ג. קומבינטוריקה כללית

ג.1 עוצמות ושוויון עוצמות

קומבינטוריקה היא ענף במתמטיקה, העוסק בעיקר בשאלה: "כמה איברים יש בקבוצה נתונה?". התואר "כללית", שנלווה למלה "קומבינטוריקה" בכותרת חלק זה, בא להדגיש, שבשלב ראשון נעסוק בעקרונות קומבינטוריים, החלים על קבוצות *כלשהן*, כולל קבוצות אינסופיות.

הצהרה אחרונה זו מעוררת, מן הסתם, תמיהה עוד בטרם נתחיל. מה פירוש "מספר איברים בקבוצה אינסופית"? מה עוד ניתן לפרט כאן פרט לכך, ש"מספר" האיברים בקבוצה כזו הוא אינסופי? אנו נראה בפרק זה, שיש אכן מקום לפירוט, ושיש אכן גדלים שונים גם בתחום האינסוף. דבר זה יוביל אותנו להרחבת מאגר המספרים, בהם אנו משתמשים למדידת קבוצות סופיות (הלא הוא N), למאגר רחב יותר, שיאפשר גם מדידת קבוצות אינסופיות. אנו נעשה זאת, כמובן, באופן, שיכליל בצורה טבעית את מושג המספר הטבעי המונה ("סופר")[1].

כדי שהרחבה מהסוג שהבטחנו לפני רגע תיעשה כראוי, היה רצוי מאוד, שתהיה לנו הגדרה ראויה לשמה של מושג המספר הטבעי. בשלב זה, לרוע המזל, אין בידינו הגדרה כזו. כדי להיווכח בכך, נסו להסביר לעצמכם, או (להבדיל) לילד קטן, מה זה "חמש", "שלושים" או "מספר". ספק בלבי אם תצליחו. אין פירוש הדבר, אבל, שאין לכולנו *הבנה* טובה של משמעות מושגים אלו. הדרך שנלך בה, עת נכליל את מושג המספר, תסתמך על ניתוח הבנה זו.

כדי לקבל פרספקטיבה טובה יותר על מה שאנו עומדים לעשות, הבה נחזור לדוגמה של מושג ה"כיוון של קרן", אותו הגדרנו בפרק הקודם. נניח שמישהו מבין הקוראים היה נשאל: "מה זה כיוון של קרן?", *לפני* שקרא את הפרק הקודם. האם היתה ההגדרה הרשמית, אותה הבאנו שם, הדבר הראשון, שהיה עולה על דעתו? קשה להאמין. למעשה, ספק אם היה מצליח להגיע להגדרה כלשהי מתקבלת על הדעת. ייתכן, שהיה אומר, שכיוון של קרן זה המספר, שמודד את הזווית בינה ובין קרן ייחוס מסוימת. זוהי אינה הגדרה מוצלחת במיוחד. ראשית, מושג הכיוון ברור לנו, ואנו משתמשים בו, עוד

---

[1] הכוונה למספרים הטבעיים, כשהם בצורה של "אחת, שתיים, שלוש, ארבע...". בצורה זו משמשים הם למניית מספר האיברים בקבוצות סופיות. למספרים הטבעיים בצורתם "ראשון, שני, שלישי, רביעי..." קוראים, לעומת זאת, מספרים סודרים, כי הם משמשים לצורך סידור איברים בתוך קבוצה.

בטרם נדע למדוד אותו (אנו הרי מודדים *משהו*, לא?). שנית, אותו כיוון עצמו ניתן למדוד בעזרת מספרים שונים: המספר תלוי ביחידת המידה ובקרן הייחוס. כיוון שכך, ברור שהכיוון אינו יכול להיות דבר, *זהה* עם המספר. לעומת זאת, אין כל בעיה להגדיר במדויק, מתי יש לשתי קרניים *אותו כיוון*. קצת חשיבה תוביל אותנו בדיוק ליחס D של הפרק הקודם: לשתי קרניים יש אותו כיוון, אם אחת מהן מוכלת בשנייה, או אם הן מקבילות ונמצאות באותו צד של הישר, המחבר את נקודות ההתחלה שלהן. יחס זה הינו, כזכור, יחס שקילות.

המצב, שתיארנו כרגע, הינו מצב שחוזר הרבה. אנו מתחילים *ביחס* מוגדר היטב בין עצמים מסוימים. כשיחס זה הינו יחס *שקילות*, אנו חשים, שיש משהו המשותף לכל שני עצמים, המתייחסים לפיו זה לזה. בצעד הבא אנו מבצעים תהליך של *הפשטה* (אבסטרקציה). בלי להגדיר במדויק את אותו "דבר משותף", אנו מכניסים לשימוש מונח חדש עבורו. במקום לדבר על קיום היחס בין שני עצמים, אנו מתחילים לדבר אז על *השוויון* עבורם של אותו דבר משותף. כך במקום להגיד, ששתי קרניים נמצאות ביחס D זו לגבי זו, אנו אומרים, שיש להן אותו כיוון. אנו עושים זאת, בטרם הגדרנו מה זה בכלל "כיוון". הבנת המושג "שוות כיוון" קודמת אפוא להבנת מושג הכיוון!

