל- $\varphi(e,z,n)$ או בהוכחה ל- $(\forall z)\neg\varphi(e,n,z)$. לכן יש $\langle e,n\rangle$ עבורו $T_e\ (n)$ אינה עוצרת אבל לא מתקיים $N\vdash(\forall z)\neg\varphi(e,n,z)$.

(הערה: בטיעון האחרון עשינו שימוש בהנחה שקיים מודל תקני למספרים הטבעיים, או לכל הפחות בהנחה החלשה יותר לפיה תורת פיאנו היא ω-עקבית. בהמשך נראה הוכחה נוספת לטענה זו, שאינה נזקקת להנחות מעין אלה).

(2) תורת המספרים האמיתית (האריתמטיקה, כלומר: כל הפסוקים שהמודל התקני של המספרים הטבעיים מספק) $Th(\mathbf{N},S,0,+,\cdot)$ היא לא אריתמטית. כלומר אין נוסחה $\varphi(x)$ בשפת תורת המספרים כך ש-

$\mathbf{N}\models\varphi(x)\Leftrightarrow$ *x מספר גדל של פסוק בשפת תורת המספרים ש- $\mathbf{N}$ מספקו*

אילו היתה נוסחה $\varphi(x)$ כנ"ל היה פסוק ψ כמובטח במשפט *Tarski* (או ליתר דיוק במפשט נקודת השבת) ולכן בפרט $\mathbf{N}\models\varphi('\psi')\Leftrightarrow\neg\psi$ (*). אבל אם $\mathbf{N}\models\psi$ אז מהגדרת $\varphi(x)$ $\mathbf{N}\models\varphi('\psi')$, אך מ-(*) זה גורר ש- $\mathbf{N}\models\neg\psi$ וזו סתירה. סתירה דומה נקבל גם אם נניח ש- $\mathbf{N}\models\neg\psi$.

(3) כל קבוצה נל"ח היא אריתמטית.

הוכחה: לכל פונקציה שלמה חשיבה $f(\bar{x})$ יש יצוג ב- N ע"י נוסחה $\varphi(\bar{x},y)$. מכיוון ש- $\mathbf{N}\models N$ נקבל ש- $f(k_1...k_m)=r\Leftrightarrow\mathbf{N}\models\varphi(k_1,...,k_m,r)$, ובפרט כל יחס חשיב גדיר. אם A נל"ח יש יחס $R(x,y)$ חשיב כך ש: $x\in A\leftrightarrow\exists y\ R(x,y)$ ואם $\varphi(x,y)$ מייצגת את R $(\exists y)\varphi(x,y)$ מגדירה את A.קיבלנו $x\in A\Leftrightarrow(\exists y)R(x,y)\Leftrightarrow N\models\exists y\varphi(x,y)$.

(4) מסקנה: תורת המספרים האמיתית איננה נל"ח. (זה נובע ממסקנות (2) ו-(3)).

(5) אם T סופית, חשיבה או אף נל"ח, אז התורה של T נל"ח. אם T חשיבה, היא אריתמטית, וכך גם תורתה.

כדי לראות זאת נביט בנוסחה: $\psi(z)=\theta_1(z)\wedge\theta_2(z)$

באשר $\theta_1(z)$ אומרת ש-z מספר גדל של פסוק בשפת תורת המספרים; $\theta_2(z)$ אומרת שקיים x כך ש- x מצפין סדרה סופית, z האיבר האחרון בסדרה, וכל איבר בסדרה הוא אקסיומה של T או שהוא אקסיומה לוגית או שהוא מתקבל מן האיברים הקודמים לו בסדרה ע"י אחד מכללי ההיסק.

ψ לעיל מתארת את קבוצת מסקנות T. קל לבדוק שאם T נל"ח ψ מגדירה קבוצה נל"ח, ואם T אריתמטית ψ מגדירה קבוצה אריתמטית.

בפרט לתורת המספרים האמיתית אין מערכת אקסיומות חשיבה, ואפילו לא אריתמטית. בלשון אחרת: כל מערכת אקסיומות אריתמטיות שמסופקת ע"י הטבעיים נותנת תורה לא שלמה.

ממסקנה 5 לעיל ברור כי התורה N נל"ח באמת (כלומר נל"ח ואינה חשיבה), שכן היא לא כריעה.

(6) אם T תורה חשיבה ושלמה, אז היא כריעה.

הוכחה: בהנתן ψ נעבור על כל ההוכחות מ- T עד שניתקל בהוכחה ל- ψ או ל- $\neg\psi$ (זה יקרה בהכרח, כי T שלמה).

(7) תחשיב הפרדיקטים אינו כריע.

הוכחה: אחרת N היתה כריעה. במקום לשאול אם $N\vdash\psi$ נשאל אם $N_i\vdash\bigwedge_{l-1}^{9}N_l\to\psi$ (N_i מערכת האקסיומות הנתונה במשפט 2.2.7) (יש לדרוש שבשפה יהיו לפחות סימן יחס אחד דו מקומי או 2 סימני פונק' חד מקומים).

(8) יש פסוק ψ בתורת המספרים כך ש: P לא מוכיחה את ψ אבל לא מתקיים $P_A\vdash\neg\psi$.

הוכחה: תהי $\varphi(x)$ מגדירה את הייחס "X מספר גדל של פסוק יכיח בתורת המספרים" ו- ψ הפסוק המובטח ממשפט נקודת השבת (ראינו דוגמה לפסוק כזה גם במסקנה (1), אך לצורך הוכחת הדוגמה שם נזקקנו להנחות נוספות).

(9) **<u>(משפט האי-שלמות השני של *Gödel*)</u>**: לא ניתן להוכיח ב-N ש-N עקבית.

<u>הוכחה</u>: ראשית, אנו יודעים ש-N עקבית (כי המספרים הטבעיים מודל של N), ולכן אינה מוכיחה פסוק ושלילתו. שנית, נזכור שבהוכחת מסקנה (5) הראנו שיש פסוק (שם קראנו לפסוק זה $\psi(z)$) בשפת בתורת המספרים, האומר שהפסוק ש-z מספר גדל שלו יכיח ב-N. לכן יש בשפת N פסוק, שנסמנו $Con(N)$, האומר שהפסוק $(\exists x)(x\neq x)$ אינו יכיח ב-N, בפרט פסוק זה אומר ש-N עקבית. יהי $\chi(x)$ הפסוק האומר שהפסוק שמספר גדל שלו x אינו יכיח ב-N.

נשים לב שממשפט נקודת השבת של גדל (חלק (2) של משפט 2.2.6) נובע שאם $\varphi(x)$ נוסחה כלשהי בשפה של N אזי יש פסוק ψ_φ המקיים $N\vdash\psi_\varphi\leftrightarrow\varphi('\psi_\varphi')$ (פשוט בוחרים את שלילת הפסוק ψ, המובטח שם). עתה $Con(N)\to\neg(N\vdash\psi_\varphi)$, שהרי אילו התקיים $N\vdash\psi_\chi$ היינו מקבלים (מהגדרת ψ_φ) ש- $N\vdash\chi('\psi_\chi')$, כלומר, (מהגדרת χ), ש- ψ_φ אינו יכיח ב-N, בסתירה. נובע, אם כן, ש- $N\vdash Con(N)\to\chi('\psi_\chi')$, כלומר, אילו התקיים $N\vdash Con(N)$ היינו מקבלים $N\vdash\chi('\psi_\chi')$, ומבחירת ψ_φ זה גורר $N\vdash\psi_\chi$, בסתירה למה שהראנו לעיל.

תרגילים - משפט האי-שלמות ומסקנותיו:

1. בשאלה זו נוכיח את הגרסה החזקה של משפט האי-שלמות של גדל, שהזכרנו בפתיחת הפרק הנוכחי:

א. יהיו $R \subseteq \mathbf{N}$ יחס חשיב ו- $F : N^2 \to N$ פונקציה חשיבה ומלאה. לכל $g \in N$ נסמן $F_g := \{n \in N : F(n,g) \in R\}$ הוכיחו כי האוסף $\{F_g : g \in N\}$ אינו מכיל את אוסף כל הקבוצות החשיבות. (הראו שהטענה אינה נכונה אם לא נדרוש ש-F שלמה).

ב. תהי L שפה במילון המכיל את $S, 0$, ותהי T תורה בשפה L. נסמן $\underline{n} = S^n(0)$.
תהיינה $P,Q \subseteq N$ זרות, כך שלכל קבוצה חשיבה C יש נוסחה $\varphi(x) \in L$, כך שלכל טבעי n מתקיים: אם $n \subseteq C$ אז $g(\varphi(\underline{n})) \in P$ ואם $n \notin C$ אז $g(\varphi(\underline{n})) \in Q$, באשר $g(x)$ הוא מספר גדל של הנוסחה x. הראו ש-P,Q אינן ניתנות להפרדה חשיבה (כלומר, לא קיימת R חשיבה המקיימת $P \subseteq R$ ו- $Q \subseteq N \setminus R$). רמז: השתמשו בסעיף הקודם עבור פונקציה חשיבה מלאה המרחיבה את g.

ג. נאמר שתורה T אינה ניתנת להפרדה חשיבה אם הקבוצות $\{g(\varphi) : T \ni \varphi\}$ ו- $\{g(\neg\varphi) : T \ni \varphi\}$ אינן ניתנות להפרדה חשיבה. הראו, שאם T מייצגת כל קבוצה חשיבה ב-N אז T אינה ניתנת להפרדה חשיבה, ובפרט אינה כריעה (כלומר קבוצת מספרי גדל של הפסוקים היכיחים ב-T אינה כריעה). הסיקו ש-N אינה ניתנת להפרדה חשיבה.

ד. נאמר שתורה T מייצגת חלש קב' $C \subseteq N$ אם יש נוסחה $\varphi(x)$ כך שלכל n טבעי מתקיים $n \in C \leftrightarrow T \vdash \varphi(\underline{n})$. הוכיחו שאם T מייצגת חלש כל קבוצה חשיבה אז T אינה כריעה.

2. הוכיחו שהתורה של Z, בשפה $L=\{0,1,+,\cdot\}$ אינה כריעה. רמז: העזרו במשפט הבא של לגרנז': יהי $n \in N$ כלשהו, אזי n הוא סכום של ארבע ריבועים.

3. ידוע המשפט הבא של *Tarski*: תהי $T=Th(R,0,1,+,\cdot,<)$ (כלומר T התורה של הממשיים עם יחס הסדר) אזי T כריעה.

א. הראו היכן נכשלת הוכחת משפט גדל, אם ננסה להחילה על התורה T.

ב. הסיקו שהטבעיים אינם גדירים ב-T, כלומר לא קיימת נוסחה $\varphi(x) \in L(T)$ כך שלכל מודל $M \models T$ מתקיים $\varphi^M \models Th(N)$, באשר $\varphi^M = \{a \in M : M \models \varphi(a)\}$.

4. הסבירו מדוע משפט האי-שלמות השני של גדל נכון גם במקרים הבאים:

א. T תורה (בפרט עקבית) חשיבה כלשהי, המרחיבה את N (כלומר $\{g(\varphi) : \varphi \in T\}$ חשיבה ואם $\varphi \in N$ אז $\varphi \in T$).

ב. T היא תורת הקבוצות, ZF (ראו תרגיל 1 לפרק *3.1*), ומניחים ש-ZF עקבית.

ג. היא הרחבה חשיבה של ZF (תורת הקבוצות), שעקבית אם ZF עקבית.

ד. הסיקו שאם תורת הקבוצות עקבית אז אין לה הרחבה חשיבה ושלמה.

5.

א. *הסבירו את השגיאה בנימוק הבא: נראה ש-ZF אינה עקבית. ממה שהראתם בשאלה 4, אם ZF עקבית $\neg(ZF \vdash Con(ZF))$ לכן בפרט $T = ZF \cup \{\neg Con(ZF)\}$ עקבית. אבל $\mathrm{Con}(ZF)$

הוא הפסוק האומר ש-$(\exists x)(x \neq x)$ אינו יכיח ב-ZF, ולכן בכל מודל של T יש הוכחה לכך ש-$(\exists x)(x \neq x)$, זה לא יתכן, ולכן ההנחה ש-ZF עקבית מובילה לסתירה. מכאן ש-ZF אינה עקבית.

ב. *הסבירו את השגיאה בנימוק הבא: מתורת הקבוצות ידוע של-ZF אין אקסיומטיזציה סופית (זה משפט אמיתי, ולא כאן השגיאה. בפרק של תורת המודלים נראה הוכחה חלקית של טענה זו). ואמנם, אם תביטו באקסיומטיזציה של ZF שמופיעה בתרגיל 1 של פרק 3.1 תראו, שמופיעה בה סכמת אקסיומה מהצורה: "לכל נוסחה φ :...". נחליף את סכמת האקסיומה בפסוק $\exists x(\vartheta(x) \wedge \ldots)$, באשר $\vartheta(x)$ היא הנוסחה האומרת ש-x מצפין סדרת סימנים בשפה ושסידרה זו היא נוסחה חוקית בשפה (כלומר, במקום סכמת אקסיומה נקבל פסוק אחד האומר "לכל x, אם x מצפין נוסחה אז ...". באופן זה נקבל אקסיומטיזציה סופית של ZF, בסתירה.

3 תורת המודלים

3.0 הגדרות בסיסיות

3.0.1 סימונים:

(1) τ יסמן מילון, כלומר קבוצת סימני היחסים (=פרדיקטים) וסימני הפונקציות. ליתר דיוק זו הפונקציה המתאימה לכל סימן כזה את מספר המקומות שלו.

(2) $L = \underline{L}(\tau)$ תסמן את השפה, קבוצת הנוסחאות מסדר ראשון במילון τ. כאשר המילון קבוע נכתוב רק L.

(3) χ,ψ,φ תסמנה נוסחאות (מסדר ראשון בשפה L).

(4) M,N יסמנו מבנים או מודלים, כאשר מבנה M למילון τ (או לשפה $\underline{L}(\tau)$) הוא $\left(|M|,R^M,\ldots,F^M,\ldots\right)_{R,F\in\tau}$, כאשר $|M|$ הוא עולם המודל, קבוצה לא ריקה של אברים; R^M הוא פרוש סימן היחס $R \in \tau$ עם מספר מקומות מתאים ו- F^M הוא פרוש סימן הפונקציה $F \in \tau$ עם מספר מקומות מתאים.

(5) בהינתן מבנה M המילון של M יהיה $\tau_M = \tau(M)$ ושפת M היא $L_M = \underline{L}(\tau_M)$.

(6) e,d,c,b,a יסמנו אברים של מבנים. נכתוב בד"כ $a \in M$ במקום $a \in |M|$.

(7) $\bar{e},\bar{d},\bar{c},\bar{b},\bar{a}$ יסמנו סדרות סופיות של אברים מהמבנה. נכתוב בד"כ $\bar{a} \in M$ במקום $\bar{a} = \langle a_0,\ldots,a_{n-1}\rangle$, $a_0,\ldots,a_{n-1} \in |M|$.

(8) z,y,x יסמנו משתנים אישיים. P,Q,R יסמנו סימני יחסים. ליחס דו מקומי R נרשה לכתוב xRy במקום $R(x,y)$. H,G,F יסמנו סימני פונקציות, אבל קבועים אישיים (שהם מקרה פרטי) נסמן גם ב- $\underline{c}$.

3.0.2 הגדרה:

(1) $\varphi(\bar{x})$ הוא זוג $(\varphi,\bar{x})$ (ונרשום $\varphi = \varphi(\bar{x})$) כאשר:

א. φ נוסחה.

ב. $\bar{x}$ סדרת משתנים אישיים ללא חזרות, כך שכל משתנה אישי המופיע ב- φ באופן חופשי נמצא ביניהם. (אך יתכן שחלק מהם הינם משתני סרק, אינם מופיעים כלל ב- φ).

(2) נאמר ש- $M \models \varphi[\bar{a}]$, **המבנה M מספק** את $\varphi[\bar{a}]$ אם:

א. M מבנה ל- τ, φ נוסחה ב- $\underline{L}(\tau)$.

ב. $\varphi(\bar{x}) = (\varphi,\bar{x})$ כמו ב- (1) ונניח ש- $\bar{x} = \langle x_1,\ldots,x_n\rangle$.

ג. $\bar{a} = \langle a_1,\ldots,a_n\rangle$ סדרה של אברים של M.

ד. לכל השמה f המקיימת $f(x_\ell) = a_\ell$ המבנה M מספק את הנוסחה φ לגבי ההשמה f.

(3) לשם עצם ϑ , וסדרת משתנים $\bar{x}$ ללא חזרות, בה מופיע כל משתנה אישי המופיע ב- ϑ נכתוב $\vartheta(\bar{x})$ או $\vartheta = \vartheta(\bar{x})$.

(4) אם $\vartheta = \vartheta(\bar{x})$ שם עצם ב- $\underline{L}(\tau)$, $\bar{x} = \langle x_0,...,x_{n-1}\rangle$, M מבנה למילון τ , ו- $\bar{a} = \langle a_0,...,a_{n-1}\rangle \in M$ אז $\vartheta^M(\bar{a})$ הוא הערך של ϑ לכל השמה f למודל M, המקיימת $f(x_\ell) = a_\ell$.

3.0.3 הגדרה: למילון τ , $\underline{L}^-(\tau)$ היא השפה במילון τ ללא סימן השוויון, כלומר קבוצת הנוסחאות מסדר ראשון במילון τ בהן סימן השוויון אינו מופיע.

הערה: לסימן השוויון (=) יש מעמד ביניים: הוא קבוע לוגי כמו הקשרים $(\wedge, \vee, \neg, \rightarrow)$ והכמתים $(\forall, \exists)$ אך מתנהג כמעט כמו כל סימן יחס אחר כי בכל מבנה M הוא מתפרש כיחס השויון על M, $\approx^M$. המשפט הבא אומר שזה לא גורם לבעיות.

3.0.4 משפט: נניח כי

א. τ מילון, τ^+ אותו מילון כאשר נוסיף לו סימן יחס דו מקומי חדש E .

ב. M^+ מבנה למילון τ^+ .

ג. M^+ מקיים את אקסיומות השוויון למילון τ כאשר סימן השוויון מוחלף ב- E , זאת אומרת ש- M^+ מספק את הסגור הכולל של הנוסחות הבאות (כלומר מוסיפים כמתים כוללים על המשתנים האישיים שמופיעים):

i. רפלקסיביות: $x\mathrm{E}x$.

ii. הדדיות (= סימטריה) : $x\mathrm{E}y \rightarrow y\mathrm{E}x$.

iii. תורשתיות: $x\mathrm{E}y \wedge y\mathrm{E}z \rightarrow x\mathrm{E}y$.

iv. לכל $R \in \tau$ בן n מקומות: $x_1\mathrm{E}y_1 \wedge ... \wedge x_n\mathrm{E}y_n \rightarrow (R(x_1,...x_n) \equiv R(y_1,...y_n))$.

v. לכל $F \ni \tau$ בן n מקומות: $x_1\mathrm{E}y_1 \wedge ... \wedge x_n\mathrm{E}y_n \rightarrow (F(x_1,...x_n) = F(y_1,...y_n))$.

אז:

(1) יש מבנה M למילון τ ופונקציה f המקיימים:

א. f פונקציה מ- $|M^+|$ על $|M|$.

ב. לכל $a,b \ni M$ מתקיים $f(a) = f(b) \Leftrightarrow M^+ \models aEb$.

ג. לכל סימן יחס $R \ni \tau$ ואברים $a_1,...,a_{n(R)}$ של M^+ :

$M^+ \models R[a_1,...,a_{n(R)}] \Leftrightarrow M \models R[f(a_1),...,f(a_{n(R)})]$.

ד. לכל סימן פונקציה F ב τ ואברים $a_1,...,a_{n(R)}$ של M^+:

$f(F^{M^+})(a_1,\dots,a_n) = F^M(f(a_1),\dots,f(a_n))$.

כלומר, אם נחשוב על E כעל יחס שקילות, f מעבירה כל מחלקת שקילות לאותה התמונה תוך שהיא שומרת על הפונקציות ועל היחסים כפי שהיו ב- M^+.

(2) נניח:

i. M, M^+ ו- f מקיימים את התנאים מ-(1).

ii. φ^+ ב $\underline{L}^-(\tau^+)$ כלומר φ^+ נוסחה מסדר ראשון במילון τ^+ ללא סימן השוויון.

iii. $\varphi = sub_-^E(\varphi^+)$, כלומר φ מתקבלת מ- φ^+ על ידי החלפת E ב-"=".

iv. $\varphi^+ = \varphi^+(\bar{x})$ כאשר לשם פשטות $\bar{x} = \langle x_0,\dots,x_{n-1}\rangle$.

v. $a_0,\dots,a_{n-1}$ אברים של M^+.

אז $M^+ \models \varphi^+[a_0,\dots a_{n-1}] \Leftrightarrow M \models \varphi[f(a_0),\dots,f(a_{n-1})]$, כלומר, f שומרת על הנוסחאות כאשר ב- M היחס E מפורש כשוויון.

<u>הוכחה</u>:

(1) לכל a ב M^+ נגדיר: $a/E^{M^+} = \{b : M^+ \mid aEb\}$. קל לראות (מהנחות *(i)*, *(ii)* ו-*(iii)* בהתאמה) ש:

i. $a \in a/E^{M^+}$ (כי $M^+ \models \forall x(xEx)$).

ii. $a \in b/E^{M^+} \Leftrightarrow b \in a/E^{M^+}$.

iii. אם $a \in b/E^{M^+}$ ו- $b \in c/E^{M^+}$ אז $a \in c/E^{M^+}$.