אם נסמן ב- $\mathrm{direction}(a)$ את הכיוון של הקרן a, הרי הרעיון המרכזי סביב מושג הכיוון הוא, ש- aDb אם"ם $\mathrm{direction}(a) = \mathrm{direction}(b)$. תהליך דומה מקובל עבור כל יחס R, שהוא יחס שקילות: אנו עוברים בתהליך הפשטה מטענה מהצורה aRb לטענה מהצורה $d_R(a) = d_R(b)$, כש- d_R הוא מושג חדש, שהתקבל על-ידי *הפשטה*. ל- d_R אין בדרך-כלל הגדרה. כל שאנו יודעים עליו הוא, ש:

$$d_R(a) = d_R(b) \quad \Leftrightarrow \quad aRb$$

למה תהליך זה מקובל? בראש ובראשונה, משום שפסיכולוגית, נוח לנו יותר לעבוד עם שוויונות מאשר עם יחסים. כך ברור לנו, למשל, שאם $d_R(a) = d_R(b)$ ו- $d_R(b) = d_R(c)$, אז $d_R(a) = d_R(c)$. פחות רגילים אנו לרעיון, ש"היחס R הוא טרנסיטיבי" (שזה אותו הדבר בדיוק!). סיבה חשובה נוספת היא, שאחרי שאנו קונים הבנה אינטואיטיבית של העצמים החדשים, אותם יוצר תהליך ההפשטה, אנו מתחילים לעשות עמם מה שאנו עושים עם כל סוג של עצמים: אנו מגדירים יחסים מועילים ופעולות מועילות על עצמים אלה. גילוין של עובדות חשובות (גם כאלה, שאינן מתייחסות ישירות לעצמים החדשים) יכול להיות אז קל מאוד. בדוגמה של כיוונים, למשל, מוביל מושג הכיוון למושג הוקטור (במרחב) ואחר-כך לתחשיב הוקטורים (שהינו, בדרך-כלל, מכשיר הרבה יותר נוח לעבודה מאשר הגיאומטריה האוקלידית הרגילה).

ומה אם מישהו לוחץ ושואל שאלה כמו: "אז מה זה בכל זאת 'כיוון'?". לאחד כזה ניתן לתת שתי תשובות. האחת, המעשית, היא: "מה זה בכלל חשוב, מה הם כיוונים? העיקר הוא, שאנו יכולים לעבוד איתם!". אנלוגיה טובה נוכל להביא כאן משחמט: אפשר להסתבך קשות בניסיון לענות על השאלה: מהו "פרש" בשחמט? זה בוודאי לא הכלי המגולף, שאנו מזיזים על הלוח (אפשר הרי לשחק שחמט בעל-פה, ללא שימוש בכלים פיזיים כלל!). בסופו של דבר, מה שקובע את מהותו של הכלי בשחמט אלה הכללים, הקשורים בו ובצורת הזזתו, כלומר: הפעולות שעושים אתו.
הצורה השנייה לענות על שאלה מהסוג "מה זה כיוון?" (או כל מונח אחר, שמקורו בתהליך אבסטרקציה), היא לספק בכל זאת הגדרה כלשהי, אפילו מסובכת, כך שיובטח הקשר הבסיסי:

$$aRb \iff d_R(a) = d_R(b)$$

זוהי דרכם של המתמטיקאים, כיוון שאלה מרגישים חובה לא להשאיר דברים תלויים באוויר באופן מיסטי. יש להם אפילו דרך סטנדרטית איך לעשות זאת, אותה ראינו בפעולה בפרק הקודם. היא מתבססת על כך, שאם R יחס שקילות, אז:

$$aRb \iff [a]_R = [b]_R$$

השוואה של נוסחה זו עם הקשר הבסיסי, אותו אנו מחפשים, מראה, שנוכל להגדיר פשוט:

$$d_R(a) =_{Df} [a]_R$$

ההפשטה המבוקשת יכולה אפוא להינתן על-ידי מחלקות השקילות, אותן היחס משרה. בדוגמה של "כיוון", למשל, אנו יכולים להגדיר את הכיוון של קרן a בתור מחלקת השקילות של a ביחס ל- D, דהיינו: הכיוון של קרן a הוא קבוצת כל הקרניים, שיש להן "אותו כיוון" כמו a. כך בדיוק הגדרנו אכן את הכיוון של a בפרק הקודם! (נעיר שוב, שאנו מבינים היטב מתי לשתי קרניים יש "אותו כיוון" גם בלי להגדיר מה זה "כיוון", ושמושג ה"כיוון" היה היסטורית מובן ושימושי, עוד בטרם ניתנה לו ההגדרה הרשמית הזו).

נחזור עתה אל מושג המספר. גם ביחס אליו, מה שאנו מבינים תחילה הוא מה פירוש הדבר, שלשתי קבוצות יש *"אותו מספר"* של איברים. מושג המספר עצמו מובן רק אחר-כך, ומתקבל בתהליך הפשטה.[2]

[2] טעות נפוצה היא לחשוב, שכדי להבין מה זה "אותו מספר" צריך תחילה להבין את פשר המלים "אותו" ו"מספר". אין זה נכון. רובנו, למשל, מבינים את פירוש הביטוי "ישב על המדוכה" בלי שיהיה לנו מושג מה זה "מדוכה"...

ובכן, מתי נאמר, ששתי קבוצות סופיות הן שוות בגודלן? אולי תאמרו: אם נקבל אותה תוצאה, כאשר נספור כמה איברים יש בכל אחת. זה נכון, אמנם, אבל מבוסס כבר על *אמצעי*, שפותח לצורך מתן תשובה לשאלה זו עצמה (לא תמיד האמצעי היעיל ביותר, אגב!). לאמתו של דבר, אפשר לדעת על שתי קבוצות, שהן שוות בגודלן, בלי לדעת כלל לספור (וילדים קטנים אכן עושים זאת לפעמים). נניח, לדוגמה, שאנו נכנסים לאולם ריקודים ומגלים בו זוגות רוקדים. נניח עוד, שכולם מעורבים, וההתלהבות בשיאה: איש אינו יושב בצד. בלי שום ספירה ברור לנו מיד, שמספר הנשים בחדר (לפני שנכנסנו אנו) היה שווה למספר הגברים בו. בדומה, אין כל צורך בספירה כדי לדעת, שבכל לוח שחמט יש מספר שווה של משבצות לבנות ושחורות!

ברור משתי הדוגמאות, ששתי קבוצות הן "שוות-גודל" אם ניתן לבצע התאמה של זוגות בין אחת לשנייה. זוהי ההבנה היסודית. רק מאוחר יותר בהיסטוריה האנושית (או בהתפתחותו של ילד) נעשות *אבסטרקציות*. אז ניתן, למשל, השם "חמש" למשותף לכל הקבוצות, שהן שוות-גודל עם קבוצת האצבעות ביד ימין של אדם נורמלי, והשם "עשר" – למשותף לאלה, שהן שוות-גודל לקבוצת האצבעות בשתי הידיים. מושג המספר עצמו נוצר בשעתו על-ידי אבסטרקציה נוספת. שום הגדרות לא ניתנו אז!