(זאת אומרת, E^{M^+} יחס שקילות, a/E^{M^+} מחלקות השקילות) לכן

$(*)_1$ לכל a,b מ- M^+ הקבוצות a/E^{M^+}, b/E^{M^+} שוות או זרות (ואינן ריקות).

נגדיר את המבנה M:

- עולמו $\{a/E^{M^+} : a \in M^+\}$;
- לסימן יחס R נגדיר: $R^M = \{(a_0/E^{M^+},\dots,a_{n-1}/E^{M^+}) : (a_0,\dots,a_{n-1}) \in R^M\}$;
- לסימן פונקציה F, $n = n(F)$, נגדיר:

$F^M(a_0/E^{M^+},\dots,a_{n-1}/E^{M^+}) = F^{M^+}(a_0,\dots,a_n)/E^{M^+}$;

לבסוף, נגדיר את הפונקציה f על ידי $f(a) = a/E^M$.

האם M הוא אכן מבנה למילון τ? ברור ש-$|M|$ קבוצה לא ריקה, ו-R^M יחס $n(R)$ מקומי על $|M|$, אך האם F^M אכן פונקציה $n(F)$ מקומית מ-$|M|$ ל-$|M|$? לשם כך מספיק לוודא:

$(*)_2$ אם $a_{n-1}/E^{M^+} = b_{n-1}/E^{M^+},....,a_0/E^{M^+} = b_0/E^{M^+}$ אז

$(F^{M^+}(a_0,...,a_{n-1}))/E^{M^+} = (F^{M^+}(b_0,...,b_{n-1}))/E^{M^+}$.

בסימון אחר: $f(F^{M^+}(a_0,...,a_{n-1}) = f(F^{M^+}(b_0,...,b_{n-1}))$, אך זה נובע מהנחה (*iv*). באופן דומה, מהנחה (*iii*) נובע:

$(*)_3$ לכל סימן יחס n-מקומי R ב τ ואברים $a_0,...,a_{n-1}$ של M^+:

$M^+ \models R[a_0,...,a_{n-1}] \Leftrightarrow M \models R[f(a_0),...,f(a_{n-1})]$.

בזאת סיימנו את הוכחת חלק (1).

(2) בשביל להוכיח חלק זה השלב הבא הוא:

$(*)_4$ לכל שם עצם $\vartheta = \vartheta(x_0,...,x_{n-1})$ ב-$\underline{L}(\tau)$ ואיברים $a_0,....,a_{n-1} \in M$ מתקיים

$f(\vartheta^{M^+}(a_0,...,a_{n-1})) = \vartheta^M(f(a_0),...,f(a_{n-1}))$.

ההוכחה באינדוקציה:

<u>מקרה 1</u>: ϑ קבוע אישי $\underline{c}$:

$$\vartheta^{M^+}(a_0,...,a_{n-1}) = \underline{c}^{M^+}$$

לכן:

$$f(\vartheta^{M^+}(a_0,...,a_{n-1})) = f(\underline{c}^{M^+}) = \underline{c}^{M^+}/E^{M^+}$$

אך לפי הגדרת M

$$\underline{c}^M = \underline{c}^{M^+}/E^{M^+}$$

<u>מקרה 2</u>: ϑ משתנה אישי, נאמר x_k, אזי:

$$\vartheta^{M^+}(a_0,...,a_{n-1}) = a_k$$

לכן:

$$f(\vartheta^{M^+}(a_0,...,a_{n-1})) = f(a_k) = a_k/E^{M^+}$$

$$\vartheta^M(f(a_0),...,f(a_{n-1})) = f(a_k) = a_k/E^{M^+}$$

כנדרש.

<u>מקרה 3</u>: $\vartheta = F(\vartheta_0,...,\vartheta_{m-1})$, F סימן פונקציה m-מקומי וכן $\vartheta_k = \vartheta_k(x_0,...,x_{n-1})$. עתה, לפי הגדרת פרוש שם עצם ב-M.

$$\vartheta^M(f(a_0),...,f(a_{n-1})) =$$

$$= F^M(\vartheta_0^M(f(a_0),\ldots,f(a_{n-1})),\ldots,\vartheta_{m-1}^M(f(a_0),\ldots,f(a_{n-1})) =$$

לפי הנחת האינדוקציה:

$$= F^M(f(\vartheta_0^{M^+}(a_0,...,a_{n-1}),...,f(\vartheta_{m-1}^{M^+}(a_0,...,a_{n-1})) =$$

לפי הגדרת F^M ו-$(*)_2$:

$$= f(F^{M^+}(\vartheta_0^{M^+}(a_0,\ldots,a_{n-1})),\ldots,\vartheta_{m-1}^{M^+}(a_0,\ldots,a_{n-1})) =$$

לפי הגדרת פרוש שם עצם ב-M^+ :

$$= f(\vartheta^{M^+}(a_0,...,a_{n-1}))$$

עתה נוכל לגשת להוכחת מסקנת חלק (2). נוכיח אותה באינדוקציה על הנוסחה φ :

<u>מקרה 1</u>: $\varphi^+(\bar{x}) = \vartheta_1(\bar{x}) E \vartheta_2(\bar{x})$ ולכן $\varphi(\bar{x}) = [\vartheta_1(\bar{x}) = \vartheta_2(\bar{x})]$ זה נובע מהקשר בין f ו-E (ב' מהמסקנות של חלק (1)).

<u>מקרה 2</u>: $\varphi^+(\bar{x}) = R(\vartheta_1,...,\vartheta_{n-1})$, כאשר ϑ_k שמות עצם ב-$\underline{L}(\tau)$. יוצא $\varphi(\bar{x}) = \varphi^+(\bar{x})$ וכיוון שהרשנו משתני סרק מותר לכתוב $\vartheta_k = \vartheta_k(\bar{x})$ (זה נובע מ-$(*)_3$ ו- $(*)_4$).

<u>מקרה 3</u>: $\varphi^+(\bar{x}) = \varphi_1^+ \to \varphi_2^+$. שוב מותר לרשום $\varphi_1^+ = \varphi_1^+(\bar{x})$ וכן $\varphi_2^+ = \varphi_2^+(\bar{x})$. המסקנה הנדרשת נובעת לפי הנחת האינדוקציה ולוח האמת של הקשר.

<u>מקרה 4</u>: $\varphi^+ = \neg\varphi_1^+(\bar{x})$ לפי הנחת האינדוקציה ולוח האמת של הקשר.

<u>מקרה 5</u>: $\varphi^+(\bar{x}) = \exists y \varphi_1^+(\bar{x}, y)$. ב.ה.כ. y אינו מופיע ב-$\bar{x}$ ומותר לכתוב $\varphi_1 = \varphi_1(\bar{x}, y)$, כלומר, אם $\bar{x} = \langle x_0,...,x_{n-1}\rangle$ ב.ה.כ. אפשר לרשום $y = x_n$, לכן $\varphi_1^+ = \varphi_1^+(x_0,...,x_n)$ עתה נשתמש בהנחת האינדוקציה והגדרת הסיפוק של הכמת הישי. ■

<u>3.0.5 הגדרה</u>:

(1) M מודל של T אם:

i. M מבנה במילון τ.

ii. T קבוצת פסוקים ב-$L_M = \underline{L}(\tau)$ (שפת M).

iii. לכל $\psi \in T$, M מספק את ψ.

(2) תורה היא זוג (T,τ) , כאשר τ מילון ו-T היא קבוצת פסוקים בשפה $\underline{L}(\tau)$, שלכל תת קבוצה סופית שלה יש מודל. כרגיל נכתוב רק את T, ונניח כי המילון ברור מההקשר או נאמר T תורה ב-$L = \underline{L}(\tau)$.

<u>3.0.6 משפט הקומפקטיות</u>: לכל תורה T יש מודל, כלומר, אם T קבוצת פסוקים בשפה $\underline{L}(\tau)$ ולכל תת קבוצה סופית יש מודל אז ל-T יש מודל.

אפשר להוכיח משפט זה בעזרת משפט השלמות, אך נראה בהמשך הוכחה אחרת שאינה נזקקת למושג ההוכחה.

אי הבהירות בהגדרה 3.0.5-(2) מוצדקת על ידי ההגדרה הבאה:

3.0.7 הגדרה: נניח כי $\tau_1 \subseteq \tau_2$ מילונים, M_2 מודל ל-τ_2, נגדיר את $M_1 = M_2 \uparrow \tau_1$ בתור $M_1 = (|M_2|,\ldots,R^{M_2},\ldots,F^{M_2},\ldots)_{R,F\in\tau_1}$.

נאמר כי M_2 העשרה של M_1 למילון τ_2 (או השפה $\underline{L}(\tau_2)$) ו-M_1 צמצום של M_2 למילון τ_1 (או לשפה $\underline{L}(\tau_1)$).

3.0.8 טענה: נניח כי $\tau_1 \subseteq \tau_2$ מלונים M_2 מבנה ל-τ_2, אזי:

(1) $M_2 \uparrow \tau_1$ מבנה ל-τ_1.

(2) אם $\varphi(\bar{x})$ נוסחה ב-$\underline{L}(\tau_1)$ אז $\varphi(\bar{x})$ ב-$\underline{L}(\tau_2)$ ולכל סדרה $\bar{a}$ מ-M_2 באורך של $\bar{x}$ מתקיים $M_2 \models \varphi[\bar{a}] \Leftrightarrow M_1 \models \varphi[\bar{a}]$.

(3) אם T תורה בשפה $\underline{L}(\tau_1)$ אז:

i. M_2 (מבנה לשפה $\underline{L}(\tau_2)$) מודל של T אם $M_2 \uparrow \tau_1$ הוא מודל של T.

ii. יש ל-T מודל בשפה $\underline{L}(\tau_2)$ אם יש ל-T מודל בשפה $\underline{L}(\tau_1)$.

את הוכחת הטענה נשאיר כתרגיל לקורא.

3.0.9 הגדרה: יהי M מבנה, התורה של M היא קבוצת הפסוקים $Th(M) = \{\psi \in L_M : \psi \text{ מספק את } M\}$.

3.0.10 הגדרה:

תהי T תורה בשפה $\underline{L}(\tau)$. קבוצת המסקנות של T היא $con(T) = \{\psi \in L(\tau) : M \models \psi\}$.

תורה T בשפה $\underline{L}(\tau)$ הינה שלמה אם לכל פסוק ψ ב-$\underline{L}(\tau)$ $\psi \in T$ או $\neg\psi \in T$.

הערה: לעיתים נאמר "T שלמה" ונתכוון ל-"$con(T)$ שלמה".

תרגילים - הגדרות בסיסיות בתורת המודלים

1. תהי $L = \langle +,\cdot,0,1 \rangle$ השפה של תורת החוגים.

א. כתבו פסוקים ב-L המבטאים את הטענות הבאות:

i) העולם הוא שדה.

ii) העולם הוא שדה ממצין $p>0$.

iii) העולם הוא שדה ממצין 0.

iv) העולם הוא שדה בו יש שורש למשוואה $x^2 = -1$.

ב. כתבו פסוק ב-L האומר שלכל פולינום ממעלה 2 יש שורש. כתבו פסוק האומר שכל פולינום ממעלה 2 מתפצל (כלומר מתפרק לגורמים לינארים).

ג. כתבו פסוק האומר שלכל פולינום ממעלה 7 יש בדיוק 7 שורשים.

ד. כתבו פסוק (או קבוצת פסוקים) האומרים שהשדה סגור אלגברית (כלומר שלכל פולינום יש שורש בשדה).

2. תהי $L = \langle \in \rangle$, שפת תורת הקבוצות.

א. כתבו במילים את משמעות האקסיומות הבאות:

i) $(\exists x \forall y)(y \notin x)$. הערה: הסימון $y \notin x$ הוא קיצור לנוסחה $\neg(y \in x)$.

ii) $(\forall x \forall y)(x = y \leftrightarrow (\forall z)(z \in x \leftrightarrow z \in y))$.

iii) $(\forall x \exists y \forall z)(z \in y \leftrightarrow z \subseteq y)$. הערה: מצאו נוסחה ב-$L$ השקולה ל- $z \subseteq y$.

iv) $(\forall x \forall y \exists z \forall s)(s \in z \leftrightarrow s = y \vee s = x)$.

v) $(\forall x \exists y \forall z)(z \in y \leftrightarrow (\exists s)(s \in x \wedge z \in s))$.

vi) $(\forall x \exists y)(y \in x \wedge y \cap x = \phi)$. הערה: ϕ היא הקבוצה הריקה. מדוע ניתן לכתוב את הפסוק האחרון ב-L.

vii) לכל נוסחה φ בשפה L הפסוק: $(\forall x \exists y \forall z)(z \in y \leftrightarrow (\varphi(z) \wedge z \in x))$.

ב. כתבו פסוקים מסדר ראשון ב-L המבטאים את הטענות הבאות:

i) קיימת קבוצה תורשתית (=טרנזיטיבית), כלומר, קבוצה שכל איבר שלה הוא גם תת קבוצה שלה.

ii) f היא פונקציה. הערה: תוכלו להניח שניתן להגדיר ב-L, זוג סדור, איבר ראשון בזוג סדור ואיבר שני בזוג סדור. סמנו ב- $z = (x, y)$ את הנוסחה האומרת ש-z זוג סדור שאיברו הראשון x ואיברו השני y.

iii) אקסיומת הבחירה.

iv) אם f פונקציה והתחום של f הוא קבוצה אז כך גם הטווח של f.

הערה: הפסוקים הנ"ל (לבד מזה המופיע בסעיף ב-2) הם מערכת האקסיומות המקובלת לתורת הקבוצות - האקסיומות של צרמלו-פרנקל - ומסומנות בקיצור ZFC.

3. הוכיחו שלכל מבנה M התורה של M ($\mathrm{Th}(M)$) שלמה.

4. הגדרה: יהיו M,N מבנים לשפה L. נאמר שפונקציה $f : M \to N$ היא איזומורפיזם אם:

i. f חח"ע ועל.

ii. לכל סימן יחס $R \in \tau$ מתקיים $M \models R(a_1 \ldots a_n) \Leftrightarrow N \models R(f(a_1) \ldots f(a_n))$.

iii. לכל סימן פונקציה $F \in \tau$ מתקיים
$M \models F(a_1 \ldots a_n) = b \Leftrightarrow N \models F(f(a_1) \ldots f(a_n)) = f(b)$.

במקרה זה נסמן $M \cong N$.

הוכיחו את משפט האיזומורפיזם: יהיו M,N מבנים לשפה L, ויהי $f : M \to N$ איזומורפיזם, אזי לכל פסוק $\varphi \in L$ מתקיים $M \models \varphi \Leftrightarrow N \models \varphi$. יתר על כן, אם $\varphi \in L(M)$, כלומר

$\varphi = \varphi(\bar{a})$, באשר $\varphi(\bar{x}) \in L$ נוסחה, ו- $\bar{a} \in M$ n-ית איברים באורך של $\bar{x}$) אזי $M \models \varphi(\bar{a}) \Leftrightarrow N \models \varphi(f(\bar{a}))$. הסיקו בפרט, שאם M ו-N מבנים לשפה L וקיים $\varphi \in L$ כך ש- $N \models \varphi$ אבל $M \models \neg\varphi$ אז M ו-N אינם איזומורפיים.

5. תהי L שפה בת מניה כלשהי. הוכיחו שמספר המבנים הלא איזומורפיים ל-L שעולמם בן מניה הוא לכל היותר $2^{\aleph_0}$.

6. תהי $L=\{<\}$ שפה עם סימן יחס דו מקומי יחיד.

א. כתבו את האקסיומות האומרות ש-< סדר קווי (=מלא). נקרא לתורה זו TL.

ב. הראו ש-Q ו-N אינם איזומורפיים כמודלים של TL.

ג. הוכיחו כי ל-TL $2^{\aleph_0}$ מודלים בני מניה שאינם איזומורפיים. הדרכה: העזרו בסעיף ב' כדי להתאים לכל סדרה בינרית מודל, כך שמודלים המתאימים לסדרות שונות אינם איזומורפיים.

7. תהי $L=\{0,S\}$. באשר 0 קבוע אישי ו-S פונקציה חד-מקומית, שתקרא פונקצית העוקב.

א. כתבו ב-L מערכת אקסיומות מסדר ראשון, האומרת ש:

i. S פונקציה חח"ע.

ii. כל איבר פרט לאפס הוא עוקב.

iii. ב-S אין מעגלים (כלומר, אם נתחיל מאיבר כלשהו x ונתקדם רק תוך שימוש ב-S לא נוכל לחזור ל-x).

נסמן תורה זו ב-TS.

ב. לכל n טבעי מצאו מודל $M_n \models T_S$ כך ש- $M_n \cong M_m \Leftrightarrow m = n$.

ג. הוכיחו כי ל-TS מספר בן מניה של מודלים בני מניה עד כדי איזומורפיזם.

8. תהי T תורה כלשהי. נניח שלכל $M,N \models T$ אם $||M||=||N||$ (עצמת M שווה לעצמת N) אז $M \cong N$, אזי T תורה שלמה. הדרכה: השתמשו במסקנה 3.4.14.

3.1 תת מודלים והרחבות

3.1.1 הגדרה:

(1) נאמר כי M_0 **תת מודל (או תת מבנה)** של M_1 ונסמן $M_0 \subseteq M_1$ אם

א. M_0 מבנה למילון τ_0, M_1 מבנה למילון τ_1 ו-$\tau_0 = \tau_1$.

ב. לכל סימן יחס n-מקומי R ב-τ_0, $R^{M_0} = R^{M_1} \upharpoonright M_0$, כלומר לכל $a_0,a_1,...,a_{n-1}$ ב-מתקיים: $(a_0,...,a_{n-1}) \in R^{M_0} \Leftrightarrow (a_0,...,a_{n-1}) \in R^{M_1}$.

ג. לכל סימן פונקציה n- מקומי F ב-τ_0, $F^{M_0} = F^{M_1} \upharpoonright M_0$, לומר לכל $a_0,a_1,...,a_{n-1}$ ב-M_0 מתקיים: $F^{M_0}(a_0,...,a_{n-1}) = F^{M_1}(a_0,...,a_{n-1})$ (ויוצא כי $F^{M_1}(a_0,...,a_{n-1}) \in M_0$).

לחילופין, נאמר ש-M_1 **הרחבה** של M_0.

(2) יהי M מבנה למילון τ, ו- $|M| \supseteq A$ (כלומר קבוצה של אברים של M). משמעות $M_0 = M \upharpoonright A$ היא כי M_0 מבנה למילון τ, $M_0 \subseteq M$ ו-$|M_0|$ (עולמו של M_0, הוא A).

3.1.2 משפטון: נניח כי

i. $M \subseteq N$.

ii. $\vartheta(\bar{x})$ שם עצם בשפת M.

iii. $\bar{a}$ סדרת אברים של M באורך של $\bar{x}$.

אז $\vartheta^M(\bar{a}) = \vartheta^N(\bar{a})$.

הוכחה: באינדוקציה על שם העצם ϑ.

3.1.3 משפטון: יהיו M מבנה ו-A קבוצה אזי התנאים הבאים שקולים:

(1) $M \upharpoonright A$ מוגדר היטב.

(2) יש ל-M תת מודל M_0 שעולמו A.

(3) A קבוצה לא ריקה של אברים של M ולכל סימן פונקציה F במילון של M, A סגורה תחת F, כלומר, אם F סימן פונקציה n-מקומי אז $a_0,...,a_{n-1} \in A \Rightarrow F^M(a_0,...,a_{n-1}) \in A$.

הוכחה: תרגיל.

3.1.4 משפטון:

(1) "תת מודל" הוא יחס סדר חלקי, כלומר: אם $M_0 \subseteq M_1$ וגם $M_1 \subseteq M_2$ אז $M_0 \subseteq M_2$ ובנוסף, לכל מבנה M $M \subseteq M$.

(2) אם I סדר קווי (=ליניארי) נתון, לכל $t \in I$ M_t מבנה כך ש- $M_s \subseteq M_t \Leftarrow s <_I t$

אז יש מבנה אחד ויחיד M כך ש:

א. המילון τ של M הוא המילון של כל M_t (אלו זהים כי $\tau(M_s) = \tau(M_\ell) \leftarrow M_s \subseteq M_t$).

ב. עולמו של M הוא $\bigcup\{|M_t|:\{t\in I\}$.

ג. לכל סימן יחס R מהמילון τ $R^M=\bigcup\{R^{M_t}:t\in I\}$.

ד. לכל סימן פונקציה F מהמילון τ, $F^M(\bar{a})=b\Leftrightarrow(\exists t\in I)[F^{M_t}(\bar{a})=b]$.

בחלק (2) מספיק ש- I סדר מכוון (כלומר לכל s,t ב-I יש איבר r של I המקיים $s\le_I r,\ t\le_I r$).

<u>הוכחה</u>: תרגיל.

<u>3.1.5 סימון</u>: אם $\langle M_t:t\in I\rangle$ כמו ב-3.1.4 נסמן $M=\bigcup\{M_t:t\in I\}$.

<u>3.1.6 דוגמה</u>: יהי $\tau=\{<\}$, $<$ סימן יחס דו מקומי. לטבעי n נגדיר מבנה M_n: עולמו הרציונליים הגדולים מ- $n-1$ ו- $<^{M_n}$ הוא הסדר הרגיל. נקבל ש- $M_n\subseteq M_{n+1}$, M_n מספק את הפסוק האומר שיש אבר ראשון בסדר: $\psi=(\exists x)(\forall y)(x=y\vee x<y)$,

אבל $M=\bigcup\{M_n:n\}$, שהוא המבנה שעולמו הרציונליים ו- $<^M$ הוא הסדר הרגיל, אינו מקיים זאת.

<u>3.1.7 הגדרה</u>: נאמר כי M_0 **תת מודל אלמנטרי** של M_1, ונסמן $M_0\prec M_1$ אם

א. $M_0\subseteq M_1$.

ב. לכל נוסחה $\varphi(\bar{x})=\varphi(x_0,\dots,x_{n-1})$ בשפה $\underline{L}(\tau_{M_0})$ ולכל $a_0,\dots,a_{n-1}\in M_0$ מתקיים $M_0\models\varphi[a_0,\dots,a_{n-1}]$ אסם $M_1\models\varphi[a_0,\dots,a_{n-1}]$.

<u>3.1.8 משפטון</u>: $\prec$ סדר חלקי.

<u>הוכחה</u>: תרגיל.

<u>3.1.9 משפט (מבחן *Tarski-Vaught*)</u>: $M\prec N$ אסם מתקיימים שני התנאים הבאים:

i. $M\subseteq N$.

ii. לכל נוסחה $\varphi(y,\bar{x})$ (בשפה של M) וסדרה $\bar{a}$ מהמבנה M (באורך של $\bar{x}$) ואיבר b של N יש אבר c של M כך ש- $N\models\varphi(b,\bar{a})\to\varphi(c,\bar{a})$.

נקרא ל-(*i*) ו-(*ii*) תנאי טרסקי-ווט.

<u>3.1.10 תרגיל</u>: ניסוח שקול של תנאי (*ii*) הוא:

iii. לכל נוסחה $\varphi(y,\bar{x})$ וסדרה $\bar{a}$ מהמבנה M (באורך של $\bar{x}$) כך ש- $N\models(\exists x)\varphi(x,\bar{b})$ יש אבר c של M כך ש: $N\models\varphi(c,\bar{b})$ (הסיבה היא שאם $N\models\neg(\exists x)(\varphi(x,\bar{a})$, הנטען ב-(*ii*) וגם ב-(*iii*) מתקיים באופן מנוון).

<u>הוכחת משפט טרסקי-ווט</u>:

בכיוון אחד: נניח כי $M\prec N$ ונוכיח את המבחן. תנאי (*i*) פשוט כלול בהגדרת $M\prec N$. לגבי תנאי (*ii*), נניח כי נתונים $\varphi(y,\bar{x})$, $\bar{a}$ ואבר b כנדרש בתנאי. אם $N\models\neg\varphi(b,\bar{a})$ נבחר אבר c כלשהו של N (נזכור כי כל מבנה עולמו אינו ריק ולכן יש c כזה). עתה $N\models\varphi(b,\bar{a})\to\varphi(c,\bar{a})$ כי הרישא שקרית. לכן נניח כי $N\models\varphi(b,\bar{a})$. לכן לפי הגדרת הסיפוק

קיים $N \models (\exists x)(x,\bar{a})$. כיון ש- $M \prec N$ (לפי הנחתנו) ו- $\bar{a}$ סדרה מהמבנה M, בהכרח $M \models (\exists y)\varphi(y,\bar{a})$. לפי הגדרת הסיפוק יש אבר c של M כך ש- $M \models \varphi(c,\bar{a})$. עתה לפי הגדרת $M \prec N$ נובע כי $N \models \varphi(c,\bar{a})$. לפי הגדרת הסיפוק נובע כי $N \models \varphi(b,\bar{a}) \to \varphi(c,\bar{a})$.

בכיוון השני: נניח כי תנאי טרסקי-ווט מתקיים, ונוכיח כי $M \prec N$. בהגדרת $M \prec N$ החלק הראשון $M \subseteq N$ נתון. עתה עלינו להראות שלכל נוסחה $\varphi(\bar{x})$ בשפת M ולכל סדרה $\bar{a}$ מהמבנה M באורך של $\bar{x}$ $M \models \varphi[\bar{a}] \Leftrightarrow N \models \varphi[\bar{a}]$. נוכיח זאת באינדוקציה על φ.

מקרה א: φ נוסחה אטומית, מהצורה $\varphi = [\vartheta_1 = \vartheta_2]$. לכן $\varphi(\bar{x}) = [\vartheta_1(\bar{x}) = \vartheta_2(\bar{x})]$. לפי משפטון 3.1.2 אנו יודעים כי $\vartheta_1^M[\bar{a}] = \vartheta_1^N[\bar{a}]$ וכן $\vartheta_2^M[\bar{a}] = \vartheta_2^N[\bar{a}]$.

עתה

$M \models \varphi[\bar{a}] \Leftrightarrow$

לפי הצגת φ $\quad M \models \vartheta_1[\bar{a}] = \vartheta_2[\bar{a}] \Leftrightarrow$

לפי הגדרת הסיפוק $\quad \vartheta_1^M[\bar{a}] = \vartheta_2^M[\bar{a}] \Leftrightarrow$

לפי השוויונות לעיל $\quad \vartheta_1^N[\bar{a}] = \vartheta_1^M[\bar{a}] = \vartheta_2^M[\bar{a}] = \vartheta_2^N[\bar{a}] \Leftrightarrow$

לפי תכונות השוויון $\quad \vartheta_1^N[\bar{a}] = \vartheta_2^N[\bar{a}] \Leftrightarrow$

לפי הגדרת הסיפוק $\quad N \models \vartheta_1[\bar{a}] = \vartheta_2[\bar{a}] \Leftrightarrow$

לפי הצגת φ $\quad N \models \varphi[\bar{a}]$

מקרה ב: φ נוסחה אטומית אחרת, כלומר, יש סימן R במילון של M כך ש- $\varphi = R(\vartheta_0,\dots,\vartheta_{n-1})$ כאשר $\vartheta_0,\dots,\vartheta_{n-1}$ הם שמות עצם, לכן $\varphi(\bar{x}) = R(\vartheta_0(\bar{x}),\vartheta_1(\bar{x}),\dots,\vartheta_{n-1}(\bar{x}))$. נסמן $b_m = \vartheta_m^M(\bar{a})$, לפי משפטון 3.1.2 מתקיים $b_m = \vartheta_m^N[\bar{a}]$ לכל $0 \le m \le n-1$.

עתה:

$M \models \varphi[\bar{a}] \Leftrightarrow$

לפי הצגת φ $\quad M \models R[\vartheta_0[\bar{a}],\dots,\vartheta_{n-1}[\bar{a}]] \Leftrightarrow$

כי $b_m = \vartheta_m^M[\bar{a}]$ $\quad M \models R[b_0,\dots,b_{n-1}] \Leftrightarrow$

לפי הגדרת הסיפוק $\quad (b_0,\dots,b_{n-1}) \in R^M \Leftrightarrow$

כי $M \subseteq N$ (M תת-מבנה של N) $\quad (b_0,\dots,b_{n-1}) \in R^N \Leftrightarrow$

כי $b_m = \vartheta_m^N[\vartheta]$ $\quad N \models R[b_0,\dots,b_{n-1}] \Leftrightarrow$

לפי הצגת φ $\quad N \models R[\vartheta_0[\bar{a}],\dots,\vartheta_{n-1}[\bar{a}]] \Leftrightarrow$

$N \models \varphi[\bar{a}]$

ובסה"כ סיימנו מקרה זה.

מקרה ג': $\varphi = \neg\psi$ לכן $\varphi(\bar{x}) = \neg\psi(\bar{x})$, ולכן

$M \models \varphi[\bar{a}] \Leftrightarrow$

לפי הצגת φ $\quad M \models \neg\psi[\bar{\vartheta}] \Leftrightarrow$

לפי הגדרת הסיפוק (לגבי $\neg$) $\Leftrightarrow$ "M אינו מספק את $\psi[\bar{a}]$"

לפי הנחת האינדוקציה $\Leftrightarrow$ "N אינו מספק את $\psi[\bar{a}]$"

לפי הגדרת הסיפוק (לגבי $\neg$) $\Leftrightarrow$ $N \models \neg\psi[\bar{\vartheta}]$

לפי הצגת φ $N \models \psi[\bar{\vartheta}]$

מקרה ד': $\psi = (\psi_1 \to \psi_2)$ (וכן שאר הקשרים הפסוקיים). הוכחה דומה בעזרת טבלת האמת של הקשר $\to$.

מקרה ה': $\varphi = \exists y\psi$

נרשום $\psi = \psi(y,\bar{x})$, וכיון שאפשר להשמיט מהסדרה $\bar{x}$ כל משתנה שאין לו הופעה חופשית ב-φ בה"כ y אינו מופיע ב-$\bar{x}$.

הכוון הקל:

נניח כי $M \models \varphi[\bar{a}]$, כלומר $M \models (\exists y)\psi(y,\bar{a})$ לכן לפי הגדרת הסיפוק יש אבר c של M כך ש-$M \models \psi[c,\bar{a}]$. לפי הנחת האינדוקציה, מתקיים גם $N \models \psi[c,\bar{a}]$, ולכן לפי הגדרת הסיפוק $N \models (\exists y)\psi(y,\bar{a})$ כלומר $N \models \varphi[\bar{a}]$ כנדרש.

הכוון הקשה:

נניח כי $N \models \varphi[\bar{a}]$, כלומר $N \models (\exists y)\psi(y,\bar{a})$ לכן לפי הגדרת הסיפוק יש אבר b של N כך ש-$N \models \psi[b,\bar{a}]$. לפי תנאי טרסקי-ווט יש אבר c של M כך ש- $N \models \psi[b,\bar{a}] \to \psi[c,\bar{a}]$. כיוון ש-$N \models \psi[b,\bar{a}]$, נובע כי $N \models \psi[c,\bar{a}]$. כיוון ש-$\bar{a}$ ו-c הם מהמבנה M נובע לפי הנחת האינדוקציה כי $M \models \psi[\bar{a}]$. לפי הגדרת הסיפוק נובע $M \models (\exists y)\psi(y,\bar{a})$ כלומר $M \models \varphi[\bar{a}]$ כנדרש. ■

תת-מודלים והרחבות - תרגילים:

1. יהי ω הסודר האינסופי הראשון. נחשוב על ω כעל מבנה לשפה L שבה סימן יחס דו מקומי אחד, $<$.
   א. הראו ש-ω ו-$\omega+\omega$ מודלים של התורה האומרת ש-$<$ סדר קווי (=סדר מלא).
   ב. הראו ש-ω אינו איזומורפי ל-$\omega+\omega$.
   ג. האם ω תת מודל אלמנטרי של $\omega+\omega$.
   ד. האם $Th(2N,<) \cong Th(N,<)$, האם הם שקולים אלמנטרית (ראו תרגיל 2).
   ה. הראו שהתורה האומרת ש-$<$ סדר קווי אינה שלמה.
2. הגדרה: יהיו A,B מבנים לשפה L. נאמר ש-A ו-B שקולים אלמנטרית, אם לכל פסוק $\varphi \in L$ מתקיים $A \models \varphi \Leftrightarrow B \models \varphi$. נסמן $A \equiv B$.
   א. הוכיחו כי $\equiv$ אמנם יחס שקילות.
   ב. הוכיחו שתורה T היא שלמה אסם לכל $A,B \models T$ מתקיים $A \equiv B$.
   ג. הוכיחו שאם $A \prec B$ אז $A \equiv B$.
   ד. תנו דוגמה למבנים $A \subseteq B$, $A \equiv B$ אבל לא $A \prec B$.

ה. תנו דוגמה למבנים כבסעיף ג' כך שלא מתקיים $A \cong B$.

ו. תנו דוגמה למבנים A,B כך ש-A תת מבנה של B, אך לא תת מבנה אלמנטרי, אבל כן מתקיים ש- $A \cong B$.

3. הגדרה: תהי T תורה מסדר ראשון. נאמר ש-T שלמה מודלית אם לכל שני מודלים A ו-B של T, אם $A \subseteq B$ אז $A \prec B$.

א. הוכיחו שאם ל-T יש חילוץ כמתים (כלומר, לכל $\varphi \in L$ יש $\psi \in L$ ללא כמתים כך ש- $T \vdash \psi \leftrightarrow \varphi$) אזי T שלמה מודלית.

ב. האם תורה שלמה מודלית בהכרח שלמה.

ג. תהי L השפה הריקה (עם סימן השוויון). כתבו תורה T האומרת שהעולם אינסופי (תורה זו תקרא תורת השוויון הטהור). הוכיחו כי לתורה T יש חילוץ כמתים. הסיקו שאם $M \models T$ אז לכל M,N עם $|N| \subseteq |M|$ אינסופי מתקיים $A \prec B$.

ד. *האם $Q \prec R$ כמודלים של תורת הסדר. רמז: זכרו שכל נוסחה חסרת כמתים ניתן לכתוב בצורת *DNF*. הסיקו שב-Q כל נוסחה מהצורה $\exists x \varphi(x,y)$ כאשר $\varphi(x,y)$ ללא כמתים שקולה לאיזו נוסחה $\psi(y)$ ללא כמתים.

4. הגדרה: נאמר שלתורה T יש פונקציות סקולם *(Skolem)* אם לכל נוסחה $\varphi(x,y)$ (x,y אולי n-יות) יש פונקציה בסיסית f_φ (כלומר, f_φ סימן פונקציה בשפה) כך ש- $T \vdash \forall x[\exists y(\varphi(x,y) \to \varphi(x, f_\varphi(x))]$. הוכיחו שאם ל-$T$ יש פונקציות סקולם אז לכל זוג מודלים M ו-N של T, אם N תת מודל של M אז $N \prec M$.

5. יהי N מבנה לשפה L. נסמן $L' = L \cup \{c_a : a \in N\}$, כלומר, השפה המועשרת בקבוע אישי עבור כל איבר ב-N. תהי $\Gamma_N = \{\varphi \in L' : N \models \varphi\}$.

א. הוכיחו כי $N \prec M$ אסם $(M,a)_{a\in N} \models \Gamma_N$ באשר $(M,a)_{a\in N}$ הוא ההרחבה של המבנה M לשפה L'.

ב. יהיו $N \equiv M$. הוכיחו כי $\Gamma_N \cup \Gamma_M$ עקבית. הסיקו שיש מבנה A, כך ש-N,M משוכנים אלמנטרית ב-A (ראו הגדרה 3.3.2). רמז: וודאו שהקבועים החדשים שהוספתם ב- Γ_N שונים מאלו שהוספתם ב- Γ_M, והשתמשו במשפט הקומפקטיות (משפט 3.0.6).

3.2 קבלת מודלים

נחזור עתה לדוגמה 3.1.6. המשפט הבא מראה כי ההגדרה של תת-מודל אלמנטרי היא ההגדרה הנכונה הנדרשת על מנת למנוע דוגמאות ממין זה.

3.2.1 משפט השרשרת העולה: נניח כי I סדר קוי או לפחות מכוון, $\langle M_t : t \in I \rangle$ סדרה עולה של מבנים (ראו 3.1.4). נניח עוד שזו שרשרת אלמנטרית, כלומר, $M_s \prec M_t \leftarrow s <_I t$, ויהי $M = \bigcup\{M_t : t \in I\}$ אז $M_s \prec M$ לכל אבר s של I.

הוכחה: אנו יודעים מ-3.1.4 כי $M_t \subseteq M \Leftarrow t \in I$. לכן מספיק להוכיח:

(*) אם $\varphi = \varphi(\bar{x})$ נוסחה בשפת M, $\bar{a}$ סדרה מהמבנה M_t (באורך של $\bar{x}$, כמובן) אז $M \models \varphi[a] \Leftrightarrow M_t \models \varphi[\bar{a}]$. נוכיח זאת באינדוקציה על הנוסחה $\varphi[\bar{x}]$.

מקרה א: φ אטומית: כלול בהוכחת 3.1.8 (מבחן טרסקי-ווט).

מקרה ב: $\varphi = \neg\psi$ או $\varphi = [\psi_1 \to \psi_2]$ כנ"ל.

מקרה ג: $\varphi = \exists y \psi$. כמו בהוכחת 3.1.8 נכתוב $\psi = \psi(y,\bar{x})$ וב.ה.כ. y אינו מופיע ב- $\bar{x}$.

הכוון הקל: נניח כי $M_t \models \varphi[\bar{a}]$ כלומר $M_t \models \exists y \psi(y,\bar{a})$. לפי הגדרת הסיפוק יש אבר $b \in M_t$ כך שמתקיים $M_t \models \psi(b,\bar{a})$. לפי הנחת האינדוקציה $M \models \psi(b,\bar{a})$ לכן לפי הגדרת הסיפוק $M \models (\exists y)\psi(y,\bar{a})$ כלומר $M \models \varphi[\bar{a}]$ כנדרש.

הכוון הקשה: נניח כי $M \models \varphi[\bar{a}]$ כלומר. $M \models (\exists y)\psi(y,\bar{a})$ לפי הגדרת הספוק יש אבר b של M כך ש- $M \models \psi(b,\bar{a})$. אבל $M = \bigcup\{M_s : s \in I\}$ ולכן יש $s \in I$ כך ש $b \in M_s$. יהי r אבר של I המקיים $s \le_I r$ וגם $t \le_I r$ (יש כזה משום ש-I סדר מכוון). לכן $b \in M_s \subseteq M_r$. $\bar{a}$ סדרה מהמבנה M_t ולכן מ-M_r, ומכיוון שגם b הוא מהמבנה M_r לפי הנחת האינדוקציה (כיון ש-$M \models \psi(b,\bar{a})$) מתקיים גם $M_r \models \psi(b,\bar{a})$. לפי הגדרת הסיפוק $M_r \models (\exists y)\psi(y,\bar{a})$ אבל $t \le_I r$ לכן $M_t \prec M_r$ (זכרו כי תמיד $M \prec M$). לפי הגדרת $\prec$ נובע כי $M_t \models (\exists y)\psi(y,\bar{a})$ כלומר $M_t \models \varphi[\bar{a}]$, כנדרש. ■

3.2.2 משפט לוונהים סקולם היורד: יהי M מודל במילון τ, A תת קבוצה של M, אזי קיים N המקיים:

i. $N \prec M$.

ii. $A \subseteq N$.

iii. $\|N\| \le |\tau| + |A| + \aleph_0$.

הערות:

(1) $|A|$ הוא מספר אברי הקבוצה A, מספר שיכול להיות מונה אינסופי. קורא שאינו מכיר מושג זה יכול להניח כי A סופית או בת מניה, המילון τ הוא בן מניה, והמודל N המובטח במסקנת המשפט הוא בן מניה (כלומר, עולמו קבוצה בת מניה).

(2) $\|N\|$ זה מספר אברי הקבוצה N, יקרא גם עצמת N.

(3) מחשבון מונים נשתמש רק במשפטים הבאים:

א. עצמת האחוד קטנה או שווה לסכום עצמות המאוחדים.

ב. $\aleph_0 + \lambda^2 = \lambda$ לכל מונה אינסופי λ.

<u>הוכחת משפט לוונהים סקולם היורד</u>:

בהיתן הקבוצה A נבנה את המודל N כנדרש. הרעיון הוא שלפי קריטריון טרסקי-ווט בכדי לבנות תת מודל אלמנטרי של M המכיל את A מספיק להוסיף ל-A עדים לנוסחאות (עם פרמטרים מ-A) המוגשמות ב-M וחוזר חלילה. נעשה זאת בשלבים, ובכל שלב נדאג שלא להגדיל את עצמת הקבוצה המתקבלת.

ראשית, נבנה את המודל: נגדיר באינדוקציה על הטבעי n קבוצה A_n באופן הבא:

ל-$n=0$ $A_0 = A$.

ל-$n = m+1$: לכל נוסחה $\varphi(y,\bar{x})$ בשפת M וסדרה $\bar{a}$ מ-A_m באורך של $\bar{x}$ נבחר אבר $b_{\varphi(y,\bar{a})} \in M$ כך ש-$M \models (\exists y)\varphi(y,\bar{a}) \to \varphi(b_{\varphi(y,\bar{a})},\bar{a})$. לפי הגדרת הסיפוק והקשר $\to$ זה אפשרי. נגדיר $A_{m+1} = A_m \cup \{b_{\varphi(\bar{y},\bar{a})}$ כנ"ל: $\varphi(y,\bar{x})$ ו- $\bar{a}\}$.

יהי $A^* = \bigcup\{A_m : m \in \mathbf{N}\}$. נראה ש-$A^*$ עונה על הדרישות.

באינדוקציה על m נקבל: $(*)_0$ $A_k \subseteq A_m$ לכל $k < m$.

$(*)_1$ A^* תת קבוצה של M.

כיוון ש-$M \models (\exists y)(y = y)$ יש b ב-$A^* \supseteq A_1$, כלומר,

$(*)_2$ A^* אינה ריקה.

$(*)_3$ אם F סימן פונקציה k-מקומי במילון של M ו-$a_0,\dots,a_{k-1},\in A^*$ אז $F^M(a_0,\dots,a_{k-1}) \in A^*$. (לכל $k > \ell$, a_ℓ ב-A^* ולכן יש n_ℓ עבורו $a_\ell \in A_{n(\ell)}$. יהי $n^* = \max\{n(0),\dots,n(k-1)\}$, ברור כי n^* מוגדר והוא טבעי. לפי $(*)_1$ אנו יודעים כי $a_0,\dots,a_{k-1} \in A_{n^*}$. תהי $\varphi(y,\bar{x}) = [y = F(x_0,\dots,x_{k-1})]$ ולכן $b_{\varphi(x,<a_0\dots a_{k-1}>)}$ מוגדר היטב ושייך ל-A_{n^*+1} ולכן ל-A^*, והוא שווה ל-$F^M(a_0,\dots,a_h)$).