הגיע הזמן, אבל, *שאנו* ניתן הגדרה כלשהיא.

הגדרה:

שתי קבוצות A ו- B נקראות *אקויפוטנטיות* (או שוות-עוצמה) אם קיימת פונקציית שקילות ביניהן.

סימון: את העובדה ש- A ו- B אקויפוטנטיות נסמן ב- $A \sim B$.

טענה:

יחס האקויפוטנטיות בין קבוצות הוא יחס שקילות.

הוכחה:

(א) רפלקטיביות: $A \sim A$ לכל A, כי i_A פונקציית שקילות מ- A על A.

(ב) סימטריות: נניח $A \sim B$. תהי f פונקציית שקילות מ- A על B. אז f^{-1} היא פונקציית שקילות מ- B על A. לכן $B \sim A$.

(ג) טרנסיטיביות: נניח $A \sim B$ ו- $B \sim C$. תהי f פונקציית שקילות מ- A על B, ותהי g פונקציית שקילות מ- B על C. אז $g \circ f$ היא פונקציית שקילות מ- A על C. לכן $A \sim C$.

%% הערה:

יחס האקויפוטנטיות בין קבוצות אינו, למעשה, יחס במובן הרשמי, כפי שהגדרנוהו בפרק הקודם: אי אפשר לתאר אותו בתור *קבוצה* של זוגות בלא להסתבך בפרדוקסים. כמו $\in$, $=$ ו- $\subseteq$, הוא יחס במובן *מוכלל*, מעל "אוסף כל הקבוצות". בהתאם, משמעות הטענה האחרונה היא, שיחס האקויפוטנטיות הוא "יחס שקילות" במובן מוכלל (דהיינו: רפלקסיבי, טרנסיטיבי ואנטי-סימטרי).

%%

דוגמאות פשוטות של קבוצות אקויפוטנטיות הן קבוצת הימים בשבוע וקבוצת הגמדים של שלגייה, כמו גם שתי קבוצות המשחקות זו נגד זו במשחק כדורגל (בתנאי ששום שחקן לא הורחק על-ידי השופט). דוגמאות חשובות יותר מהבחינה המתמטית (יחד עם פונקציות השקילות המתאימות) נכללות בטבלה ג.1.[3]

טבלה ג.**1**: דוגמאות לקבוצות שוות-עוצמה

	קבוצות	*פונקציית שקילות*
(1)	$\mathbf{N} \sim \mathbf{N}^+$	$\lambda n \in \mathbf{N}.\ n+1$
(2)	$\mathbf{N}_{\text{even}} \sim \mathbf{N}_{\text{odd}}$	$\lambda n \in \mathbf{N}_{\text{even}}.\ n+1$
(3)	$\mathbf{N} \sim \mathbf{N}_{\text{even}}$	$\lambda n \in \mathbf{N}.\ 2n$
(4)	$\mathbf{N} \times \mathbf{N} \sim \mathbf{N}$	$\lambda m \in \mathbf{N},\ k \in \mathbf{N}.\ \frac{(m+k)(m+k+1)}{2} + m$
(5)	$(a<b)\quad [a,b] \sim [0,1]$	$\lambda x \in [a,b].\ \frac{x-a}{b-a}$
(6)	$(a<b)\quad (a,b) \sim (0,1)$	$\lambda x \in (a,b).\ \frac{x-a}{b-a}$
(7)	$\mathbf{R} \sim (-1,1)$	$\lambda x \in \mathbf{R}.\ \frac{x}{1+\lvert x\rvert}$
(8)	$\mathbf{R}^+ = (0,\infty) \sim (0,1)$	$\lambda x \in (0,\infty).\ \frac{x}{1+x}$
(9)	$A \times B \sim B \times A$	$\lambda a \in A, b \in B.\ \langle b, a\rangle$
(10)	$A \times B \to C \sim A \to (B \to C)$	$Cu = \lambda f \in A \times B \to C.\ \lambda x \in A.\ \lambda y \in B.\ f(x,y)$
(11)	$P(E) \sim E \to \{0,1\}$	$\lambda A \in P(E).\ \chi_A^{(E)}$

[3] כזכור, $\mathbf{N}^+$ היא קבוצת המספרים הטבעיים בלי אפס, $\mathbf{N}_{\text{even}}$ – קבוצת המספרים הזוגיים, ו- $\mathbf{N}_{\text{odd}}$ – קבוצת המספרים האי-זוגיים.

בשתי הדוגמאות האחרונות בטבלה ג.1 נתקלנו כבר בפרק ב.4 (ראה סעיף ה שם אודות פונקציית Curry ודוגמה (4) בעמוד 130). את מרבית הדוגמאות האחרות נשאיר כתרגילים לקורא. אנו נסתפק כאן בהוכחת דוגמה מס' (7).

תהי אפוא $f = \lambda x \in R.\dfrac{x}{1+|x|}$. ברור ש- f מוגדרת אכן לכל $x \in \mathbf{R}$. כמו כן, לכל $x \in \mathbf{R}$ מתקיים: $|f(x)| = \dfrac{|x|}{1+|x|}$, ולכן $0 \le |f(x)| < 1$, וממילא $f(x) \in (-1,1)$. מכאן, שאכן $f: \mathbf{R} \to (-1,1)$. כדי להראות ש- f פונקציית שקילות, די שנראה ש- $g = \lambda x \in (-1,1).\dfrac{x}{1-|x|}$ היא פונקציה הפוכה ל- f. ברור ש- g אכן מוגדרת לכל $x \in (-1,1)$, וש- $\mathbf{R}$ היא טווח שלה. חישוב פשוט מראה, ש- $g(f(x)) = x$ לכל $x \in \mathbf{R}$ ו- $f(g(x)) = x$ לכל $x \in (-1,1)$. לכן $f \circ g = i_{(-1,1)}$ ו- $g \circ f = i_{\mathrm{R}}$. מכאן, שאכן $g = f^{-1}$.