מ-$(*)_3$ וממשפטון 3.1.4 נקבל:

$(*)_4$ יש תת מודל N של M, שעולמו A^*.

$(*)_5$ אם $\varphi(y,\bar{x})$ נוסחה במילון של M, $\bar{a}$ סדרה מ-A^* באורך של $\bar{x}$ ו-c ב-M אז יש b ב-A^* כך ש-$M \models \varphi(b,\bar{a}) \to \varphi(c,\bar{a})$. (כמו בהוכחת $(*)_3$, יש n^* כך ש $\bar{a}$ הינה סדרה מהקבוצה A_{n^*}. לכן $b_{\varphi(y,\bar{a})}$ מוגדר היטב, וברור שהוא כנדרש).

לפי $(*)_4$, $(*)_5$ ומבחן טרסקי-ווט נקבל גם:

$(*)_6$ $N \prec M$.

נותר לוודא ש-$(*)_7$ $\|N\| \le |\tau| + |A| + \aleph_0$:

נסמן $\lambda = |\tau| + |A| + \aleph_0$. נוכיח באינדוקציה על n כי $|A_n| \le \lambda$.

עבור $n = 0$ זה נכון כי $|A_0| = |A| \le \lambda$ לפי בחירת A_0 ו- λ. עבור $n = m + 1$: מספר הנוסחות $\varphi(y, \bar{x})$ בשפה L_M אינו גדול ממספר הסדרות הסופיות שאבריהן מ- τ או מבין $X \cup \{\exists, \forall, \neg, \to, \wedge, \vee, (,)\} \cup \tau$ (כאשר X קבוצת המשתנים החופשיים, שהיא בת מנייה) מספר אברי הקבוצה הזאת $\lambda \ge \aleph_0 + |\tau| \ge$.

מספר הסדרות באורך n של אברים מקבוצה זאת הוא λ^n, ומספר כל הסדרות הסופיות מקבוצה זו הוא $\sum_{\aleph \in N} \lambda^{\aleph}$, אך לכל n, $\lambda^n = \lambda$ (כי λ מונה אינסופי) ולכן סכום זה קטן או שווה ל- $\sum_{\aleph \in N} \lambda = \lambda \times \aleph_0 \le \lambda \times \lambda = \lambda^2 = \lambda$.

כמו כן מספר הסדרות הסופיות מ- A_m גם הוא $\ge \lambda$. לכן מספר האפשרויות $\varphi(y, \bar{a})$ קטן או שווה ל- $\lambda = \lambda \times \lambda$.

ולכן

$$|A_{m+1}| = |A_m \cup \{b_{\varphi(y,\bar{a})} : \bar{x} \text{ באורך של } A_m \text{ - סדרה מ } \bar{a} \text{ , } L_M \text{ - נוסחה ב- } \varphi(y, \bar{x})\}| \le$$

$$\le |A_m| + \lambda \le \lambda + \lambda \le 2\lambda \le \lambda^2 = \lambda$$

יוצא כי אכן $\lambda \ge |A_m|$ לכל n. לכן

$$|A^*| = |\bigcup\{A_n : n \in N\}| \le \sum\{|A_n| : n \in N\} \le \sum\{\lambda : n \in |N|\} = \lambda \times \aleph_0 \le \lambda \times \lambda = \lambda`$$

כלומר אכן $|A^*| \le \lambda$ כנדרש. ■

תרגילים - קבלת מודלים

1. יהיו $A_0 \subseteq B_0$ מבנים לשפה L. נסמן $T_A = Th(A), T_B = Th(B)$, ונניח שלכל זוג מבנים $A \subseteq B$ המקיימים $A \models T_A$ ו- $B \models T_B$ יש $A' \supseteq B$ המקיים $A \prec A'$ ובאופן סימטרי לכל $B \subseteq A$ כמקודם יש $B' \supseteq A$ המקיים $B \prec B'$, אזי $A_0 \prec B_0$ ובפרט $T_A = T_B$.
2. נציע הוכחה חלופית למשפט $L.S$ היורד:

א. הזכרו בהגדרה של תורה בעלת פונקציות סקולם (ראו תרגילים לסעיף תת-מודלים) והוכיחו את משפט $L.S$ עבור תורה T בעלת פונקציות סקולם. הוכיחו שלכל תורה T יש תורה $T' \supseteq T$ המקיימת:

i) ל-T' יש פונקציות סקולם.

ii) כל מודל של T ניתן להרחבה למודל של T'.

הדרכה: בהנתן נוסחה $\varphi(x,y)\in L$ הוסיפו לשפה סימן פונקציה f_φ והגדירו $L^1_\varphi = L\cup\{f_\varphi\}$.

נסחו אקסיומה A^1_φ האומרת ש- f_φ פונקצית סקולם ל- φ. הגדירו $T^1_\varphi = T\cup\{A^1_\varphi\}$. הוכיחו שעבור תורה זו מתקיימת דרישה 2). המשיכו את התהליך את שתקבלו גם את 1).

ב. הסיקו את משפט $L.S$ היורד.

ג. הראו שלתורה T' שקיבלתם יש חילוץ כמתים, כלומר, לכל נוסחה $\varphi(\bar{x})\in L(T')$ יש נוסחה חסרת כמתים $\psi(x)\in L(T')$ השקולה לה ב-T, כלומר, $T'\vdash\forall\overline{x}(\varphi(\bar{x})\leftrightarrow\psi(\bar{x}))$.

ד. הראו שגם אם התורה T שהתחלנו ממנה שלמה התורה T' אינה בהכרח שלמה. האם להשלמה של T' יש פונקציות סקולם.

3. הגדרה: קבוצת נוסחאות $\Sigma(x)$ בשפה L במשתנה החפשי x (x אולי n-יה) תקרא **עקבית** אם יש מבנה M לשפה L ואיבר $a\in M$ כך ש- $M\models\sigma(a)$ לכל $\sigma\in\Sigma$. לקבוצת פסוקים כנ"ל נקרא גם **טפוס**, ולאיבר a כנ"ל נקרא **הגשמה** של הטפוס. קב' נוסחאות עקבית במשתנה החופשי x, $\Sigma(x)$, תקרא **שלמה** אם לכל נוסחה $\varphi(x)$ או ש- $\varphi(x)\in\Sigma(x)$ או ש- $\neg\varphi(x)\in\Sigma(x)$.

א. הוכיחו כי קבוצת נוסחאות היא עקבית אסם היא עקבית מקומית (כלומר כל תת קבוצה סופית של עקבית).

ב. הוכיחו כי לכל קבוצת נוסחאות עקבית $\Sigma(x)$ יש $\Sigma'(x)\supseteq\Sigma(x)$ שלמה. רמז: השתמשו ברעיון ההוכחה שבמשפט 3.4.4.

ג. תהי T תורה שלמה ו- $M\models T$. תהי $\Sigma(x)\supseteq T$ עקבית. הראו שיש $M\prec N$ המגשים את $\Sigma(x)$.

ד. השתמשו בסעיף ג' כדי להוכיח שיש מבנה $M\prec N$ בו מוגשמת כל קבוצת נוסחאות עקבית בשפה. הדרכה: מנו את כל קב' הנוסחאות ב-L והגשימו אותן זו אחר זו. השתמשו במשפט השרשרת האלמנטרית.

4. הגדרה: יהי M מבנה בשפה L, ויהי $a\in M$ (יתכן ש- a n-יה). **הטפוס של a** זו קבוצת כל הנוסחאות ב-L המוגשמות ע"י a: $tp(a)=\{\varphi(x):M\models\varphi(a)\}$.

א. הוכיחו ש-$tp(a)$ הוא טיפוס שלם (כלומר, קב' נוסחאות עקבית ושלמה) ושכל טיפוס שלם ניתן להציג כטיפוס של איבר (כלומר, בהנתן קב' נוסחאות עקבית ושלמה $\Sigma(x)$ יש מבנה M ואיבר a ב-M כך ש- $\Sigma(x)=tp(a)$.

ב. יהי M מבנה לשפה L ויהיו a,b ב-M. נניח שיש אוטומורפיזם σ של M (כלומר σ איזומורפיזם מ-M על עצמו) המקיים $\sigma(a)=b$, אזי $tp(a)=tp(b)$.

5.

א. יהי M מודל של התורה של שוויון טהור (ראו תרגילים לסעיף 3.1). תהי $a_1,\ldots,a_n$ n-ית איברים מ-M. מצאו תנאי הכרחי ומספיק כדי של-n-יה כלשהי $b_1,\ldots,b_n$ יתקיים $tp(a_1,\ldots,a_n)=tp(b_1,\ldots,b_n)$.

ב. נביט במבנה $(Q,<)$. יהיו $q_1 < \ldots < q_n$ ו- $p_1 < \ldots < p_n$ איברים כלשהם ב-Q. הוכיחו ש- $tp(p_1,\ldots,p_n) = tp(q_1,\ldots,q_n)$. רמז: זכרו שב-$(Q,<)$ כל נוסחה שקולה לנוסחה חסרת כמתים והשתמשו בסעיף ו'.

6. יהי $\Sigma(x)$ טיפוס בשפה L ו-M מבנה לשפה L. נאמר ש-$\Sigma(x)$ ספיקה מקומית ב-M, אם לכל תת קבוצה סופית $\Delta(x) \subseteq \Sigma(x)$ יש הגשמה ב-M. הוכיחו כי כל קבוצת פסוקים $\Sigma(x)$ ספיקה מקומית ב-M מוגשמת ב-M אם M מבנה סופי.

7. תהי T תורה בשפה L, $\Sigma(x)$ טפוס ב-L. נאמר ש-T מגשימה מקומית את $\Sigma(x)$, אם יש נוסחה $\varphi(x)$ ב-L כך ש:

- $T \cup \varphi(x)$ עקבית.
- לכל $\sigma(x) \in \Sigma(x)$ מתקיים $T \mid\!- \varphi(x) \to \psi(x)$.

אם T אינה מגשימה מקומית את $\Sigma(x)$ נאמר ש-T משמיטה מקומית את $\Sigma(x)$. הוכיחו ש-T משמיטה מקומית את $\Sigma(x)$ אם לכל נוסחה $\varphi(x)$ כך ש- $T \cup \varphi(x)$ עקבית יש נוסחה $\sigma(x) \in \Sigma(x)$ כך ש- $T \cup \{\varphi(x) \wedge \neg\sigma(x)\}$ עקבית.

א. הראו שאם T שלמה ול-T יש מודל המשמיט את $\Sigma(x)$ (כלומר $\Sigma(x)$ אינה מוגשמת באיזה מודל של T) אז T משמיטה מקומית את $\Sigma(x)$.

ב. תהי T שלמה בשפה בת מניה. הוכיחו שאם T משמיטה מקומית את $\Sigma(x)$ אז יש ל-T מודל המשמיט את $\Sigma(x)$. הדרכה:

i) הניחו לשם נוחות ש-$\Sigma(x)$ במשתנה אחד. (למה זה אינו מגביל את הכלליות).

ii) תהי $C = \{c_1, c_2, \ldots\}$ רשימה בת מניה של קבועים חדשים. הגדירו $L' = L \cup C$ ותהי $\{\varphi_i\}_{i=1}^{\infty}$ רשימה (בת מניה - מדוע) של כל הפסוקים ב-L'. בנו סדרה של תורות $T_0 \subseteq T_1 \subseteq \ldots$ המקיימות:

(1) לכל m התורה T_m היא הרחבה סופית (ועקבית, כמובן) של T ב-L'.

(2) או ש- $\varphi_m \in T_m$ או ש- $\neg\varphi_m \in T_m$.

(3) אם $\varphi_m = \exists x\, \psi(x)$ אז $\psi(c_p) \in T_{m+1}$, באשר c_p הקבוע החדש הראשון שטרם נעשה בו שימוש.

(4) יש נוסחה $\sigma(x) \in \Sigma(x)$ כך ש- $\neg\sigma(c_p) \in T_{m+1}$.

3.3 משפט רובינסון

3.3.1 טענה: נניח כי

i. $\tau \subseteq \tau'$ מילונים.

ii. M_0 מודל במילון τ'.

iii. M_1 מודל במילון τ.

iv. $(M_0 \uparrow \tau) \prec M_1$.

אז יש מודל M_2 במילון τ' כך ש- $M_0 \prec M_2, M_1 \prec (M_2 \uparrow \tau)$.

הוכחה: יהיו $\{\underline{c}_a : a \in M_1\}$ קבועים אישיים חדשים. נגדיר:

$$\tau_0 = \tau,\ \tau_1 = \tau \cup \{\underline{c}_a : a \in M_0\},\ \ \tau_2 = \tau \cup \{c_a : a \in M_1\}$$

$$\tau'_0 = \tau',\ \tau'_1 = \tau' \cup \{\underline{c}_a : a \in M_0\},\ \ \tau'_2 = \tau' \cup \{c_a : a \in M_1\}$$

ברור כי $\tau_0 \subseteq \tau_1 \subseteq \tau_2$ (כי $M_0 \subseteq M_1$) וכן $\tau'_0 \subseteq \tau'_1 \subseteq \tau'_2$ ולבסוף,

$\tau'_1 \cap \tau_2 = \tau_1,\ \ \tau'_0 \cap \tau_2 = \tau'_0,\ \tau'_0 \cap \tau_1 = \tau'_0$.

נגדיר את המודל M_0^+ כהעשרה של המודל M_0 למילון τ'_1 על ידי $\underline{c}_a^{M_0^+} = a$ לכל $a \in M_0$.

נגדיר את המודל M_1^+ כהעשרה של המודל M_1 למילון τ_2 על ידי $\underline{c}_a^{M_0^+} = a$ לכל $a \in M_1$.

ראשית, נזכור שלכל מבנה M במילון τ $Th(M) = \{\psi \in L(\tau) : M \models \psi\}$ היא תורה שלמה (ראו הגדרות 3.0.9 ו-3.0.10). שנית, נראה שאם $Th(M_0^+) \cup Th(M_1^+)$ עקבית טענתנו תוכח. יהי, אם כן, $N \models Th(M_0^+) \cup Th(M_1^+)$. בה"כ נוכל להניח ש- $M_1 \subseteq N$ ע"י שלכל $c_a \in \tau_1$ נפרש $c_a^N = a \in M_1$ (ראו גם טענה 3.3.3 להלן). עתה נגדיר $M_2 = N \uparrow \tau'$ (ברור שזה מוגדר היטב, שכן המילון של N הוא $\tau' \subseteq \tau_2 \cup \tau'_1$). נראה ש- M_2 עונה על הדרישות.

מהגדרת M_2 ברור שהוא במילון הנכון, ומן האמור לעיל $M_0 \subseteq M_2$ וכן $M_1 \subseteq M_2 \uparrow \tau$.

קל לבדוק שאם ψ פסוק ב- $L(\tau_i)$ אז צורתו היא $\varphi(\underline{c}_{a_0},\dots,\underline{c}_{a_{n-1}})$ כאשר $\varphi(x_0,\dots,x_{n-1})$ נוסחה בשפה $L(\tau_0)$, וכן $M_0 \models \varphi[a_0,\dots,a_{n-1}] \Leftrightarrow M_0^+ \models \varphi[\underline{c}_{a_0},\dots,\underline{c}_{a_{n-1}}]$.

לכן אם $\varphi(\bar{y})$ נוסחה ב- τ', $\bar{b}$ סדרה מהמבנה M_0 (באורך של $\bar{y}$) ונניח ש- $M_0 \models \varphi(b_0,\dots,b_{n-1})$ אז מהגדרת τ'_1 הנוסחה $\varphi(\underline{c}_{b_0},\dots,\underline{c}_{b_{n-1}})$ הינה במילון τ'_1 ולכן $\varphi(\underline{c}_{b_0},\dots,\underline{c}_{b_{n-1}}) \in Th(M_0^+)$ לכן יוצא כי $M_0 \prec M_2$. הוכחת החלק השני של המשפט ($M_1 \prec N \uparrow \tau$) דומה.

נותר, אם כן להראות ש- $Th(M_0^+) \cup Th(M_1^+)$ עקבית. לשם כך מספיק להוכיח כי בקבוצת הפסוקים $Th(M_0^+) \cup Th(M_1^+)$ אין סתירה, ומכיוון ששתי הקבוצות סגורות תחת חיתוך לוגי, מספיק - ממשפט

הקומפקטיות - להראות כי אם $\psi_1 \in Th(M_0^+)$ $\psi_2 \in Th(M_1^+)$ אז ל-$\{\psi_1,\psi_2\}$ יש מודל. לפיכך, יהי $\psi_2 = \varphi_2(\underline{c}_{a_1},...,\underline{c}_{a_{n-1}})$ כאשר $a_0,...,a_{n-1} \in M_1$, $\varphi \in L(\tau)$. בה"כ $a_m,...,a_{n-1}$ שייכים ל-M_0 ו-$a_0,...,a_{m-1}$ שייכים ל $M_1 \setminus M_0$. עתה $M_1 \models \varphi_2[a_0,...,a_{n-1}]$ (כי $\psi_2 \in Th(M_1^+)$). לכן $M_1 \models (\exists x_0)...(\exists x_{m-1})\varphi_2(x_0,...,x_{m-1},a_m...a_{n-1})$. כיוון ש-$\varphi_2$ ב $L(\tau)$ ו-$(M_0 \uparrow \tau) \prec M_1$ ברור כי $M_0 \models (\exists x_0),...,(\exists x_{m-1})\varphi_2(x_0,..,x_{m-1},a_m,...,a_{n-1})$ כך ש:

$M_0 \models \varphi_2[b_0,...,b_{m-1},a_m,...a_{n-1}]$ ל-$b_1,...,b_m$ מתאימים ב-$|M_0|$.

נעשיר את M_0^+ למודל M_0^* במילון τ_2' ע"י שנפרש $\underline{c}_a^{M_0^*} = b_\ell$ אם $a = a_\ell$ $(\ell \in \{0,..m-1\})$, ואם $a \in M_1 \setminus M_0 \setminus \{a_0,...,a_{m-1}\}$ אז $\underline{c}_a^{M_0^*}$ יהיה אבר כלשהו של M_0. ברור כי M_0^* הוא מודל של $\{\psi_1,\psi_2\}$, ולכן אמנם ב- $Th(M_0^+) \cup Th(M_1^+)$ אין סתירה. ■

3.3.2 <u>הגדרה</u>: f הוא שכון אלמנטרי של M בתוך N אם:

i. N,M מודלים למילון τ.

ii. f פונקציה מ-M (זאת אומרת $|M|$) לתוך N (ז"א $|N|$).

iii. לכל נוסחה $\varphi(x_0,...,x_{n-1})$ ב-$L(\tau)$ ואברים $a_0,....,a_{n-1}$ של M מתקיים:

$M \models \varphi(a_0,...,a_{n-1}) \Leftrightarrow N \models \varphi(f(a_0),...,f(a_{n-1}))$.

3.3.3 <u>משפטון</u>: נניח כי

i. M_0 מודל במילון τ, $\tau^+ = \{\underline{c}_a : a \in M_0\} \cup \tau$, M_0^+ ההעשרה של M_0 על ידי הפרוש $\underline{c}_a^{M_0^+} = a$.

ii. M_1^+ מודל של $T_0^+ = Th(M_0^+)$ במילון τ^+.

iii. $M_1 = M_1^+ \uparrow \tau$.

אז:

א. יש פונקציה אחת ויחידה f מ-M_0 ל-M_1 כך ש-$a \in M_0 \Leftarrow f(a) = \underline{c}_a^{M_1^+}$.

ב. פונקציה זו היא שכון אלמנטרי של M_0 ב-M_1.

ג. אם $a \in M_0 \Leftarrow a = \underline{c}_a^{M_1^+}$ אז $M_0 \prec M_1$.

<u>הוכחה</u>: מיידי מההגדרות ומהדרישה $f(a) = \underline{c}_a^{M_1^+}$. ■

3.3.4 <u>טענה</u>: נניח כי

i. $\tau_0 \subseteq \tau_1$ מילונים.

ii. M_0 מודל במילון τ_0.

iii. T תורה שלמה במילון τ_1.

iv. M_0 מודל של התורה $T \cap L(\tau_0)$.

אז יש ל-T מודל M_1 במילון τ_1 כך ש- $M_0 \prec (M_1 \uparrow \tau_0)$.

<u>הוכחה</u>: יהיו c_a ($a \in M_0$) קבועים אישיים חדשים, (וכמובן $\underline{c}_a \neq \underline{c}_b$ אם $a \neq b$). נגדיר מילונים נוספים $\tau_0^+ = \tau_0 \cup \{\underline{c}_a : a \in M_0\}$ ו- $\tau_1^+ = \tau_1 \cup \{\underline{c}_a : a \in M_0\}$. כמובן

$\tau_0^+ \cap \tau_1^+ = \tau_0^+$, $\tau_0^+ \cup \tau_1^+ = \tau_1^+$.

נגדיר מודל M_0^+ במילון τ_0^+ באופן הבא: $M_0^+ \uparrow \tau_0 = M_0$ ו- $\underline{c}_a^{M_0^+} = a$, לכל אבר a של M_0.

תהי $T_0^+ = Th(M_0^+) = \{\psi \in L(\tau_0^+) : M_0^+ \models \psi\}$.

נגדיר $T_2 = T \cup T_0^+$. בדומה להוכחת טענה 3.3.1 נקבל שב- T_2 אין סתירה (כאן משתמשים בשלמות T).

יהי M_1^+ מודל של T_2 (במילון τ_1^+). נשים לב שכיוון ש- $a_1 \neq a_2 \Leftarrow c_{a_1} \neq c_{a_2}$ ב T_0^+ יצא כי $a_1 \neq a_2 \Leftarrow \underline{c}_{a_1}^{M_1^+} \neq \underline{c}_{a_2}^{M_1^+}$. לכן על ידי שינוי שמות, נוכל להניח בה"כ $\underline{c}_a^{M_1} = a$. יהי עתה $M_1 = M_1^+ \uparrow \tau_1$, ונוכיח כי M_1 הוא כנדרש, כלומר, M_1 מודל במילון τ_1 ו- $M_0 \prec M \uparrow \tau_0$. M_1 הוא כמובן במילון הנכון τ_1, כמו כן M_1 הוא מודל של T. בנוסף, $M_1 \uparrow \tau_0 = \left(M_1^+ \uparrow \tau_0^+\right) \uparrow \tau_0$, וכמו כן $M_1^+ \uparrow \tau_0^+$ הוא מודל של $T_0^+ = Th(M_0^+)$ לכן הטענה נובעת מטענות 3.3.1 ו- 3.3.3 . ■

<u>3.3.5 משפט רובינסון</u>: נניח כי

i. τ_0, τ_1, τ_2 הם מילונים.

ii. $\tau_0 = \tau_1 \cap \tau_2$.

iii. T_ℓ הינה תורה שלמה במילון τ_ℓ (ל- $\ell = 0,1,2$) ו - $T_0 = T_1 \cap T_2$.

אז לתורה $T_1 \cup T_2$ יש מודל (במילון $\tau = \tau_1 \cup \tau_2$).

<u>הוכחה</u>: אנו נבחר באינדוקציה על הטבעי n מודל M_n כך ש:

- אם n זוגי אז M_n מודל של T_2 (במילון τ_2).
- אם n אי זוגי אז M_n מודל של T_1 (במילון τ_1).
- $M_n \prec M_{n+2}$ לכל n.
- $\left(M_n \uparrow \tau_0\right) \prec \left(M_{n+1} \uparrow \tau_0\right)$ לכל n.

תחילה נראה כי זה מספיק.

נגדיר את המודלים N_0, N_1, N_2 באופן הבא:

$N_0 = \bigcup\{M_{2n+1} \uparrow \tau_0 : n \in N\}$ הוא מודל במילון τ_0. לפי 3.2.1 הוא מוגדר היטב ו- $M_{2n+1} \uparrow \tau_0 \prec N_0$ לכל n.

$N_1 = \bigcup\{M_{2n+1} : n \in N\}$ הוא מודל במילון τ_1. לפי 3.2.1 הוא מוגדר היטב ו- $M_{2n+1} \prec N_1$ לכל n. ולכן בפרט הוא מודל של T_1.

$N_2 = \bigcup\{M_{2n+1} : n \in N)$ הוא מודל במילון τ_2. לפי 3.2.1 הוא מוגדר היטב ו- $M_{2n} \prec N_2$ לכל n ולכן בפרט הוא מודל של T_2.

קל לראות כי $N_2 \uparrow \tau_0 = N_1 \uparrow \tau_0$, לכן יש מודל N (במילון $\tau_1 \cup \tau_2$) כך ש- $N \uparrow \tau_1 = N_1$ (כי $\tau_1 \cap \tau_2 = \tau_0$ ו- $N_2 \uparrow \tau_0 = N_1 \uparrow \tau_0$).

N הוא מודל של T_i, כי $N \uparrow \tau_i = N_i$ הוא שהינו מודל של T_i. לכן N הוא מודל של $\tau_1 \cup \tau_2$ (ובמילון $\tau = \tau_1 \cup \tau_2$) כנדרש.

נותר לבנות את המודלים M_n.

<u>מקרה 1:</u> $n = 0$

כיוון ש- T_2 תורה יש לה מודל (במילון τ_2).

<u>מקרה 2:</u> $n = 1$

זה לפי משפט עזר 3.3.4 לעיל, כאשר $\tau_0, \tau_1, M_0 \uparrow \tau_0, M_1, T_1$ כאן מתאימים ל- $\tau_0, \tau_1, M_0, M_1, T$ שם.

<u>מקרה 3:</u> $n = n + 2$ (והמודלים M_m, M_{m+1} כבר הוגדרו).

זה נובע ממשפט עזר 3.3.1 לעיל (כאשר, אם n אי זוגי, $\tau_0, \tau_1, M_m, M_{m+1} \uparrow \tau_0, M_{m+2}$ כאן מתאים ל- $\tau_0, \tau_1,\ M_0 M_1 M_2$ שם. ואם n זוגי אז $\tau_0, \tau_2, M_m, M_{m+1} \uparrow \tau_0, M_{m+1}$ כאן מתאימים ל- $\tau_0, \tau_1, M_0, M_1, M_2$ שם). ■

3.4 על מכפלות

3.4.1 הגדרה: D יקרא **מסנן** על קבוצה I אם:

i. D משפחה של תת קבוצות של I.

ii. $I \in D$ אבל $\phi \notin D$.

iii. (סגירות כלפי מעלה): אם $A \subseteq B \subseteq I$ ו- $A \in D$ אז $B \in D$.

iv. (סגירות תחת חתוך): אם A, B שייכות ל- D אז חתוכם $A \cap B$ שייך ל- D.

3.4.2 הגדרה: D יקרא **על מסנן** על קבוצה I אם הוא מסנן על I וכן

v. אם לכל $A \subseteq I$ או A שייכת ל-D או משלימתה, $I \setminus A$, שייכת ל- D.

3.4.3 דוגמה: תהי W אינסופית, ותהי I משפחת התת קבוצות הסופיות של W.

נגדיר את $D = D_W$ מסנן על I באופן הבא:

לכל $t \in I$ נגדיר $X_t = \{s \in I : t \subseteq s\}$. עתה נגדיר $D_W = \bigcup_{t \in I} \{S \subseteq I : S \supseteq X_t\}$. קל לוודא כי D מסנן על I.

3.4.4 משפט: אם D_0 מסנן על קבוצה I אז יש על מסנן D_1 על הקבוצה I שמרחיב את D_0.

רעיון ההוכחה: לכל קבוצה $A \subseteq I$ ומסנן D על I לפחות אחת משתי המשפחות הבאות הינה מסנן על I:

$$D + A = \{B \subseteq A : \quad B \cup (I \setminus A) \in D\}$$
$$D + (I \setminus A) = \{B \subseteq A : \quad B \cup A \in D\}$$

נשים לב: שתי המשפחות מקיימות כמעט את כל הדרישות בהגדרה 3.4.1, חוץ אולי מהדרישה כי הקבוצה הריקה ϕ אינה שייכת למשפחה. עתה יתכן כי $\phi \in D + A$ (כאשר $I \setminus A \in D$) וכן יתכן כי $\phi \in D + (I \setminus A)$ (כאשר $A \in D$) אך לא שני הדברים.

בזה הצלחנו לקיים את דרישת "על מסנן" לקבוצה אחת A. על ידי אינדוקציה על סופית (=טרנספיניטית) או בעזרת הלמה של צורן-קורטובסקי אפשר לבנות על מסנן המרחיב את D. ■

3.4.5 הגדרה: נניח כי $\langle M_t : t \in I \rangle$ סדרת מבנים למילון τ, ונניח כי D מסנן על I. **המכפלה המצומצמת ללא שיוויון** $M = \prod_{t \in I}' M_t / D$ היא המבנה המקיים:

i. העולם של M הוא $M = \prod_{t \in I} M_t$ כלומר משפחת הפונקציות f שתחום הגדרתן I ומקיימות $t \in I \Rightarrow f(t) \in M_t$. (זו קבוצה לא ריקה כי כל $|M_t|$ אינה ריקה, ולכן המכפלה אינה ריקה לפי אכסיומות הבחירה).

ii. לכל סימן יחס n – מקומי R מ- τ נגדיר את R^M בתור משפחת ה- n –יות $\langle f_1, \ldots, f_n \rangle$

המקיימות :

א. $f_1 \in M_1 \;\; f_2 \in M,\ldots, f_n \in M$.

ב. הקבוצה $\{t \in I : \langle f_1(t), f_2(t),\ldots, f_n(t)\rangle \in R^{M_t}\}$ שייכת למסנן D .

ג. לכל סימן פונקציה n-מקומי F מ- τ ולכל $\langle f_1,\ldots, f_n\rangle$ נגדיר

$F^M(f_1,\ldots, f_n)(t) = F^{M_t}(f_1(t),\ldots, f_n(t))$ (כלומר, הפרוש של F ב-M זו הפונקציה

אשר ערכה בקו-אורדינטה ה-t נקבע ע"פ הפרוש של F ב- M_t).

<u>3.4.6 משפט</u>: נניח כי D על מסנן על הקבוצה I, $\langle M_t : t \in I\rangle$ סדרת מבנים למילון τ ,

ו- $M = \prod_{t\in I}' M_t / D$.

(1) יהיו $\vartheta(x_0,\ldots, x_{n-1})$ שם עצם במילון τ , $f_1,\ldots, f_{n-1} \in M$ ו- $t \in I$ אז

$(\vartheta^M(f_1,\ldots, f_{n-1}))(t) = \vartheta^{M_t}(f_1(t),\ldots, f_{n-1}(t))$.

(2) לכל נוסחה $\varphi = \varphi(\bar{x})$ במילון τ , נאמר $\bar{x} = \langle x_1,\ldots, x_n\rangle$, ולכל סדרת אברים $\bar{f}$

מ- M באורך n , נאמר $\bar{f} = \langle f_1,\ldots, f_n\rangle$, התנאים הבאים שקולים :

i. $M \models \varphi[\bar{f}]$.

ii. הקבוצה $\{t \in I : M_t \models \varphi[f_1(t),\ldots, f_n(t)]\}$ שייכת לעל מסנן D.

<u>הוכחה</u>:

(1) נוכיח באינדוקציה על שם העצם ϑ .

<u>מקרה 1</u>: $\vartheta(\bar{x}) = x_k$.

לכן	$\vartheta^M(f_1,\ldots, f_n) = f_k$
ולכן	$(\vartheta^M(f_1,\ldots, f_n))(t) = f_k(t)$
כמו כן	$\vartheta^{M_t}(f_1(t),\ldots, f_n(t)) = f_k(t)$

ולכן סיימנו.

<u>מקרה 2</u>: $\vartheta = F(\vartheta_1,\ldots,\vartheta_m)$.

למשל, ϑ קבוע אישי (כלומר $m = 0$). נרשום $\vartheta_k = \vartheta_k(\bar{x})$ (כי כל משתנה חופשי של ϑ_k הוא

משתנה חופשי של ϑ) ולכן :

$\vartheta(\bar{x}) = F(\vartheta_1(\bar{x}),\ldots,\vartheta_m(\bar{x}))$.

נסמן $g_k = \vartheta_k(f_1,\ldots, f_n)$. נקבל:

לפי הגדרת ϑ^M $\qquad (\vartheta^M(f_1,\ldots, f_n))(t) =$

לפי הגדרת g_k $\quad \left(F^M(\vartheta_1^M(f_1,...,f_n),...,\vartheta_m^M(f_1,...,f_n))\right)(t) =$

לפי הגדרת F^M $\quad (F^M(g_1,...,g_n))(t) =$

לפי הגדרת g_k $\quad F^{M_t}(g_1(t),...,g_m(t)) =$

לפי הנחת האינדוקציה $\quad F^{M_t}((\vartheta_1^M(f_1,...,f_n))(t),...,(\vartheta_m(f_1,...,f_n))(t)) =$

לפי הגדרת ϑ^{M_t} $\quad F^{M_t}((\vartheta_1^{M_t}(f_1(t),...,f_n(t)),...,(\vartheta_m^{M_t}(f_1(t),...,f_n)(t)) =$

$\vartheta^{M_t}(f_1,....,f_n)(t)$

בזה הוכחנו את השוויון הדרוש.

(2) נוכיח את השקילות באינדוקציה על φ.

<u>מקרה 1</u>: $\varphi = R(\vartheta_1,...,\vartheta_m)$.

לכן $\vartheta_k = \vartheta_k(\bar{x})$ כי כל משתנה חופשי של ϑ_k הוא משתנה חופשי של φ.

$M \models \varphi[f_1,...,f_n] \Leftrightarrow$

$M \models R[\vartheta_1[f_1,...,f_n],...,\vartheta_m[f_1,...,f_n]] \Leftrightarrow$

לפי הגדרת הסיפוק:

$\langle \vartheta_1^M[f_1,...,f_n],...,\vartheta_m^M[f_1,...,f_n]\rangle \in R^M \Leftrightarrow$

לפי הגדרת R^M:

$\{t \in I : \langle (\vartheta_1^M[f_1,...,f_n](t),...,\vartheta_m^M[f_1,...,f_n](t)]\rangle \in R^{M_t}\} \in D \Leftrightarrow$

לפי חלק (1):

$\{t \in I : \langle \vartheta_1^{M_t}[f_1(t),...,f_n(t)],...,\vartheta_m^{M_t}[f_1(t),...,f_n(t)]\rangle \in R^{M_t}\} \in D \Leftrightarrow$

לפי הגדרת הסיפוק:

$\{t \in I : M_t \models R[\vartheta_1 m_t[f_1(t),...,f_n(t)],...,\vartheta_m m_t[f_1(t),...,f_n(t)]\} \in D \Leftrightarrow$

לפי ההגדרות:

$\{t \in I : M_t \models \varphi[f_1(t),...,f_n(t)\} \in D$

בזה הוכחנו את השקילות הנדרשת.

<u>מקרה 2</u>: $\varphi = \neg\psi$

כיוון שכל משתנה חופשי של ψ הוא משתנה חופשי של φ, מותר לכתוב $\psi = \psi(\bar{x})$.

נסמן: $A = \{t \in I : M_t \models \varphi[f_1(t),...,f_n(t)]$, $B = \{t \in I : M_t \models \psi[f_1(t),...,f_n(t)]$

לפי הגדרת הסיפוק $\quad A \cup B = I$ וכן $A \cap B = \phi$

לפי הגדרת "D על מסנן על I" יוצא $\quad A \in D \Leftrightarrow B \notin D$

לכן לפי הגדרת הסיפוק $\quad M \not\models \psi[f_1,...,f_n] \Leftrightarrow M \models \varphi[f_1,...,f_n]$

לפי הנחת האינדוקציה זה שקול לכך ש: $\{t \in I : M_t \models \psi[f_1(t),...,f_n(t)]\} \notin D$

ומכיוון, שכאמור $A \in D \Leftrightarrow B \notin D$

נקבל שזה שקול לכך ש: $\{t \in I : M_t \models \varphi[f_1(t),...,f_n(t)]\} \in D$

<u>מקרה 3</u> : $\varphi = \varphi_1 \wedge \varphi_2$. מותר לכתוב $\varphi_1 = \varphi_1[\bar{x}]$ וכן $\varphi_2 = \varphi_2[\bar{x}]$. נסמן:

$A = \{t \in I : \ M_t \models \varphi[f_1(t),...,f_n(t)]\}$, $A_1 = \{t \in I : \ M_t \models \varphi_1[f_1(t),...,f_n(t)]\}$,

$A_2 = \{t \in I : \ M_t \models \varphi_2[f_1(t),...,f_n(t)]\}$.

לפי הגדרת הספוק (ב-M_t): $A = A_1 \cap A_2$

לפי הנחת האינדוקציה: $M \models \varphi_1[f_1,...,f_n] \Leftrightarrow A_1 \in D$

$M \models \varphi_2[f_1,...,f_n] \Leftrightarrow A_2 \in D$

יוצא לפי הגדרת הסיפוק (ב- M): $M \models \varphi[f_1,...,f_n] \Leftrightarrow (A_1 \in D \wedge A_2 \in D)$

לפי הגדרת מסנן: $(A_1 \in D \wedge A_2 \in D \Leftrightarrow A_1 \cap A_2 \in D)$

יחד, בזכרנו כי $A = A_1 \cap A_2$, נקבל: $M \models \varphi[f_1,...,f_n] \Leftrightarrow A \in D$

וזה בדיוק מה שנדרש.

<u>מקרה 4</u>: $\varphi = (\exists y)\psi$.

בה"כ y אינו מופיע ב- $\bar{x}$ (אחרת, אפשר להשמיטו מ- $\bar{x}$ כי הוא משתנה סרק). לכן מותר לכתוב $\psi = \psi(y, \bar{x})$.

הוכחת $(i) \leftarrow (ii)$:

אנו מניחים כי $M \models \varphi[f_1,...,f_n]$. לפי הגדרת הספוק יש אבר f_0 של M כך שמתקיים $M \models \psi[f_0, f_1 ..., f_n]$. לפי הנחת האינדוקציה:

$B = \{t \in I : M_t \models \psi[f_0(t), f_1(t),...,f_n(t)\} \in D$.

עתה לכל $t \in B$ כמובן $M_t \models \psi[f_0(t),\ldots,f_n(t)]$, לכן לפי הגדרת הספוק ב-$M_t$ יצא $M_t \models (\exists y)\psi(y, f_1(t),...,f_n(t))$, כלומר, $M_t \models \varphi[f_1(t),...,f_n(t)]$. לכן אם נגדיר $A = \{t \in I : M_t \models \varphi[f_1(t),...,f_n(t)]\}$ יוצא כי $B \subseteq A \subseteq I$ ומכיוון ש-$B \in D$ נובע מהגדרת "D מסנן על I" ש-$A \in D$, כנדרש.

הוכחת $(i) \leftarrow (ii)$:

אנו מניחים כי $A \in D$ כאשר $A = \{t \in I : M_t \models \varphi[f_1(t),...,f_n(t)]\}$. לכן לכל $t \in A$ יצא כי $M_t \models (\exists y)\psi(y, f_1(t),...,f_n(t))$. לפי הגדרת הסיפוק יש אבר b_t של M_t כך

שמתקיים $M_t \models \psi(b_t, f(t),...,f_n(t))$ נבחר פונקציה f_0 שתחום הגדרתה הוא I וכך ש:

אם $t \in A$ אז $f_0(t) = b_t$ ואם $t \in I \setminus A$ אז $f_0(t)$ הוא אבר כלשהו של M_t (אפשרי כי קבוצת אברי M_t אינה ריקה). עתה ברור כי

$A = \{t \in I : M_t \models \psi(f_0(t) f(t),...,f_n(t))\}$, ולכן לפי הנחת האינדוקציה

$M \models \psi[f_0, f_1,..., f_n]$. לפי הגדרת הסיפוק נובע כי $M \models (\exists y)\psi[y, f_1,..., f_n]$ כלומר:

$M \models \varphi[f_1,..., f_n]$ כנדרש. ■

3.4.7 מסקנה: נניח כי D על מסנן על הקבוצה I. לכל $t \in I$ M_t מודל בשפה L. יהי E סימן יחס דו מקומי שאינו ב- L ו- $L^+ = L \cup \{E\}$.

לכל $t \in I$, תהי N_t העשרה של M_t למבנה בשפה L^+, $N_t = (M_t, E_t)$ כאשר E הוא $\approx_{M_t}$ יחס השוויון על M_t.

יהי $M = \prod_{t \in I}' M_t / D$, $N = \prod_{t \in I}' N_t / D$, אזי:

(1) המבנה N הוא העשרה של המבנה M.

(2) E^N הוא יחס חפיפה על המבנה M כלומר:

א. E^N יחס שקילות על קבוצת אברי M.

ב. לכל סימן יחס n – מקומי R מהשפה L ולכל אברים $f_1',...,f_n'$, $f_1'',...,f_n''$ של M אם $f_1'E^N f_1'',...,f_n'E^N f_n''$ אז $(f_1'',...,f_n'') \in R^M \Leftrightarrow (f_1',...,f_n') \in R^M$.

ג. לכל סימן פונקציה n–מקומי F מהשפה L, ולכל אברים $f_1'',...,f_n'', f_1',...,f_n'$ של M אם $f_1'E^N f_1'',...,f_n'E^N f_n''$ אז $(F^N(f_1'',...,f_n''))E^N(F^N(f_1',...,f_n'))$

הוכחה: נשתמש במשפט 3.4.6 לגבי הנוסחאות המבטאות את אכסיומות השוויון. ■

3.4.8 הגדרה: נניח כי L שפה, I קבוצה $t \in I$, ו- D על מסנן על I. יהיו $M = \Pi' M_t / D$, E_t, N_t ו- N כמו ב 3.4.7.

נגדיר את $\prod_{t \in I} M_t / D$, **העל מכפלה** של $\langle M_t : t \in I \rangle$ לגבי D בתור M / E^N (ראו משפט 3.0.4)

אברי המבנה המתקבל יסומנו ב- f / D במקום ב- f / E^N.

3.4.9 משפט *Łos* המלא: נניח כי M_t מבנה בשפה L לכל $t \in I$, D על מסנן על הקבוצה I אזי:

(1) $M = \prod_{t \in I} M_t / D$ הוא מבנה בשפה L.