הערות:

1. עבור מרבית שאר הדוגמאות קל למצוא פונקציה הפוכה מתאימה, ולכן קל להוכיחן באופן דומה לזה של הוכחת דוגמה (7). דוגמה מס' (4) היא יוצאת מן הכלל כאן. פה יהיה קל יותר להוכיח, שהפונקציה בה מדובר היא ח.ח.ע. ועל $\mathbf{N}$. דוגמה זו מהווה תרגיל, שהינו יחסית קשה יותר, ועוד נחזור אליה מאוחר יותר (בפרק ג.4).

2. הפונקציה בדוגמה (2) היא הצמצום של הפונקציה בדוגמה (1) ל- $\mathbf{N}_{\text{even}}$. בדומה, הפונקציה בדוגמה (6) היא הצמצום של הפונקציה בדוגמה (5) לקטע (a, b), והפונקציה בדוגמה (8) היא הצמצום של הפונקציה בדוגמה (7) לקטע $(0, \infty)$. כל זאת מדגים את העובדה, שהשימוש בצמצומים של פונקציות שקילות הוא נפוץ לצורך בניית פונקציות שקילות אחרות. שתי העובדות הפשוטות הבאות אודות צמצומים כאלה עשויות אז להועיל. את הוכחתן נשאיר לקורא.

טענה:

1. אם f היא פונקציה ח.ח.ע. מ- A אל B ו- $X \subseteq A$, אז f/X היא פונקציית שקילות בין X ל- $f(X)$ (התמונה של X לפי f), ולכן $X \sim f(X)$. בפרט $A \sim f(A)$ במקרה זה.

2. תהי $f: A \to B$ פונקציית שקילות. נניח ש- $X \subseteq A$ ו- $Y \subseteq B$ הן שתי קבוצות, כך ש- $f(X) \subseteq Y$ ו- $f^{-1}(Y) \subseteq X$, אז $X \sim Y$, ו- f/X היא פונקציית שקילות ביניהן.[4]

דוגמה

בדוגמה מס' (7) ראינו ש- $g = \lambda x. \dfrac{x}{1-|x|}$ היא הפונקציה ההפוכה ל- f (כאשר $f = \lambda x. \dfrac{x}{1+|x|}$). כדי להסיק את דוגמה (8) מדוגמה (7) די לכן להראות (על-פי החלק השני של הטענה האחרונה), שאם $x \in (0, \infty)$ אז $f(x) \in (0,1)$, ושאם $x \in (0,1)$ אז $g(x) \in (0, \infty)$. זה קל.

דוגמאות (3), (7) ו- (8) עלולות להיראות פרדוקסליות במבט ראשון. דוגמאות אלה מציגות מקרים, בהם קבוצה היא שוות-עוצמה עם קבוצה, החלקית לה ממש. מהגדרותינו יוצא אכן, ש"יש אותו מספר של מספרים טבעיים זוגיים ושל מספרים טבעיים בכלל", וכן ש"יש אותו מספר של מספרים ממשיים בין 0 ל- 1 ומספרים ממשיים חיוביים בכלל". זה סותר את האינטואיציה הבסיסית שלנו, שאם $A \subset B$, אז ב- A יש פחות איברים מאשר ב- B. ברם, אינטואיציה זו נקנתה מתוך התנסות בקבוצות *סופיות* בלבד, ואילו בדוגמאות הללו מדובר בקבוצות *אינסופיות*. כדאי, שהקוראים יסכינו מרגע זה ואילך עם העובדה, שאינטואיציות הנכונות לקבוצות סופיות אינן תמיד נכונות לקבוצות אינסופיות, ועוד נראה דוגמאות רבות לכך.

אחרי שהגדרנו, מתי שתי קבוצות הן "שוות-עוצמה", נעבור בשלב הבא לבצע את תהליך ההפשטה, אותו תיארנו בראשית פרק זה. כתוצאה מכך יתווסף מושג חדש לעולם הקבוצות:

"הגדרה":

לדבר המשותף לקבוצה A ולכל הקבוצות, שהן אקויפוטנטיות עמה, קוראים *העוצמה* של A (או "מספר האיברים ב- A", או ה"קרדינליות של A"), ומסמנים אותה ב- $|A|$ (או ב- $\overline{\overline{A}}$).

התכונה העיקרית של מושג העוצמה הינה:

$$\boxed{|A| = |B| \iff A \sim B}$$

[4] את הביטוי $f^{-1}(Y)$ אפשר להבין כאן בשתי צורות: כמקור של Y לפי f, או התמונה של Y לפי f^{-1}. קל לראות, ששני הפירושים הם זהים במקרה זה (הוכח!).

ברור, *שלא* הגדרנו כאן בדיוק, מה זה $|A|$. הגדרנו רק, מה פירוש הדבר ש- $|A| = |B|$. בהמשך נגדיר עוד יחסים אחרים על עוצמות (כמו $|A| < |B|$) ופעולות עליהן (כמו $|A| + |B|$). אנו נשתמש בכל אלה בהצלחה, כשאנו מסתמכים אך ורק על מושג העוצמה, שמספק תהליך ההפשטה, ומבלי שניתן למושג זה הגדרה מדויקת. בכך משחזרים אנו, למעשה, את דרכו של קנטור, אבי תורת הקבוצות. נרגיע אבל את קוראינו, שעובדה זו מדאיגה אותם (ובצדק!), שבמסגרת תורת הקבוצות האקסיומטית ניתנת גם ניתנת הגדרה מדויקת למושג "העוצמה של קבוצה" במונחים של תורת הקבוצות בלבד. הטענה בתוך המסגרת למעלה הופכת שם להיות *משפט* (עם הוכחה). ברם, בטרם אפשר יהיה להציג הגדרה זו, יש ללמוד תחילה חומר, שהוא הרבה מעבר לטווח של קורס זה.