(2) לכל נוסחה $\varphi = \varphi(x_1,...,x_n)$ בשפה L, ואברים $f_1 / D,...,f_n / D$ של M, כלומר, $f_1,...,f_n \in \prod_{t\in I} M_t$ מתקיים $M \models \varphi[f_1 / D,...,f_n / D)$ אסם הקבוצה $\{t : M_t \models \varphi[f_1(t),...,f_n(t)\}$ שייכת לעל מסנן D.

<u>הוכחה</u>: לפי 3.4.6 -3.4.8. ■

<u>3.4.10 מסקנה</u>: ב- 3.4.9 אפשר להוסיף:

(1) לכל פסוק ψ בשפה L $M \models \psi \Leftrightarrow \{t \in I : M_t \models \psi\} \in D$.

(2) התורה מסדר ראשון של M, $Th(M)$ תלויה רק בסדרה $< Th \mid M_t \mid : t \in I >$ ובעל המסנן D.

(3) לתורה T (מסדר ראשון) בשפה L, המחלקה $MOD(T) = \{M :$ M מודל של $T\}$ בשפה L סגורה תחת על מכפלות.

<u>3.4.11 הגדרה</u>:

(1) אם לכל $t \in I$ $M_t = M$ אז M^I / D משמעו $\prod_{t\in I} M_t / D$. למבנה זה נקרא **על חזקה**.

(2) נניח כי $N = M^I / D$ כאשר D על מסנן על I. נגדיר פונקציה $j = j_{M,D}$ מהמבנה M למבנה N באופן הבא: לכל $a \in M$, $j(a)$ הוא הפונקציה שתחום הגדרתה I ו- $(j(a))(t) = a$ לכל $t \in I$.

<u>3.4.12 מסקנה</u>: אם D על מסנן על I אז j הוא שכון אלמנטרי של M ב- $N = M^I / D$

<u>הוכחה</u>: לפי משפט *Łos*. ■

נראה עתה שימוש של משפט *Łos* - קבלת הוכחה חלופית למשפט הקומפקטיות.

תזכורת:

<u>3.0.6 משפט הקומפקטיות</u>: נניח כי Γ קבוצת פסוקים (מסדר ראשון) בשפה L, ולכל תת קבוצה סופית של Γ יש מודל אז לקבוצה Γ יש מודל.

<u>הוכחה</u>: תהי I משפחת התת קבוצות הסופיות של Γ. לכל $t \in I$ נבחר מודל M_t של Γ בשפה L (למה בשפה L? יתכן כי יש סימנים של L שאינם מופיעים בפסוקים של t אך הם לא ישנו, שכן אפשר להעשיר את המבנה). לפי הנחתנו M_t קיים לכל t. עתה לפי 3.4.2 ו- 3.4.4 יש על מסנן D על הקבוצה I המקיים

(*) $t \in I \Rightarrow X_t = \{s : t \subseteq s \in I\} \in D$.

יהי $M = \prod_{t\in I} M_t / D$. ברור כי M מבנה בשפה L, ולכן מספיק להוכיח כי $M \models \varphi$ כאשר $\varphi \in \Gamma$ (ולכן בפרט φ פסוק בשפה L).

ברור כי $\{\varphi\} \ni I$ ולכן $X_{\{\varphi\}} \in D$. אבל לפי בחירת M_t יצא $t \in X_{\{\varphi\}} \Rightarrow \{\varphi\} \subseteq t \Rightarrow M_t \models \varphi$,

ולכן הקבוצה $\{t \in I : M_t \models \varphi\}$ היא תת קבוצה של I המכילה את X_φ, אך $X_\varphi \in D$ (לפי (*))

ולכן הקבוצה $\{t \in I : M_t \models \varphi\}$ שייכת ל- D. לפי משפט *Łos* יצא $M \models \varphi$. כיוון שזה נכון לכל פסוק של Γ נובע כי M מודל של Γ כנדרש. ■

נראה שימוש נוסף למשפט *Łos*, שהוא גרסה "הפוכה" למשפט 3.2.2:

<u>3.4.13 משפט *L.S.* העולה</u>: אם M מבנה אינסופי, λ מונה אינסופי אז יש הרחבה אלמנטרית N של M שעוצמתה $\lambda \leq$.

<u>הוכחה</u>: תהי W קבוצה אינסופית שעוצמתה $\lambda \leq$, תהי I משפחת התת הקבוצות הסופיות של W כמקודם. יהי D על מסנן על I המקיים $t \in I \Rightarrow \{s : t \subseteq s \in I\} \in D$. יהיו $\langle a_m : m < \omega \rangle$ אברים שונים של M. לכל $t \ni I$ נבחר מניה (ללא חזרות) $\langle w_{t,1}, \ldots, w_{t,|t|} \rangle$ של t שהיא, כזכור, תת קבוצה סופית של W.

נגדיר לכל $w \in W$ פונקציה f_w מ- I אל M באופן הבא:

$$f_w(t) = \begin{cases} a_k & w = w_{t,k} \quad \text{אם} \\ a_0 & w \notin t \quad \text{אם} \end{cases}$$

ברור כי:

$(*)_1$ $w \in I \Rightarrow \quad (f_w / D) \in M^I / D$.

כמו כן:

$(*)_2$ אם $w_1 \neq w_2$ אברים של W אז $f_{w_1} / D \neq f_{w_2} / D$.

שהרי אם w_1, w_2 אברים של $t \ni I$ אז יש k_1, k_2 כך ש- $w_1 = w_{t,k_1}$ $w_2 = w_{0,k_1}$ כיוון ש- $w_1 \neq w_2$ נובע כי $k_1 \neq k_2$ ולכן $a_{k_1} \neq a_{k_2}$ ולכן $f_{w_1}(t) = a_{k_1} \neq a_{k_2} = f_{w_2}(t)$ לכן הקבוצה $\{t \in I : M_t \models f_{w_1}(t) \neq f_{w_2}(t)\}$

מכילה את $\{t \in I : \{w_1, w_2\} \subseteq t\}$ ששייכת ל- D, ולכן לפי משפט *Łos* נקבל את המסקנה המבוקשת ב- $(*)_2$).

יצא כי $\{f_w / D : w \in W\}$ היא תת קבוצה של M^I / D. שמספר אבריה $\lambda \leq |W|$, לכן מספר אברי M^I / D הוא $\lambda \leq$. לפי 3.4.12 $j_{M,D}$ הוא שכון אלמנטרי של M לתוך M^I / D, לכן יש תת מודל אלמטרי M' של M^I / D שהינו איזומורפי ל- M. יוצא כי למודל M' יש הרחבה אלמנטרית בעצמה $\lambda \leq$ ולכן גם ל- M יש הרחבה כזו. ■

3.4.14 מסקנה: תהי T תורה מסדר ראשון במילון מעצמה λ. אם ל- T יש מודל אינסופי אזי יש לה מודל בכל עצמה $\lambda \leq$.

הוכחה: משפט 3.2.2 + משפט 3.4.13. ■

3.5 טיפוסים ומודלים רווים

3.5.1 סימון: כזכור, למבנה M אנו מסמנים ב- $\tau = \tau(M)$ את המילון של M. נסמן $\tau^+ = \tau[M] = \tau(M) \cup \{c_a : a \in M\}$ כאשר c_a קבועים אישיים שונים שאינם ב- $\tau(M)$.

הערה: כפי שראינו כבר בפרק 3.3 למבנה M יש העשרה טבעית למילון τ^+ ע"י הפרוש $c_a = a$.

כיוון שכבר טיפלנו בסוגיה זו בהרחבה בפרק 3.3 לא נקפיד על ההבחנה בין a ל- c_a ובין M להעשרתו.

מושג בסיסי בתורת המודלים הוא:

3.5.2 הגדרה:

(1) יהי M מבנה ו- $p(\bar{x})$ קבוצת נוסחות מהצורה $\varphi(\bar{x},\bar{a})$ כאשר $\bar{x} = \langle x_0,\ldots,x_{n-1}\rangle$, $\varphi(\bar{x},\bar{y}) \in L_{\tau(M)}$ ו- $\bar{a}$ סדרת איברים מ-M (במילים אחרות, אלו נוסחות במילון τ^+). נאמר ש- $p(\bar{x})$ **מתגשמת ב-M** אם יש ב-M סדרת איברים $\bar{b}$ באורך n כך שלכל $\varphi(\bar{x}) \in p(x)$ מתקיים $M \models \varphi(\bar{b})$. במקרה זה נאמר כי $\bar{b}$ **מגשימה את** $p(\bar{x})$.

(2) נאמר כי קבוצת נוסחות $p(\bar{x})$ היא **טיפוס n-י (או n-טיפוס) במבנה M** אם:

א. $p(\bar{x})$ קבוצת נוסחות מהצורה $\varphi(\bar{x},\bar{a})$ כאשר $\bar{x} = \langle x_0,\ldots,x_{n-1}\rangle$, $\varphi(\bar{x},\bar{y}) \in L_{\tau(M)}$ ו- $\bar{a}$ סדרת איברים מ-M.

ב. כל תת-קבוצה סופית q של p מתגשמת ב-M.

מבין הטיפוסים חשובים במיוחד הטיפוסים השלמים, בהם נדון עתה:

3.5.3 הגדרה:

(1) למבנה M וקבוצה $A \subseteq M$ נאמר ש- $p(\bar{x})$ הוא **טיפוס n-י ב-M מעל A** אם $p(\bar{x})$ טיפוס n-י ב-M ולכל נוסחה $\varphi(\bar{x},\bar{a}) \in p(\bar{x})$ מתקיים ש- $\bar{a} \in {}^{\omega>}A$ (כלומר, הפרמטרים המופיעים בנוסחות של $p(\bar{x})$ הם מתוך A).

(2) נאמר שטיפוס $p(\bar{x})$ כב-(1) הוא **שלם מעל A בתוך M** אם הוא טיפוס n-י ב-M מעל A ולכל נוסחה $\varphi(\bar{x},\bar{y}) \in L_{\tau(M)}$ וסדרה $\bar{a}$ של איברים מ-M באורך של $\bar{y}$ מתקיים $\varphi(\bar{x},\bar{a}) \in p(\bar{x})$ או $\neg\varphi(\bar{x},\bar{a}) \in p(\bar{x})$.

(3) $\underline{S}^n(A,M) = \{p : M$ *בתוך* A *שלם מעל* $n-$ *י טיפוס* $p\}$.

3.5.4 הערה: ברור שב-(2)-3.5.3 לא יתכנו שתי האפשרויות גם יחד.

בהגדרת טיפוס n-י אפשר להתחיל גם מכיוון שונה: לכל מבנה M ולכל תת קבוצה $A \subseteq M$ כל סדרה סופית של איברים מ-M מגשימה טיפוס n-י שלם אחד ויחיד ב-M מעל A. ביתר פירוט:

3.5.5 הגדרה: יהיו M מודל, $A \subseteq M$ ו- $\bar{b}$ סדרה סופית של איברים מתוך M. הטיפוס השלם שהסדרה $\bar{b}$ מגשימה מעל A בתוך M הוא

$tp(\bar{b}, A, M) = \{\varphi(\bar{x}, \bar{a}) : \varphi(\bar{x}, \bar{y}) \in L_{\tau(M)}, \bar{a} \in^{\lg(\bar{y})} A, M \models \varphi(\bar{b}, \bar{a})\}$.

הקשר בין שתי הגישות הנ"ל להגדרת המושג של טיפוס נתון במשפטון הבא:

3.5.6 משפטון: יהיו M מודל ו- $A \subseteq M$.

(1) אם $M \prec N$ ו- $\bar{b} \in^n N$ אז $tp(\bar{b}, A, N) \in S^n(A, M)$.

(2) אם $p \in S^n(A, M)$ אז יש הרחבה אלמנטרית N של M וסדרה סופית $\bar{b}$ של איברים ב-N כך ש- $p = tp(\bar{b}, A, N)$.

(3) $\|N\| = \|M\|$

את הוכחת המשפטון נותיר כתרגיל (בשביל להוכיח את סעיף (2) עליכם לבנות את המודל N בדומה להוכחות שהופיעו בפרק 3.3, כדי לקבל את (3) משתמשים במשפט לוונהים-סקולם היורד).

3.5.7 מסקנה: תהי T תורה שלמה. נניח שלכל מודל $M \models T$ ולכל $A \subseteq M$ סופית מתקיים $|S^1(A, M)| \leq \aleph_0$ אזי ל-T יש מודל רווי בן-מניה.

הוכחה: תרגיל.

לתורה מסדר ראשון יש, במקרה הכללי, הרבה מודלים. השאלה עתה היא האם יש לה מודלים "מיוחדים" כאלו שיהיו "קלים יותר להבנה". אחת הדרישות הטבעיות ממודל "מיוחד" הנה ש"כל מה שיכול לקרות אכן קורה" (טבעית גם הדרישה ההפוכה: "כל מה שאינו מוכרח לקרות אינו קורה", הדיון בדרישה זו מורכב בהרבה). מושג שמממש תובנה זו הוא:

3.5.8 הגדרה:

(1) נאמר כי **מודל M הוא רווי ב- λ** (λ עצמה אינסופית) אם לכל תת קבוצה $A \subseteq M$ שעצמתה קטנה מ- λ כל טיפוס $p \in S^1(A, M)$ מתגשם ב-M.

(2) נאמר כי **M רווי** אם הוא רווי ב- $\|M\|$.

3.5.9 משפטון: אם M מודל, $A \subseteq M$ ו- $p \in S^n(A, M)$ אז יש מודל N המקיים:

i. $M \prec N$.

ii. עצמת N היא לכל היותר $\|M\| + |\tau(M)| + \aleph_0$.

iii. p מוגשם ב-N.

את הוכחת המשפטון נשאיר כתרגיל (השתמשו במשפטון 3.5.6 ובמשפט לוונהים-סקולם היורד 3.3.2).

3.5.10 משפט: נניח כי:

א. M מודל אינסופי.

ב. λ מונה אינסופי סדיר (כלומר, אין ב- λ סדרה באורך קטן מ- λ השואפת ל- λ) המקיים $\|M\|+|\tau(M)|+\aleph_0 \le \lambda = \lambda^{<\kappa}$ (באשר $\lambda^{<\kappa} = \sum_{0\le\alpha<\kappa}\lambda^{|\alpha|} = \sum_{\mu<\kappa}\lambda^{\mu}$).

ג. אם $\mu<\kappa$ אז $2^{\mu+|\tau(M)|+\aleph_0} \le \lambda$.

אז קיים מודל N המקיים:

i. $M \prec N$.

ii. $\|N\| = \lambda$.

iii. N רווי ב- κ.

<u>הוכחה</u>: ההוכחה מעט טכנית, אך אין בה כל קושי אמיתי. למעשה ההוכחה אינה אלא שימוש חוזר ונשנה במשפטון 3.5.8, תוך שימת לב שהנהלת חשבונות נכונה מבטיחה שאיננו שוכחים להגשים אף טיפוס.

ראשית, נזכיר כי מספר התת-קבוצות של M שעצמתן קטנה מ- κ חסום מלעיל ע"י $\lambda^{<\kappa}$ וע"פ הנחתנו $\lambda = \lambda^{<\kappa}$. עתה, בהינתן קבוצה $A \subseteq M$ מעצמה קטנה מ- κ מספר הנוסחות ב- $L_{\tau(M)}$ עם פרמטרים מ-A חסום מלעיל ע"י $|A|+|\tau(M)|+\aleph_0$ (ראו פרוט בהוכחת משפט לוונהים-סקולם היורד 3.3.2). לכן אם $|A| = \mu < \kappa$ מספר הטיפוסים השלמים מעל A ב-M חסום מלעיל ע"י $2^{\mu+|\tau(M)|+\aleph_0}$ (כי לכל נוסחה עלינו לבחור האם היא נמצאת ב-p או לא, וזהו מספר הבחירות האפשרי). אבל מהנתון $2^{\mu+|\tau(M)|+\aleph_0} \le \lambda$. לכן קיימת מניה $\{p_\alpha : \alpha<\lambda\}$ של $\bigcup_{|A|<\lambda} S^1(A,M)$.

נגדיר $N_0 = M$. באינדוקציה על $\alpha<\lambda$ נבנה סדרת מודלים $\{N_{1,\alpha}\}$ כך ש:

(1) $N_{1,0} = N_0$.

(2) עבור δ גבולי $N_{1,\delta} = \bigcup_{j<\delta} N_{1,j}$.

(3) עבור $\alpha = \beta+1$ $N_{1,\beta} \prec N_{1,\alpha}$.

(4) p_α מוגשם ב- $N_{1,\alpha}$.

(5) $\|N_{1,\alpha}\| \le \lambda$.

שני התנאים הראשונים טריביאליים ואילו שלושת התנאים האחרונים מובטחים ע"י משפטון 3.5.8 ביחס למודל $N_{1,\beta}$ ולטיפוס p_α (ברור שאם $p \in S^n(A,M)$ ו- $M \prec N$ אז $p \in S^n(A,N)$). עתה נגדיר $N_1 = \bigcup_{\alpha<\lambda} N_{1,\alpha}$ וממשפט השרשרת העולה (3.2.1) $N_0 \prec N_1$.

מהבניה נקבל עוד שלכל $A \subseteq M$ אם $|A|<\kappa$ אז כל $p \in S^1(A,M)$ מוגשם ב- N_1.

ע"י חזרה על אותו תהליך בדיוק נוכל להגדיר באינדוקציה על $\alpha<\lambda$ סדרת מבנים $\{N_\alpha\}$ כך ש:

(1) עבור δ גבולי $N_\delta = \bigcup_{j<\delta} N_j$.

(2) עבור $\alpha = \beta + 1$ $N_\beta \prec N_\alpha$.

(3) $\|N_\alpha\| = \lambda$

(4) לכל $A \subseteq N_\alpha$ עם $|A| < \kappa$ ו- $p \in S^1(A, N_\alpha)$, p מוגשם ב- $N_{\alpha+1}$.

לבסוף נגדיר $N = \bigcup_{\alpha<\beta} N_\alpha$. נראה כי N עונה על הדרישות: ממשפט השרשרת העולה ברור ש- $M \prec N$ ומחשבון עצמות $\|N\| = \lambda$. נותר לוודא ש-N רווי ב- κ. תהי $A \subseteq N$, $|A| < \kappa$.

כיוון ש- $\kappa \le \lambda$ ו- λ מונה סדיר יוצא ש- $A \subseteq N_\alpha$ לאיזה $\alpha < \lambda$ מספיק גדול (אחרת סדרת האינדקסים של המבנים בהם יש אברי A קצרה מ- λ ומתכנסת ל- λ). מתכונה (4) של הבניה נקבל שכל $p \in S^1(A, N_\alpha) = S^1(A, N)$ מוגשם ב-N, כנדרש.

3.5.11 מסקנה: אם M מודל אינסופי כך ש- $\|M\| \le \lambda^{<\lambda}$ ו- $\tau(M) + \aleph_0 < \lambda$ אז יש ל-M הרחבה אלמנטרית שהיא רוויה בעצמה λ.

3.5.12 הגדרה: יהיו M, N מבנים למילון τ. נאמר ש-f העתקה אלמנטרית עבור (M, N) (או מ-M ל-N) אם:

א. f פונקציה.

ב. תחום f הוא תת קבוצה של M (כלומר, $Dom(f) \subseteq M$).

ג. טווח f הוא תת קבוצה של N (כלומר, $Rang(f) \subseteq N$).

ד. אם $\bar{x} = \langle x_0, \ldots, x_{n-1} \rangle$, $\varphi(\bar{x}) \in L(\tau)$ ו- $\bar{a} = \langle a_0, \ldots, a_{n-1} \rangle$, $a_0, \ldots, a_{n-1} \in |M|$ אז $M \models \varphi(a_0, \ldots, a_{n-1}) \Leftrightarrow N \models \varphi(f(a_0), \ldots, f(a_{n-1}))$ (או בסימון מקוצר $M \models \varphi(\bar{a}) \Leftrightarrow N \models \varphi(f(\bar{a}))$).

3.5.13 משפטון:

(1) הפונקציה הריקה היא פונקציה אלמנטרית מ-M ל-N אסם M, N שקולים אלמנטרית.

(2) פונקציה אלמנטרית מ-M ל-N היא חח"ע (ולכן הפיכה).

(3) f אלמנטרית עבור (M, N) אסם f^{-1} אלמנטרית עבור (N, M).

את ההוכחה נותיר כתרגיל.

3.5.14 משפטון: תהי f אלמנטרית עבור (M, N) אזי:

(1) אם $\bar{b} \in {}^n M$, $A \subseteq Dom(f)$ ו- $p = tp(\bar{b}, A, M) \in S^n(A, M)$ אז $f(p) := \{\varphi(x, f(\bar{a})) : \varphi(\bar{x}, \bar{a}) \in p\} \in S^n(f(A), N)$.

(2) לכל $a \in M, b \in N$ הפונקציה $f^+ := f \cup \{(a, b)\}$ היא אלמנטרית ל- (M, N) אסם b מגשים ב-N את $f(p)$ עבור $p = tp(a, Dom(f), M)$.

<u>הוכחה</u>: תרגיל.

לאחר ההכנות הללו נוכל להוכיח:

<u>3.5.15 משפטון</u>: נניח ש:

א. I סדר מכוון.

ב. לכל $t \in I$ f_t העתקה אלמנטרית לגבי (M,N).

ג. אם $t \leq_I s$ אז $f_t \subseteq f_s$.

אז $f = \bigcup_{t \in I} f_t$ היא העתקה אלמנטרית עבור (M,N).