כדאי לציין בהקשר זה, שבטקסטים לא מעטים, העוסקים בתורת הקבוצות הנאיבית, מפעילים את אותה הפרוצדורה, שהפעלנו במקרה של הגדרת "כיוון". במלים אחרות: מגדירים את $|A|$, העוצמה של A, ***בתור מחלקת השקילות של A לפי יחס האקויפוטנציה.*** הבעיה עם "הגדרה" זו הינה, שיחס האקויפוטנציה הינו, כזכור, יחס רק במובן *מוכלל*: אי אפשר לתאר אותו בתור *קבוצה* של זוגות! יתר על כן, גם "מחלקות השקילות" שלו אינן קבוצות (לו היו קבוצות, היינו מסתבכים בסתירות לוגיות, הדומות לזו של פרדוקס ראסל). כיוון שכך, אין הן עצמים ואין הן יכולות, לכן, להיות איברים בשום קבוצה – גם לא **N**. (היסטורית, ההגדרה המדויקת הראשונה, שניסה מישהו לתת למושג "עוצמה", היתה בדיוק זו – והיא אכן הובילה לסתירות!).

ג.2 עוצמות סופיות ואינסופיות

לא פעם במהלך הקורס עד כאן השתמשנו במושגים של "קבוצה סופית" ו"קבוצה אינסופית", מתוך הנחה, שאלו מושגים ברורים. כאשר מפתחים את תורת הקבוצות בצורה מסודרת, מגדירים, כמובן, גם מושגים אלה. הדבר יכול להיעשות בשני מסלולי התקדמות אפשריים. במסלול האחד מגדירים תחילה מהי קבוצה סופית (על סמך אפיון, המופיע כ"מסקנה" בסוף פרק זה). לאחר מכן מוגדרים המספרים הטבעיים בתור העוצמות של קבוצות סופיות, ותכונותיהם הבסיסיות מוכחות על סמך זאת. במסלול השני מגדירים תחילה את המספרים הטבעיים (בצורה אחרת, כמובן), מוכיחים את תכונותיהם הבסיסיות על סמך הגדרה זו, ***ואז*** מגדירים קבוצות סופיות בעזרתם. הדבר נעשה כך, שהמספרים הטבעיים ישמשו כעוצמות של קבוצות סופיות, וקבוצה תהיה סופית, אם ורק אם עוצמתה הינה מספר טבעי. בקורס זה נלך במסלול השני. יהיה רק הבדל משמעותי אחד: אנו ***לא*** נגדיר את המספרים הטבעיים, אלא נניח, שאנו מכירים אותם ואת תכונותיהם הבסיסיות (אותן למדנו בבית-הספר העממי). כיוון שכך, יש להתייחס להגדרה של קבוצות סופיות, שניתן מיד, ***כהגדרת עבודה***. אין לראותה בגדר הגדרה במובן המדוקדק של המלה.

הגדרה:

1. **קבוצה A נקראת *סופית* אם קיים מספר טבעי n כך ש- A אקויפוטנטית עם $\mathbf{N}_n=\{0, 1, \ldots, n-1\}$. n זה נחשב אז כעוצמת הקבוצה A (או "מספר איבריה"), דהיינו $|A|=n$ במקרה זה.**
2. **קבוצה תיקרא אינסופית אם אינה סופית.**

הערות:

1. מההגדרה ברור, שהמספרים הטבעיים הינם העוצמות של הקבוצות הסופיות.
2. הגדרתנו כוללת את המקרה $n=0$. במקרה זה הקבוצה $\mathbf{N}_n=\{0, 1, \ldots, n-1\}$ היא פשוט $\varnothing$. הקבוצה הריקה נחשבת, לכן, קבוצה סופית, ומספר איבריה הוא המספר הטבעי 0.[5]
3. החלק השני של הגדרת קבוצה סופית, זה המתייחס למספר איבריה, מכיל הנחה סמויה: שלכל קבוצה A ייתכן מספר טבעי n אחד לכל היותר, כך ש- $A\sim\mathbf{N}_n$

[5] זו הסיבה, שבמסגרת תורת הקבוצות טבעי לקבל את אפס בתור מספר טבעי.

ההנחה מתבטאת בצירוף "n זה", שמניח יחידותו. אנו מניחים, אם כן, שלא ייתכן, למשל, שקבוצה A תהיה אקויפוטנטית גם עם $\{0, \ldots, 1{,}000{,}000\}$ וגם עם $\{0, \ldots, 999{,}999\}$. על מה מבוססת אמונה זו? לרובנו – על ניסיוננו עם קבוצות קטנות. למעשה, אפשר (וצריך!) להוכיח זאת:

משפט:

אם $A \sim \mathbf{N}_n$ ו- $A \sim \mathbf{N}_k$ $(n, k \in \mathbf{N})$, אז $n = k$.

את ההוכחה נביא בנספח לפרק זה.

4. מההגדרה ברור, שאם A סופית ו- $B \sim A$, אז B סופית (וכמובן $|B| = |A|$).

טבלה ג.2 בעמוד הבא כוללת רשימה של תכונות ידועות היטב של קבוצות סופיות. אנו נקבל תכונות אלו ללא הוכחה (הוכחות מלאות לאותן תכונות, שאינן מיידיות מההגדרות, ניתנות במסגרת קורס מלא בתורת הקבוצות האקסיומטית. חלק מהן ניתנות במסגרת הנספח לפרק זה).

מרשימה זו ומהגדרת קבוצה אינסופית, נובעת מיידית רשימת התכונות הבאה של קבוצות אינסופיות:

1. אם A אינסופית ו- $B \sim A$, אז B אינסופית.
2. אם A אינסופית ו- $A \subseteq B$, אז B אינסופית.
3. אם A אקויפוטנטית עם קבוצה חלקית ממש שלה, אז A אינסופית.
4. אם A אינסופית ו- f פונקציה ח.ח.ע. מ- A ל- B, אז B אינסופית.
5. אם A אינסופית ו- f פונקציה מ- B על A, אז B אינסופית.