<u>הוכחה</u>: ברור ש-f פונקציה עם $Dom(f) \subseteq M$ ו- $Rang(f) \subseteq N$, לכן יספיק לוודא את האלמנטריות. לכל נוסחה $\varphi(x_0,\ldots,x_{n-1}) \in L_{\tau(M)}$ ואיברים $a_0,\ldots,a_{n-1} \in Dom(f)$ יש איברים $t_0,\ldots,t_{n-1} \in I$ כך ש- $a_i \in Dom(f_i)$, מכיוון שהסדר מכוון יש $t^* \in I$ המקיים $t_i \leq t^*$ לכל $0 \leq i \leq n-1$. לכן $a_i \in Dom(f_{t^*})$ לכל $0 \leq i \leq n-1$. אבל $f_{t^*} \subseteq f$, ולכן נקבל את המבוקש.

<u>3.5.16 משפט</u>: תהי T תורה שלמה אזי כל שני מודלים רווים של T, שעצמתם שווה הם איזומורפים.

<u>הוכחה</u>: יהיו M,N מודלים רווים ל-T עם $\|M\| = \|N\| = \lambda$. יהיו $\{a_\alpha : \alpha < \lambda\},\{b_\alpha : \alpha < \lambda\}$ מניות של M,N בהתאמה (למי שאינו מכיר את מושג הסודר מומלץ לחשוב על האנלוגיה במקרה שבו $\lambda = \aleph_0$ ואברי M,N נמנים ע"י המספרים הטבעיים. מניה זו מגדירה סדר טוב על המבנים כך שכל רישא ממש שלהם היא מעצמה קטנה מ- $\aleph_0$. משפט הסדר הטוב של *Zermelo* מבטיח שניתן למצוא מניה בעלות תכונות דומות למבנים בכל עצמה).

עתה נגדיר באינדוקציה על $\alpha < \lambda$ העתקות f_α כך ש:

(1) f_α העתקה אלמנטרית מ-M ל-N או להיפך.

(2) $|Dom(f_\alpha)| \leq |2\alpha|$.

(3) $a_\alpha \in Dom(f_{2\alpha+1})$.

(4) $b_\alpha \in Dom(f_{2\alpha+2})$.

(5) $f_\alpha^{-1} \subseteq f_{\alpha+!}$.

- עבור $\alpha = 0$ נשתמש במשפטון (1)-3.5.12.
- עבור $\alpha = 2\beta + 1$ נשתמש במשפטון 3.5.13 (כאן אנו משתמשים ברוויה של N: בהנתן $a_\alpha \in M$ יש איזה $b \in N$ המגשים את $f_{2\beta}(p)$ עבור $p = tp(a, Dom(f_{2\beta}), M)$, והפונקציה f_α תהיה הפונקציה f^+ המובטחת במשפטון ביחס לפונקציה האלמנטרית $f_{2\beta}$ ולזוג (a,b)). שימו לב שאם $a_\alpha \in Rang(f_{2\beta})$ אז דרישה (5) כופה עלינו לבחור $b = f_{2\beta}^{-1}(a_\alpha)$

- עבור $\alpha = 2\beta + 2$ נשתמש שוב במשפטון 3.5.13, הפעם עבור $f^{-1}_{2\beta+1}$ (אפשר בגלל משפטון 3.5.12).
- עבור α גבולי נגדיר $f_\alpha = \bigcup\{f_\beta : \beta = 2\gamma + 1 < \alpha\}$, ונשתמש במשפטון 3.5.14.

לבסוף, נגדיר $f = \bigcup\{f_\beta : \beta = 2\gamma + 1 < \lambda\}$, וקל לבדוק ש-$f$ הוא איזומורפיזם כנדרש (f פונקציה אלמנטרית בגלל משפטון 3.5.14, לכן כדי להבטיח שהיא איזומורפיזם די לוודא ש-$Dom(f) = M$, אבל זה ברור מהבניה).

3.5.17 מסקנה: אם T תורה שלמה במילון τ ו-$|T| + \tau + \aleph_0 < \lambda = \lambda^{<\lambda}$ אז עד כדי איזומורפיזם יש ל-T מודל רווי אחד ויחיד שעצמתו λ.

3.5.18 משפטון: יהי M מודל רווי לתורה T. יהי $N \models T$ מודל כלשהו המקיים $\|N\| \le \|M\|$ אזי יש שיכון אלמנטרי של N לתוך M.

הוכחה: יהי $\lambda = \|N\|$. נבחר מניה של אברי N לפי λ. נבנה את השיכון באינדוקציה. נגדיר $f_0 = \phi$, לפי משפטון 3.5.13 הפונקציה הריקה היא אלמנטרית מ-N ל-M, וזהו עוגן האינדוקציה. אם $\alpha = \beta + 1$ אז נקח $a_\alpha \in N$ האיבר ה-α במניה של אברי N שבחרנו. נסמן $p_\alpha(x) = tp(a_\alpha / \{a_\beta : \beta < \alpha\})$ (הטיפוס של a_α מעל כל אברי N הקודמים לו במניה). לפי משפטון 3.5.14 $p'_\alpha = f_\beta(p_\alpha(x))$ טיפוס שלם ב-M, ומכיוון ש-$|\alpha| < \lambda \le \|M\|$ ו-M רווי יש הגשמה b_α של p'_α ב-M. נגדיר $f_\alpha = f_\beta \cup (a_\alpha, b_\alpha)$ לפי החל השני של משפטון 3.5.14 f_α העתקה אלמנטרית. לבסוף אם אם δ סודר גבולי נגדיר $f'_\delta = \bigcup_{\alpha<\delta} f_\alpha$. לפי משפטון 3.5.15 ולפי הנחת האינדוקציה f'_δ העתקה אלמנטרית, ועתה נמשיך בדיוק כמו במקרה של סודר עוקב, עם f'_δ בתפקיד f_β.

תרגילים – טיפוסים ומודלים רווים

1. יהי M מבנה כלשהו ו-$p(\bar{x})$ קבוצת נוסחות מהצורה $\varphi(\bar{x}, \bar{a})$ כאשר, $\bar{a} \in M$. הראו ש-$p(\bar{x})$ טיפוס אסם $M \models \exists \bar{x} \bigwedge_{i-1}^{n} \varphi_i(\bar{x}, \bar{a}_i)$ לכל n ולכל n-יה של נוסחות $\varphi_i(\bar{x}, \bar{a}_i)$ מ-$p(\bar{x})$.
2. יהי M מבנה כלשהו. נניח ש-$M \prec N$ ו-$p(\bar{x})$ טיפוס ב-M מעל A. אזי $p(\bar{x})$ טיפוס ב-N מעל A, ואם $p(\bar{x})$ שלם ב-M אז הוא שלם גם ב-N.
3. תהי T תורה שלמה. יהיו $M_1, M_2 \models T$ אזי כל טיפוס ב-M_1 מעל הקבוצה הריקה הוא טיפוס ב-M_2 מעל הקבוצה הריקה.

3.6 מודלים בני-מניה

3.6.1 הגדרה: תורה T תקרא **קטגורית** בעצמה λ אם יש לה מודל יחיד בעצמה λ עד כדי איזומורפיזם.

מטרתנו העיקרית בפרק זה היא למצוא אפיון לתורות בנות מניה קטגוריות ב- $\aleph_0$. לשם כך נצטרך לפתח מספר כלים חדשים.

3.6.2 סימון: תהי T תורה שלמה ויהי $M \models T$ מודל כלשהו. נסמן $D_n(T) = S^n(\phi, M)$.

3.6.3 הערה: הראנו שזה מוגדר היטב (כלומר, לא תלוי בבחירת M). ראו תרגילים לפרק "טיפוסים ומודלים רווים".

3.6.4 טענה: עבור תורה שלמה T בת מניה ללא מודלים סופיים התנאים הבאים שקולים:

(1) ל-T יש מודל רווי בעצמה $\aleph_0$.

(2) לכל מודל $M \models T$ ולכל $A \subseteq M$ סופית מתקיים $\left|S^1(A,M)\right| \le \aleph_0$.

(3) $D_n(T)$ בת מניה לכל n.

הוכחה: הכיוון $(1) \Leftarrow (2)$ הוא מסקנה 3.5.7.

$(3) \Leftarrow (1)$: יהי M מודל רווי בן מניה של T ויהי $p = p(\bar{x}) \in D_n(T)$. לכל $q \subseteq p$ סופית קבוצת הפסוקים $\exists \bar{x} \bigwedge \{\varphi(\bar{x}) : \varphi \in q\} \in T$, ולכן יש לכך עדים ב-$M$. לכן יש מודל $M \prec N_p$ שבו הטיפוס p מוגשם, נאמר ע"י הסדרה $\bar{a}$. לפי משפטון 3.5.6 בה"כ $\|M\| = \|N_p\|$. לפי משפטון 3.5.18 יש שיכון אלמנטרי $f : N \to M$, ואז $f(\bar{a})$ הגשמה של p ב-M.

$(2) \Leftarrow (3)$: יהיו $M \models T$ ו- $A \subseteq M$ סופית תהי $\bar{a}$ מניה כלשהי של אברי A. לכל $p \in S^1(A,M)$ נבחר $M \prec M_p$ ו- $b_p \in M_p$ המגשים את p. נגדיר:

$q_p = tp((b_p, \bar{a}), \phi, M_p) \in D_{n+1}(T)$. מההנחה (3) יספיק להראות שההעתקה $p \to q_p$ חח"ע, ואת זה נותיר כתרגיל קל לקוראים. ■

באופן אינטואיטיבי, קטגוריות אמורה להצביע על קיום "מעט" טיפוסים. הטענה הבאה מספקת הצדקה מסוימת לטענה זו:

3.6.5 טענה: תהי T תורה בת מניה ושלמה. אם יש n כך ש- $\left|D_n(T)\right| = \lambda > \aleph_0$ אזי ל-T יש לפחות λ מודלים לא איזומורפים בעצמה $\aleph_0$.

הוכחה: לכל $p \in D_n(T)$ נמצא מודל בן-מניה M_p וסידרה $\bar{b}_p \in M_p$ המגשימה את p. נגדיר יחס דו-מקומי על $D_n(T)$ באופן הבא: $E(p,q) \Leftrightarrow M_p \cong M_q$. ברור שזהו יחס שקילות. יספיק להראות שכל מחלקת שקילות היא בת מניה (זה מספיק משום שהנחנו ש- $\lambda > \aleph_0$, ומכיוון ש- $\aleph_0 \cdot \kappa = \kappa$ לכל עצמה κ אינסופית, נקבל שבהכרח יש ל-E λ מחלקות שקילות). נניח, אם כן, בשלילה שיש איזה טיפוס q כך שקיימים יותר מ- $\aleph_0$ טיפוסים q_i המקיימים $E(q_i, q)$. מהגדרת

E לכל i יש איזומורפיזם $f_i : M_{q_i} \to M_q$. הסדרה $\{f_i(\bar{b}_{q_i})\}$ באורך גדול מ- $\aleph_0$, ולכן יש $i \neq j$ כך ש- $f_i(\bar{b}_{q_i}) = f_j(\bar{b}_{q_j})$ (כי $\{f_i(\bar{b}_{q_i})\}$ היא סדרה של n-יות ב- M_q ומכיוון ש- M_q בן מניה יש רק מספר בן-מניה של n-יות שונות ב- M_q). אבל זה גורר ש- $q_i = q_j$, בסתירה להנחה). ■

גרסה כללית יותר של הטענה הנ"ל ראו בתרגילים לסעיף זה.

3.6.6 הגדרה: מודל M של תורה שלמה T יקרא **ראשוני** בעצמה $|T| + \aleph_0 \leq \lambda$ אם לכל מודל N כך ש- $\|N\| = \lambda$ יש שיכון אלמנטרי של M לתוך N.

3.6.7 משפטון: אם T שלמה, $M \models T$, $\|M\| \leq \lambda$ ו-M ראשוני בעצמה $\lambda \geq$ אזי לכל $N \models T$, אם $\|N\| \geq \lambda$ יש שיכון אלמנטרי של M לתוך N.

הוכחה: תרגיל. ■

3.6.8 הגדרה: טיפוס $p \in S^n(A,M)$ יקרא **מבודד** אם יש נוסחה $\varphi(\bar{x},\bar{a})$, $\bar{a} \in A$, כך ש- $\varphi(\bar{x},\bar{a}) \vdash p$, כלומר, לכל $M \prec N$ ו- $\bar{b} \in N$ אם $N \models \varphi(\bar{b},\bar{a})$ אז $\bar{b}$ מגשים את p. במקרה זה נאמר ש- $\varphi(\bar{x},\bar{a})$ **מבודדת** את p.

3.6.9 משפטון: אם $p \in S^n(A,M)$ אז $\varphi(\bar{x},\bar{a})$ **מבודדת** את p אסם לכל $\psi(\bar{x},\bar{b}) \in p$ מתקיים $M \models \forall \bar{x}(\varphi(\bar{x},\bar{a}) \to \psi(\bar{x},\bar{b}))$.

הוכחה: תרגיל. ■

3.6.10 הגדרה: מודל M יקרא **אטומי**, אם לכל n ולכל $\bar{a} \in M$ מאורך n $tp(\bar{a},\phi,M)$ מבודד.

3.6.11 משפט: אם M אטומי ובן מניה אז M ראשוני.

הוכחה: תהי $T = Th(M)$, ו- $N \models T$. תהי $\{a_i\}_{i=1}^{\infty}$ מניה של אברי M (יש מניה כזו כי M בן מניה). נבנה את השיכון של M ב-N באינדוקציה על N.

ל- $i = 0$ נגדיר $f_0 = \phi$. לפי משפטון 3.5.13, זוהי העתקה אלמנטרית ל- (M,N).

עתה נניח שהגדרנו $f_n : \{a_i\}_{i=1}^{n} \to N$ אלמנטרית ל- (M,N), ונגדיר $f_{n+1} : \{a_i\}_{i=1}^{n+1} \to N$ אלמנטרית. יהי $p = tp(\{a_i\}_{i=1}^{n+1},\phi,M)$. מהנחתנו על M, p טיפוס מבודד, נאמר ע"י הנוסחה $\varphi(\bar{x})$. כיוון ש-p טיפוס שלם בהכרח $\varphi(\bar{x}) \in p$ (למשל, לפי משפטון 3.6.9). ולכן $M \models \exists x \varphi(a_1,\ldots,a_n,x)$, מהנחת האינדוקציה $N \models \exists x \varphi(f_n(a_1),\ldots,f_n(a_n),x)$. לכן, אם נסמן $b_i = f_n(a_i)$ נקבל שיש $b_{n+1} \in N$ כך ש- $N \models \varphi(b_1,\ldots,b_n,b_{n+1})$. ממשפטון 3.6.9 נובע ש- $b_1,\ldots,b_n,b_{n+1}$ מגשים את p ב-N (כי p מבודד ע"י $\varphi(\bar{x})$). ממשפטון 3.5.14 נובע ש- $f_{n+1} := f_n \cup (a_{n+1},b_{n+1})$ אלמנטרית ל- (M,N) (כי ישירות מן ההגדרה נקבל ש- $tp(a_{n+1},\{a_i\}_{i=1}^{n},M) = tp(b_{n+1},\{b_i\}_{i=1}^{n},N)$, וזאת כיוון ש- $b_1,\ldots,b_n,b_{n+1}$ ו- $a_1,\ldots,a_n,a_{n+1}$ מגשימות אותו טיפוס מעל ϕ).

עתה נגדיר $f=\bigcup_n f_n$ ולפי משפטון 3.5.15, f היא שיכון, כנדרש. ■

עתה נרצה להראות שגם ההיפך נכון, כלומר:

3.6.12 משפט: אם T תורה שלמה ובת מניה ו-M מודל בן מניה אז התנאים הבאים שקולים:

(1) M ראשוני.

(2) M אטומי.

הצעד העיקרי בהוכחה הוא המשפט הבא:

3.6.13 משפט השמטת הטיפוס: נניח כי:

א. T תורה במילון בן מניה.

ב. $p(\bar{x})$ קבוצת נוסחות כך ש- $T\cup p(\bar{x})$ עקבית (ו- $\bar{x}$ מאורך סופי).

ג. לכל נוסחה $\psi(\bar{x})$ כך ש- $T\cup\{\exists\bar{x}\psi(x)\}$ עקבית יש נוסחה $\varphi\in p$ כך ש- $T\cup\{\exists\bar{x}(\psi(\bar{x})\wedge\neg\varphi(\bar{x})\}$ עקבית.

אזי יש מודל בן מניה M של T כך ש-p אינה מוגשמת ב-M (ונאמר ש-M **משמיט** את p).

הוכחה: משפט זה הוכח בתרגילים לסעיף 3.2 (שם גם הראינו שתנאי (ג) במשפט הנו הכרחי). ניתן עתה הוכחה מלאה: נסמן $\bar{x}_i=x_0,\dots,x_i$. נגדיר

$\Gamma=\{\Psi:\exists m(\Psi=\{\psi_i(\bar{x}_i):i\le m\}\wedge$ *עקבית* $T\cup\{\exists\bar{x}_m\bigwedge_{i-0}^{m}\psi_i(\bar{x}_i)\}\}$ (נזכור שהנוסחות $\psi_i(\bar{x}_i)$ עשויות להכיל משתני סרק). כלומר, Γ היא אוסף של קבוצות של נוסחות, שהגשמותיהן מקרבות מודלים T. נשים לב ש- $\Gamma\neq\phi$ (כי $\Psi=\exists x(x=x)\in\Gamma$). עתה, מהגדרת הסיפוק (ומן העובדה שקבוצת פסוקים עקבית אסם יש לה מודל) נובע:

טענת עזר 1: אם $\Psi=\{\psi_i(\bar{x}_i)\}_{i\le m}\in\Gamma$ אזי:

i. אם $\psi_k=\psi_k'\wedge\psi_k''$ אזי $\Psi\cup\{\psi_k',\psi_k''\}\in\Gamma$.

ii. אם $\psi_k=\psi_k'\vee\psi_k''$ אזי או ש- $\Psi\cup\{\psi_k'\}\in\Gamma$ או ש- $\Psi\cup\{\psi_k''\}\in\Gamma$.

iii. אם $\psi_k=\forall x(\psi_k'(x,\bar{x}_k))$ וההצבה $s\begin{pmatrix}x\\x_t\end{pmatrix}$ כשרה ל- ψ_k' עבור $x_t\in\{\bar{x}_m\}$ אזי $\Psi\cup\{\psi_k'(x_t,\bar{x}_k)\}\in\Gamma$.

iv. אם $\psi_k=\exists x(\psi_k'(x,\bar{x}_k))$ אזי $\Psi\cup\{\psi_k'(x_{m+1},\bar{x}_k)\}\in\Gamma$.

v. לכל נוסחה ψ, $\Psi\cup\{\psi\}\in\Gamma$ או $\Psi\cup\{\neg\psi\}\in\Gamma$.

vi. אם $\vartheta(\bar{x}_k)$ שם עצם אזי $\Psi\cup\{x_{m+1}=\vartheta(\bar{x}_k)\}\in\Gamma$.

נוכיח עתה טענת עזר נוספת:

<u>טענת עזר 2</u>: נניח ש- $x_{i_0},\dots,x_{i_n}$ סדרה באורך של המשתנים המופיעים ב- $p(\bar{x})$ וש- $\Psi=\{\psi_i(\bar{x}_i)\}_{i\le m}\in\Gamma$ כך ש- $m>\{i_0,\dots,i_n\}$, אזי יש נוסחה $\varphi(\bar{x})\in p$ כך ש- $\Psi\cup\{\neg\varphi(x_{i_0},\dots,x_{i_n})\}\in\Gamma$.

<u>הוכחה</u>: נסמן $\bar{y}=\bar{x}_m\setminus\{x_{i_0},\dots,x_{i_n}\}$. נגדיר $\psi(x_{i_0},\dots,x_{i_n})=\exists\bar{y}\bigwedge_{i--0}^{m}\psi_i(\bar{x}_i)$. לכן (מהנחה (ג) בתנאי המשפט) יש $\varphi(x_{i_0},\dots,x_{i_n})\in p$ כך ש- $T\cup\{(\exists x_{i_0},\dots,x_{i_n})(\psi(x_{i_0},\dots,x_{i_n})\wedge\neg\varphi(x_{i_0},\dots,x_{i_n}))\}$ עקבית. עתה הטענה נובעת מטענת עזר 1.

עתה נפנה להוכחת המשפט: נבנה סדרה $\{\psi_i(\bar{x}_i)\}_{i-0}^{\infty}$ כך שמתקיים:

(1) לכל m טבעי $\Psi_m=\{\psi_i(\bar{x}_i)\}_{i\le m}\in\Gamma$.

(2) לכל k אם ψ_k מקיימת את אחד התנאים של טענת עזר 1 אז יש m מספיק גדול כך ש- Ψ_m מקיימת את מסקנת טענת עזר 1.

(3) לכל נוסחה ψ, יש m מספיק גדול כך ש- $\psi\in\Psi_m$ או $\neg\psi\in\Psi_m$.

(4) אם בה"כ $x_{i_0},\dots,x_{i_n}$ ללא חזרות אז יש m ונוסחה $\varphi(x_{i_0},\dots,x_{i_n})\in p$ כך ש- $\neg\varphi\in\Psi_m$.

(בניית הסדרה היא תרגיל קל בהנהלת חשבונות, ונותיר אותה לקוראים).

עתה, כמו בהוכחת משפט השלמות, נגדיר יחס דו מקומי על המספרים הטבעיים:

$E=\{(n,m):\exists k(\psi_k="x_n=x_m")\}$ ונגדיר את המבנה $M=\varpi/E$. כמו בהוכחת משפט השלמות נגדיר עתה לכל n ולכל סימן יחס n מקומי R במילון, $R^M=\{(i_0/E,\dots,i_{n-1}/E):\exists m(R(x_{i_0},\dots,x_{i_{n-1}})=\psi_m)\}$, ולכל סימן פונקציה n מקומי F $F^M(i_0/E,\dots,i_{n-1}/E)=i_n/E\Leftrightarrow\exists m("F(x_{i_0},\dots,x_{i_{n-1}})=x_{i_n}"=\psi_m)$. כמו בהוכחת משפט השלמות, קל לוודא שההגדרות הנ"ל טובות (כלומר, אינן תלויות בבחירת הנציגים למחלקות השקילות) וש-M מודל של T (כי $M\models\psi_m$ לכל m טבעי, ובגלל תנאי (3) בבניית הסדרה, בצרוף עם תנאי (1) של הבניה נובע שכל פסוקי T שייכים לסדרה). בנוסף, M משמיט את p בגלל תנאי (4) בבניית הסדרה. ■

עתה נוכל לחזור להוכחת משפט 3.6.13:

<u>הוכחת משפט 3.6.13</u>: עלינו להוכיח רק את הכיוון (1) גורר (2): נניח, אם כן, ש-M אינו מודל אטומי. אזי יש $\bar{a}\in M$ כך ש- $p=tp(\bar{a},\phi,M)$ אינו מבודד. כלומר, לכל נוסחה $\psi(\bar{x})$ אם יש נוסחה $\varphi(\bar{x})\in p$ כך ש- $\neg(\psi\to\varphi)$, בפרט $T\cup\{\exists\bar{x}(\psi(\bar{x})\wedge\neg\varphi(\bar{x}))\}$ עקבית אם $T\cup\{\exists\bar{x}(\psi(\bar{x}))\}$ עקבית. מכאן שתנאי משפט 3.6.14 מתקיימים, ולכן יש מודל בן מניה N של T המשמיט את p אבל אז לא יתכן ש-M משוכן לתוך N (מה יכולה להיות תמונת $\bar{a}$ תחת שיכון אפשרי), כלומר, M אינו ראשוני. ■

3.6.14 הערה: נשים לב שבהוכחת משפט 3.6.13 יכולנו בעצם לקבל יותר: תהי T תורה שלמה בשפה בת מניה ו- $\{p(\bar{x}_i)\}_{i=1}^{\infty}$ משפחה של טיפוסים כך שלכל i מתקיימים התנאים:

א. $p_i(\bar{x}_i)$ קבוצת נוסחות כך ש- $T \cup p_i(\bar{x}_i)$ עקבית (ו- $\bar{x}_i$ מאורך סופי).

ב. לכל נוסחה $\psi(\bar{x})$ כך ש- $T \cup \{\exists \bar{x}\psi(x)\}$ עקבית יש נוסחה $\varphi \in p_i$ כך ש- $T \cup \{\exists \bar{x}(\psi(\bar{x}) \wedge \neg\varphi(\bar{x})\}$ עקבית.

אזי יש מודל בן-מניה של M המשמיט את כל הטיפוסים $\{p(\bar{x}_i)\}_{i=1}^{\infty}$.

הוכחה: ההבדל היחיד ביחס להוכחת משפט 3.6.13 הוא בתנאי (4) בבניית הסדרה $\{\psi_i(\bar{x}_i)\}_{i=0}^{\infty}$, אבל כיוון ש- $\{p(\bar{x}_i)\}_{i=1}^{\infty}$ בת מניה ברור שאין כל קושי לדאוג לתנאי זה לכל אחד מן הטיפוסים.

■

3.6.15 הערה: מסקנה מיידית ממשפט השמטת הטיפוס הוא, שאם ב- $D_n(T)$ יש טיפוס לא מבודד אזי ל-T יש לפחות שני מודלים שאינם איזומורפים.

הוכחה: יהי $p \in D_n(T)$ טיפוס לא מבודד. אזי ממה שכבר הראינו יש מודל בן מניה של T שבו p מוגשם. מאידך ממשפט השמטת הטיפוס יש מודל בן מניה שבו p מושמט. ברור ששני מודלים אלו אינם איזומורפים. ■

עד כה טרחנו רבות כדי לקשור בין מודלים בני מניה אטומיים למודלים ראשוניים, אך עדיין איננו יודעים מתי לתורה T יש מודל אטומי בן מניה. המשפט הבא נותן תשובה מלאה לבעיה זו:

3.6.16 משפט: תהי T תורה שלמה בשפה בת מניה, אזי התנאים הבאים שקולים:

(1) ל-T יש מודל אטומי בן מניה.

(2) לכל n, קבוצת הטיפוסים המבודדים ב- $D_n(T)$ **צפופה**, כלומר, אם $T \vdash \exists \bar{x}\varphi(\bar{x})$ אז יש $p \in D_n(T)$ מבודד כך ש- $\varphi(\bar{x}) \in p$.

הוכחה: $(1) \Leftarrow (2)$: יהי M מודל אטומי בן מניה של T. נניח ש- $T \vdash \exists \bar{x}\varphi(\bar{x})$, לכן יש $\bar{a} \in M$ כך ש- $M \models \varphi(\bar{a})$. נביט ב- $p = tp(\bar{a}, \phi, M)$, אזי מהגדרה $p \in D_n(T)$, p מבודד (כי M אטומי) ולפי בחירת p ברור ש- $\varphi(\bar{x}) \in p$.

$(2) \Leftarrow (1)$: לכל n טבעי נגדיר $q_n = \{\neg\varphi(x_0,\ldots,x_{n-1}) : \exists q \in D_n(T),\ q \text{ מבודדת את } \varphi\}$. לכל n נבחן את המקרה שבו q_n טיפוס (כלומר עקבי ביחס ל-T). תהי $\varphi(\bar{x})$ נוסחה כלשהי כך ש- $T \vdash \exists \bar{x}\varphi(\bar{x})$. לפי ההנחה יש טיפוס מבודד $p \in D_n(T)$ כך ש- $\varphi(\bar{x}) \in p$. נניח עתה ש- p מבודד ע"י הנוסחה $\psi(\bar{x})$. ז"א ש- $\neg\psi \in q_n$. כיוון ש- $\varphi, \psi \in p$ יוצא ש- $T \vdash \exists \bar{x}(\varphi(\bar{x}) \wedge \psi(\bar{x}))$, כלומר, הטיפוס q_n מקיים את תנאי משפט השמטת הטיפוס (כי $\varphi(\bar{x})$ הייתה נוסחה כלשהי). לכן, לפי הערה 3.6.14 יש מודל בן מניה M של T המשמיט את כל אותם q_n

שהם עקביים. נראה ש-M מודל אטומי: יהי $\bar{a} \in M$ באורך n. יתכנו שני מקרים: אם q_n אינו עקבי, אז בוודאי $M \models \varphi(\bar{a})$ לאיזו $\varphi(\bar{x})$ כך ש-$\neg\varphi(\bar{x}) \in q_n$ (כי אחרת M יגשים את q_n בסתירה להנחה שאינו עקבי), כלומר – מהגדרת q_n - יש טיפוס p שמבודד ע"י $\varphi(\bar{x})$. יספיק להראות ש-$p = tp(\bar{a},\phi,M)$ אבל זו מסקנה מיידית ממשפטון 3.6.9 ומן העובדה ש-$M \models \varphi(\bar{a})$. המקרה שבו q_n כן עקבי מטופל באופן זהה (ההבדל היחיד הוא שקיום הנוסחה $\varphi(\bar{x})$ כך ש-$M \models \varphi(\bar{a})$ ו-$\neg\varphi(\bar{x}) \in q_n$ מובטח ע"י העובדה ש-M משמיט את q_n). ■

ראינו כבר שאם $|D_n(T)|$ מעצמה גדולה מ-$\aleph_0$ אז T אינה קטגורית ב-$\aleph_0$. צעד נוסף להבנת הקשר שבין קטגוריות ב-$\aleph_0$ לבין העצמה של $|D_n(T)|$ נקבל מן הטענה הקלה הבאה:

<u>3.6.17 משפטון</u>: תהי T תורה שלמה בשפה בת מניה, אזי התנאים הבאים שקולים:

(1) $D_n(T)$ סופית.

(2) כל טיפוס ב-$D_n(T)$ מבודד.

<u>הוכחה</u>: $(1) \Leftarrow (2)$. אם $D_n(T)$ סופית אז לכל $p \neq q \in D_n(T)$ נמצא נוסחה $\varphi_{p,q} \in p$ כך ש-$\neg\varphi_{p,q} \in q$. מסופיות $D_n(T)$ הקבוצה $\Gamma_p = \{\varphi_{p,q} : p \neq q \in D_n(T)\}$ סופית. כיוון ש-p טיפוס שלם, יוצא ש-$\varphi_p := \bigwedge\{\varphi : \varphi \in \Gamma_p\}$ נוסחה ב-p. נראה ש-φ_p מבודדת את p, כיוון ש-p היה שרירותי, זה יוכיח את הטענה. נניח, אם כן, ש-φ_p אינה מבודדת את p, זה אומר, שיש טיפוס $q \neq p$ כך ש-$\varphi_p \in q$ (כי מהנחת השלילה מתקיים ש-$T \vdash \exists\bar{x}(\varphi_p(\bar{x}) \wedge \neg\psi(\bar{x}))$ לאיזו נוסחה $\psi(\bar{x}) \in p$. כיוון שכך הקבוצה $T \cup \{\varphi_p(\bar{x}) \wedge \neg\psi(\bar{x})\}$ עקבית, ולכן ניתן להשלימה לטיפוס שלם ב-$D_n(T)$). אבל מהגדרת φ_p נובע ש-$\varphi_p \in q$ אסם $p = q$ וזו סתירה.

$(2) \Leftarrow (1)$. נניח שכל טיפוס ב-$D_n(T)$ מבודד. לכל $p \in D_n(T)$ תהי φ_p נוסחה המבודדת את p. נגדיר $\Gamma = \{\neg\varphi_p : p \in D_n(T)\}$. קבוצת הנוסחות $T \cup \Gamma$ אינה עקבית, כי אחרת יש מודל M של T שבו Γ מסופקת, נאמר ע"י סדרה $\bar{a} \in M$. אבל אז מצד אחד, לפי ההגדרה, $q = tp(\bar{a},\phi,M) \in D_n(T)$, ומאידך לכל $p \in D_n(T)$ מתקיים ש-$\neg\varphi_p \in q$, כלומר $p \neq q$ לכל $p \in D_n(T)$, וזו סתירה. לכן, ממשפט הקומפקטיות, יש קבוצה סופית $\Delta \subseteq \Gamma$ כך ש-$T \cup \Delta$ אינה עקבית. מכאן נובע שאם $p \in D_n(T)$ אז יש $\varphi_q \in \Delta$ כך ש-$\neg\varphi_q \notin p$ (כי אחרת נקבל ש-$T \cup \Delta$ עקבית). זה אומר ש-$q \subseteq p$ (כי φ_q מבודדת את q, ולכן מנביעה כל נוסחה ב-q) כיוון ש-p ו-q שלמים נובע ש-$q = p$. מכיוון ש-Δ סופית נובע שיש רק מספר סופי של טיפוסים ב-$D_n(T)$, כנדרש. ■

עתה אנו מוכנים להוכחת המשפט העיקרי בסעיף זה:

3.6.18 משפט *(Ryll-Narjewski)*: תהי T תורה שלמה במילון בן מניה. אם ל-T יש מודלים אינסופיים, אזי התנאים הבאים שקולים:

(1) T קטגורית ב-$\aleph_0$.

(2) לכל n $D_n(T)$ סופית.

(3) כל מודל בן מניה של T הוא אטומי.

(4) כל מודל בן מניה של T הוא ראשוני.

(5) כל מודל בן מניה של T הוא רווי.

(6) לכל n קימות נוסחות $\{\varphi_i(x_0,\dots,x_{n-1})\}_{i<m}$ כך שלכל נוסחה $\psi(x_0,\dots,x_{n-1})$ מתקיים $T\vdash\bigvee_{i<m}(\varphi_i(\bar{x})\leftrightarrow\psi(\bar{x}))$ (כלומר, לכל n יש ב-T מספר סופי של נוסחות ב-n משתנים עד כדי שקילות).

הוכחה: נוכיח ראשית את השקילויות (1)-(5), ואח"כ את השקילות $(2)\Leftrightarrow(6)$. ממשפטון 3.6.17 אנחנו יודעים ש-$D_n(T)$ סופית אסם כל טיפוס ב-$D_n(T)$ מבודד. מהערה 3.6.15 אנחנו יודעים שאם יש לאיזה n טיפוס לא מבודד ב-$D_n(T)$ אזי T לא קטגורית. לכן $(2)\Leftarrow(1)$. שוב ממשפטון 3.6.17 אנחנו מקבלים ישירות מן ההגדרה ש-$(3)\Leftarrow(2)$. את השקילות $(4)\Leftrightarrow(3)$ כבר הוכחנו במשפט 3.6.12. יחידות המודל הרווי מראה ש-$(1)\Leftarrow(5)$, לכן כדי להשלים את הוכחת השקילויות (1)-(5) יספיק להראות ש-$(5)\Leftarrow(3)$. נראה זאת:

יהי M מודל בן מניה. עלינו להראות, שלכל $A\subseteq M$ סופית, ולכל טיפוס $p\in S^1(A,M)$ יש הגשמה ב-M. יהי $M\prec M^*$ מודל בן-מניה כך ש-p מוגשם ב-M^*, נאמר ע"י b. עתה, תהי $\bar{a}$ מניה כלשהי של אברי A. נביט ב-$q=tp((b,\bar{a}),\phi,M^*)$. כיוון ש-$M^*$ אטומי (כמודל בן-מניה של T) יש $\varphi_q(x,\bar{y})$ שמבודדת את q, וברור ש-$M^*\models\exists x\varphi_q(x,\bar{a})$ (כי b עד לכך). כיוון ש-$\bar{a}\in M$ ו-$M\prec M^*$ גם $M\models\exists x\varphi_q(x,\bar{a})$, לכן יש $b'\in M$ כך ש-$M\models\varphi_q(b',\bar{a})$. נותיר זאת כתרגיל קל לקוראים לוודא ש-b' מגשים את p.

לבסוף, נראה ש-$(2)\Leftrightarrow(6)$. ברור ש-$(6)\Rightarrow(2)$, ולכן נוכיח רק ש-$(2)\Leftarrow(6)$. לכל טיפוס $p\in D_n(T)$ נבחר נוסחה φ_p שמבודדת אותו. כעת, בהינתן נוסחה $\varphi(\bar{x})$ (ונניח שהאורך של $\bar{x}$ הוא n) נגדיר $\Gamma_\varphi=\{p\in D_n(T):\varphi\in p\}$ ו-$\psi_\varphi=\bigvee\{\varphi_p:p\in\Gamma_\varphi\}$. כיוון ש-$D_n(T)$ סופית ψ_φ היא נוסחה, וקל לוודא ש-$\psi_\varphi\equiv\varphi$. ■

נראה עתה שימוש נוסף לכלים שפיתחנו בסעיף זה:

3.6.19 משפט *(Vaught)*: תהי T תורה שלמה בת מניה, אזי לא יתכן של-T יש בדיוק שני מודלים בני מניה (עד כדי איזומורפיזם).

הוכחה: נניח ש-T אינה קטגורית ב-$\aleph_0$. ממשפט 3.6.19 אנחנו יודעים ש-$D_n(T)$ אינסופית, לאיזה n טבעי. מטענה 3.6.5 אפשר להניח בה"כ שלכל n $|D_n(T)| \le \aleph_0$, כי אחרת ל-T יש מספר לא בן-מניה של מודלים לא איזומורפים, וסיימנו. לכן, לפי משפטון 3.6.4 יש ל-T מודל רווי בן-מניה, נסמנו M_1. לפי משפט 3.6.19 יש טיפוס $p \in D_n(T)$ לאיזה n טבעי, כך ש-p אינו מבודד. לכן לפי משפט השמטת הטיפוס יש מודל בן-מניה של T שמשמיט את p, נסמנו M_3. נראה שיש מודל M_2 שמגשים את p אך אינו רווי, ובזאת נגמור, שכן p מוגשם ב-M_1, מהיות המודל רווי, לכן M_1 אינו איזומורפי ל-M_3, ומאותו השיקול גם M_2 אינו איזומורפי ל-M_3, כיוון ש-M_2 אינו רווי נקבל שגם M_2 אינו איזומורפי ל-M_1, ובזאת מצאנו שלושה מודלים בני מניה שונים של T.

עלינו למצוא, אם כן, מודל M_2 כנדרש. יהי $M \models T$ מודל בן-מניה שבו p מוגשם, נאמר ע"י $\bar{a} \in M$. נוסיף למילון של T קבועים אישיים חדשים $c_0,\dots,c_{n-1}$, ונעשיר את M למבנה M^+ במילון החדש, ע"י שנגדיר $c_i^M = a_i$. נגדיר $T^+ = Th(M^+)$, אזי זו תורה בת מניה ושלמה. נראה כי $|D_k(T^+)| \ge |D_k(T)|$: אם $p \in D_k(T)$ ו-$M \prec N$ מגשים את p, נאמר ע"י $\bar{a}_p \in N$, אז אם נעשיר את N למבנה N^+ במילון החדש, ע"י שנגדיר $c_i^N = a_i$ נקבל ש-$M^+ \prec N^+$ (למשל, לפי קריטריון טרסקי-ווט), לכן ההעתקה $h: D_k(T) \to D_k(T^+)$ הנתונה ע"י $h(p) = tp(\bar{a}_p, \phi, N^+)$ מוגדרת היטב (כי לפי קריטריון טרסקי-ווט $h(p)$ ספיקה סופית ב-M^+, ולכן גם ב-M, ויוצא שאמנם $h(p) \in D_k(T^+)$). כעת קל לבדוק ש-h חח"ע.

מכאן, ש-T^+ תורה שלמה בת-מניה שאינה קטגורית ב-$\aleph_0$, ולכן יש לה מודל M_2^+ שהוא בן-מניה ואינו רווי. נגדיר $M_2 = M_2^+ \restriction_{\tau(T)}$ אז p מוגשם ב-M_2 (ע"י הסדרה $c_0^{M_2^+},\dots,c_{n-1}^{M_2^+}$) ואינו רווי (כי אם $q \in S^1(B, M_2^+)$ אינו מוגשם ב-M_2^+ - ומהנחתנו יש טיפוס q כזה לאיזו B סופית – אזי הטיפוס $q' = \{\varphi(x,\bar{b},\bar{c}^{M_2^+}) : \varphi(x,\bar{b},\bar{c}) \in q\}$ אינו מוגשם ב-M_2). בזא סיימנו את הוכחת המשפט. ■

3.6.20 סבה: דגכגדכ

תרגילים – מודלים בני מניה

1. אם T שלמה ויש לה מודל סופי, אזי ל-T יש מודל אחד ויחיד עד כדי איזומורפיזם.

2. מצאו תורה שלה בדיוק שלושה מודלים בני מניה. הדרכה: יהי $\tau = \{<, c_0, c_1, \cdots\}$ מילון ו- $M = \langle Q, <, c_n^M \rangle$ מבנה למילון, שעולמו המספרים הרציונלים, $<^M$ הסדר הרגיל על הרציונלים, ו- $c_n^M = \frac{1}{n}$ לכל n. הראו ש- $T = Th(M)$ עונה על הדרישות.

3. יהיו M מודל רווי ב- λ, ו- $A \subseteq M$ מעצמה קטנה מ- λ. אזי:

   א. אם לכל $a \in M$ מתקיים $\left|S^1(Aa, M)\right| < \lambda$ אז $\left|S^2(A, M)\right| < \lambda$.

   ב. אם לכל $B \subseteq M$ סופית $\left|S^1(A \cup B, M)\right| < \lambda$ אז $\left|S^n(A, M)\right| < \lambda$ לכל n.

4. בשאלה זו נסביר את שימוש במושג "קבוצת טיפוסים צפופה", המופיע במשפט 3.6.15. באותה הזדמנות, נסביר גם את השם "משפט הקומפקטיות".

   א. נאמר שקבוצה $\Gamma \subseteq D_n(T)$ היא סגורה אם קיימת קבוצת נוסחות Δ כך שלכל $p \in \Gamma$ מתקיים ש- $\Delta \subseteq p$. הוכיחו אוסף הקבוצות הפתוחות ב- $D_n(T)$ מהווה טופולוגיה, ושהטופולוגיה המתקבלת היא האוסדורף.

   ב. הראו שמשפט הקומפקטיות שקול לעובדה שהטופולוגיה שהוגדרה בסעיף הקודם היא קומפקטית.

   ג. הראו שכל קבוצה פתוחה ב- $D_n(T)$ היא גם סגורה.

   ד. הראו שקבוצת טיפוסים המקיימת את ההגדרה הניתנת במשפט 3.6.14 היא אמנם צפופה בטופולוגיה שקיבלתם.

5. תהי T תורה שלמה בת מניה. הראו שכל שני מודלים אטומיים בני מניה של T הם איזומורפים. הדרכה: השתמשו ברעיונות של הוכחת יחידות המודל הרווי.

6. הראו שאם T תורה שלמה בת מניה כך ש- $D_n(T)$ בת מניה לכל n אז ל-T יש מודל אטומי בן מניה.