האם יש בכלל קבוצות אינסופיות? אינטואיטיבית, ברור שכן. למעשה, זה גם נובע ממה שראינו עד עכשיו! כך ראינו, ש- $\mathbf{N}$ אקויפוטנטית עם קבוצה חלקית ממש שלה ($\mathbf{N}_{\text{even}}$). לכן $\mathbf{N}$ אינסופית, מתכונה 3 ברשימה האחרונה. מאותה סיבה גם $\mathbf{R}^+$ אינסופית: היא אקויפוטנטית עם $(0,1)$, שהיא קבוצה חלקית ממש שלה (דוגמה (8) בטבלה ג.1). כיוון ש- $\mathbf{N} \sim \mathbf{N}_{\text{even}}$ ו- $\mathbf{R}^+ \sim (0,1)$, גם $\mathbf{N}_{\text{even}}$ ו- $(0,1)$ אינסופיות. כיוון ש- $\mathbf{R}^+ \subseteq \mathbf{R}$, גם $\mathbf{R}$ אינסופית (תכונה 2 ברשימה האחרונה).

השאלה המתבקשת עתה הינה: האם כל הקבוצות האינסופיות הינן אקויפוטנטיות, או שמא קיימת יותר מעוצמה אינסופית אחת? אנו נראה עתה, שהאפשרות השנייה היא הנכונה. זה יפתח את הפתח לתיאוריה עשירה ומרתקת של עוצמות אינסופיות. הפרקים הבאים יוקדשו בעיקרם לתיאוריה זו.

טבלה ג.2: תכונות בסיסיות של קבוצות סופיות

(1)	(i) לכל $n \in \mathbf{N}$, $\mathbf{N}_n = \{0, 1, \ldots, n-1\}$ הינה סופית (בפרט $\varnothing$ הינה סופית). (ii) אם $A \sim \mathbf{N}_n$ ו- $A \sim \mathbf{N}_k$ $(n, k \in \mathbf{N})$, אז $n = k$.
(2)	אם A סופית ו- $A \sim B$, אז B סופית.
(3)	(i) אם A סופית ו- $B \subseteq A$, אז B סופית ו- $\|B\| \leq \|A\|$. (ii) אם A סופית ו- $B \subset A$, אז B סופית ו- $\|B\| < \|A\|$.
(4)	(i) קבוצה סופית אינה אקויפוטנטית עם שום קבוצה חלקית-ממש שלה. (ii) אם $\|A\| = \|B\|$, A סופית, ו- $f: A \to B$ ח.ח.ע. **או** על B, אז f פונקציית שקילות מ- A על B.
(5)	אם A סופית ו- f פונקציה ח.ח.ע. מ- B ל- A, אז B סופית ו- $\|B\| \leq \|A\|$.
(6)	אם A סופית ו- f פונקציה מ- A על B, אז B סופית ו- $\|B\| \leq \|A\|$.
(7)	אם A סופית ו- R יחס שקילות על A, אז A/R סופית ו- $\|A/R\| \leq \|A\|$.
(8)	אם A ו- B סופיות, אז גם $A \cup B$, $A \times B$ ו- $A \to B$ הן סופיות, ומתקיים: (i) $A \cap B = \varnothing \;\Rightarrow\; \|A \cup B\| = \|A\| + \|B\|$ (ii) $\|A \times B\| = \|A\| \cdot \|B\|$ (iii) $\|A \to B\| = \|B\|^{\|A\|}$ (ובסימון אחר: $\|B^A\| = \|B\|^{\|A\|}$)

משפט:

$|\mathbf{N}^+| \neq |(0,1]|$. כלומר: $\mathbf{N}^+$ וקבוצת המספרים הממשיים בין 0 ל- 1 (כולל 1) אינן אקויפוטנטיות.

הוכחה:

אנו נסתמך על העובדה הבאה בדבר מספרים ממשיים בין 0 ל- 1: כל מספר כזה אפשר לייצג בצורה יחידה על-ידי שבר עשרוני אינסופי מהצורה:

$$0.\, d_1 d_2 d_3 d_4 \ldots$$

כאשר d_1, d_2, d_3, וכו' הן ספרות בין 0 ו- 9, וכך שאין מקום, שממנו ואילך כל הספרות הן אפסים (1/8, למשל, תיוצג על-ידי ...0.12499999 ולא על-ידי ...0.125000. 1 עצמו הוא ...0.9999). אנו נוכיח, שאין בכלל פונקציה מ- N^+ *על* [0,1) (וממילא אין פונקציית שקילות מ- N^+ על [0,1)). נוכיח זאת בדרך השלילה. נניח אפוא, ש- f היא פונקציה מ- N^+ על [0,1). נסמן ב- $(f(i))_j$ את הספרה ה- j של $f(i)$. נגדיר עתה מספר b בצורה הבאה:

$$b = 0.\,b_1 b_2 b_3 \ldots$$

כאשר

$$b_i = \begin{cases} 1 & (f(i))_i \neq 1 \\ \\ 2 & (f(i))_i = 1 \end{cases}$$

עתה $b \in (0,1]$, אבל $b \neq f(i)$ לכל i, כיוון ש- b ו- $f(i)$ שונים בספרה ה- i-ית שלהם. זוהי סתירה לכך ש- f היא על [0,1), כיוון ש- b אינו בתמונה של f (נשים לב, שבייצוג $0.\,b_1 b_2 b_3\ldots$ אין אפסים כלל, ולכן הוא ייצוג כשר למהדרין של מספר ממשי בקטע [0,1)).

הערה:

שיטת ההוכחה של המשפט האחרון נקראת "שיטת האלכסון". הסיבה היא, שאינטואיטיבית, מה שעושים בה, הוא הדבר הבא: מסדרים את $f(1)$, $f(2)$,... במטריצה האינסופית הבאה:

$$\begin{array}{llllll}
f(1) = & 0.f(1)_1 & f(1)_2 & f(1)_3 & f(1)_4 & \cdots \\
f(2) = & 0.f(2)_1 & f(2)_2 & f(2)_3 & f(2)_4 & \cdots \\
f(3) = & 0.f(3)_1 & f(3)_2 & f(3)_3 & f(3)_4 & \cdots \\
f(4) = & 0.f(4)_1 & f(4)_2 & f(4)_3 & f(4)_4 & \cdots \\
 & & & & & \searrow \\
\vdots & & \ddots & & &
\end{array}$$

המספר b נוצר (אינטואיטיבית) על-ידי שמתקדמים לאורך האלכסון של מטריצה אינסופית זו, ומחליפים את הספרות, שמוצאים שם, בספרות אחרות (ואין משתמשים ב- 0). כך מבטיחים, ש- b יהיה שונה בספרה אחת לפחות מכל אחד מהמספרים, המיוצגים במטריצה.

סימונים: את העוצמה של N^+ מסמנים ב- $\aleph_0$.

את העוצמה של [0,1) מסמנים ב- c או ב- $\aleph$.

המשפט האחרון הראה, לכן, ש- $\aleph_0 \neq$ א.

הערה:
כיוון ש- $\lambda n \in \mathbf{N}.\ n+1$ היא פונקציית שקילות בין $\mathbf{N}$ ל- $\mathbf{N}^+$, גם $|\mathbf{N}| = \aleph_0$.
כיוון ש- $\mathbf{N} \sim \mathbf{N}_{\text{even}}$ ו- $\mathbf{N}_{\text{even}} \sim \mathbf{N}_{\text{odd}}$, גם $|\mathbf{N}_{\text{even}}| = |\mathbf{N}_{\text{odd}}| = \aleph_0$.

הגדרה:

לקבוצות שעוצמתן $\aleph_0$ קוראים קבוצות *בנות-מניה* (*ב"מ*, בקיצור). במלים אחרות: קבוצה A נקראת בת-מניה אם"ם היא אקויפוטנטית עם $\mathbf{N}$ (או עם $\mathbf{N}^+$).

המשפט העיקרי של פרק זה מספק אפיונים של קבוצות אינסופיות. לצורך הוכחתו נזדקק ללמה הפשוטה הבאה, שיש לה חשיבות בפני עצמה:

למה:

אם $A \cap B = \varnothing$, $A' \cap B' = \varnothing$, $A \sim A'$ ו- $B \sim B'$, אז $A \cup B \sim A' \cup B'$.

הוכחה:
נניח ש- f היא פונקציית שקילות מ- A על A', וש- g היא פונקציית שקילות מ- B על B'. נגדיר $h: (A \cup B) \to (A' \cup B')$ על-ידי:

$$h(x) = \begin{cases} f(x) & x \in A \\ \\ g(x) & x \in B \end{cases}$$

(בסימון λ: $h = \lambda x \in A \cup B.\ \text{if } x \in A \text{ then } f(x) \text{ else } g(x)$). כיוון ש- $A \cap B = \varnothing$, h הינה מוגדרת היטב.[6] נראה ש- h היא פונקציית שקילות.

h ח.ח.ע.: נניח $h(x_1) = h(x_2)$. לא ייתכן ש- $x_1 \in A$ ו- $x_2 \in B$, כי אז $h(x_1) \in A'$, בעוד $h(x_2) \in B'$. נקבל אז לכן סתירה לכך, ש- $A' \cap B' = \varnothing$. בדומה, לא ייתכן גם ש- $x_1 \in B$ ו- $x_2 \in A$. אם, לעומת זאת, $x_1 \in A$ וגם $x_2 \in A$, אז השוויון $h(x_1) = h(x_2)$ פירושו $f(x_1) = f(x_2)$. כיוון ש- f ח.ח.ע., נקבל ש- $x_1 = x_2$. גם כאשר $x_1 \in B$ ו- $x_2 \in B$, נקבל ש- $x_1 = x_2$, הפעם בגלל חד-חד-ערכיות g. סה"כ $x_1 = x_2$ בכל המקרים האפשריים.

h על: נניח $y \in A' \cup B'$. אז $y \in A'$ או $y \in B'$. אם $y \in A'$, אז יש $x \in A$, כך ש- $f(x) = y$ (כיוון ש- f על A'). לכן $h(x) = y$. אם $y \in B'$, אז יש $x \in B$ כך ש- $g(x) = y$ (כי g על B'), ולכן $h(x) = y$. בכל מקרה יש $x \in A \cup B$ כך ש- $h(x) = y$.

---

[6] לו היה איבר y ב- $A \cap B$, אזי לא היה ברור, אם $h(y) = f(y)$, או שמא $h(y) = g(y)$!

הערה:

אלטרנטיבית, לא קשה להוכיח ש- $\lambda x \in A' \cup B'.\ \text{if}\ y \in A'\ \text{then}\ f^{-1}(y)\ \text{else}\ g^{-1}(y)$ הינה פונקציה הפוכה ל- h.

משפט:

התכונות הבאות של קבוצה A הינן שקולות:

(א) A מכילה קבוצה חלקית בת-מניה.

(ב) A אקויפוטנטית עם איזו תת-קבוצה חלקית-ממש שלה.

(ג) A הינה אינסופית.

הוכחה:

(א) $\Leftarrow$ (ב):

נראה תחילה, שאם B בת-מניה, אז ל- B קבוצה חלקית-ממש, שהיא אקויפוטנטית עמה. זה ודאי נכון ל- $\mathbf{N}$, כי $\mathbf{N} \sim \mathbf{N}^+ \subset \mathbf{N}$. עתה, אם $B \sim \mathbf{N}$, אז יש פונקציית שקילות f מ- $\mathbf{N}$ על B. תהי $B^+ = f(\mathbf{N}^+)$. אז $B^+ \sim \mathbf{N}^+$, וברור ש- $B^+ \subset B$ (כי $f(0) \notin B^+$). כיוון ש- $B \sim \mathbf{N} \sim \mathbf{N}^+ \sim B^+$, אנו מקבלים ש- $B^+ \sim B$, ולכן B^+ קבוצה כמבוקש.

נניח עתה, ש- A מכילה קבוצה ב"מ B. כפי שראינו זה עתה, יש $B^+ \subset B$ כך ש- $B^+ \sim B$. עתה $(A - B) \cap B = \varnothing$, וממילא $(A - B) \cap B^+ = \varnothing$ (כי $B^+ \subset B$). כמו כן $(A - B) \sim (A - B)$ ו- $B \sim B^+$. מכל זה ומהלמה לפני המשפט נקבל:

$$A = (A - B) \cup B \ \sim\ (A - B) \cup B^+$$

כמו כן, $(A - B) \cup B^+ \subset A$, כי אם $x \in B - B^+$, אז $x \notin A - B$ ו- $x \notin B^+$, ולכן $x \in A$ ו- $x \notin (A - B) \cup B^+$. סה"כ $(A - B) \cup B^+$ קבוצה חלקית-ממש ל- A, שהינה שוות-עוצמה עם A.

(ב) $\Leftarrow$ (ג):

זה מיידי מהעובדה, שציינו למעלה, שקבוצה סופית אינה יכולה להיות אקויפוטנטית עם קבוצה חלקית שלה.

(ג) $\Leftarrow$ (א):

הוכחה מדויקת מסתמכת כאן על אקסיומה מיוחדת, שלא נלמדת בצורה מסודרת בקורס זה, ונקראת "אקסיומת הבחירה". לכן לא נביא הוכחה זו במלואה. *הרעיון* שמאחוריה הוא כזה: כיוון ש- A אינסופית, $A \neq \varnothing$ לכן יש בה איזה איבר. יהי a_0 איבר כזה. כיוון ש- A אינסופית, $A \neq \{a_0\}$ לכן יש איבר a_1 ב- $A - \{a_0\}$. עתה $A \neq \{a_0, a_1\}$ (כי A אינסופית), ולכן יש איבר $a_2 \in A - \{a_0, a_1\}$. בצורה זו נמשיך ונקבל סדרה

$a_0, a_1, a_2, a_3, \ldots$ של איברים מ- A, שכולם שונים זה מזה. הקבוצה B, המורכבת מאיברי סדרה זו, היא תת-קבוצה ב"מ של A.

%%

שאלה: מדוע מה שתיארנו למעלה, אינו הוכחה שלמה?

התשובה נעוצה במלים "בצורה זו נמשיך" המופיעות שם. עלינו להמשיך כאן בתהליך אינסופי, שבו בכל שלב אנו בוחרים באופן אקראי איבר חדש של A. לבסוף אנו מסתכלים במה שהתקבל ב*כל* התהליך, כאילו ***התהליך הושלם*** (מעשית, הוא לא יושלם לעולם, כמובן !). נשים לב, שאם נקח איבר x מסוים של A וננסה לברר, האם הוא נמצא ב- B, הרי לא תהיה לנו כל דרך לעשות זאת. אין ביכולתנו לדעת מראש, אם x ייבחר באופן אקראי באיזה שלב עתידי בבניית B! אקסיומת הבחירה מבטיחה, אינטואיטיבית, שקבוצות המתקבלות בתהליך אינסופי כזה של בחירות אקראיות, אכן קיימות – למרות שאין לנו כל דרך לתאר אותן או להכיר אותן. בכך היא שונה מאוד מכל העקרונות, שראינו בחלק הקודם. העקרונות ההם סיפקו תיאור מדויק של הקבוצות, שאת קיומן הם הבטיחו, וקריטריון מדויק לשייכות בהן!

%%

מסקנה:

קבוצה הינה סופית אם"ם היא אינה אקויפוטנטית עם שום קבוצה חלקית-ממש שלה.

הערה:

מסקנה זו יכולה לשמש כבסיס להגדרה אלטרנטיבית של מושג הקבוצה הסופית, שאינה מסתמכת על המספרים הטבעיים: מגדירים קבוצה כסופית אם אינה אקויפוטנטית עם שום קבוצה חלקית-ממש שלה.

*נספח:

הוכחה שאם $A \sim \mathbf{N}_n$ ו- $A \sim \mathbf{N}_k$, אז $n = k$

טענת עזר:

אם f היא פונקציה ח.ח.ע. מ- $\mathbf{N}_n$ ל- $\mathbf{N}_n$, אז f היא על $\mathbf{N}_n$.

הוכחה:

באינדוקציה על n. עבור $n = 0$ ו- $n = 1$ זה טריביאלי. נניח שהטענה נכונה עבור n ותהי f פונקציה ח.ח.ע. מ- $\mathbf{N}_{n+1}$ אל $\mathbf{N}_{n+1}$.

אפשרות א: $n+1 \notin f(\mathbf{N}_n)$. אז $f/\mathbf{N}_n$ היא פונקציה ח.ח.ע. מ- $\mathbf{N}_n$ אל $\mathbf{N}_n$. לפי הנחת האינדוקציה, $f/\mathbf{N}_n$ היא לכן על $\mathbf{N}_n$. כיוון ש- f ח.ח.ע., נובע מזה ש- $f(n+1) \notin \mathbf{N}_n$ מכאן ש- $f(n+1) = n+1$, לכן $n+1 \in f(\mathbf{N}_{n+1})$. מזה ומהעובדה ש- $f/\mathbf{N}_n$ היא על $\mathbf{N}_n$ נקבל, ש- $\mathbf{N}_n \cup \{n+1\} = \mathbf{N}_{n+1}$ מוכלת בתמונה של f במלים אחרות: f היא על $\mathbf{N}_{n+1}$.

אפשרות ב: $n+1 \in f(\mathbf{N}_n)$. נניח אפוא, ש- $n+1 = f(j_0)$ כש- $j_0 \in \mathbf{N}_n$.
נגדיר $g : \mathbf{N}_{n+1} \to \mathbf{N}_{n+1}$ על-ידי:

$$g(i) = \begin{cases} n+1 & i = n+1 \\ f(n+1) & i = j_0 \\ f(i) & \text{אחרת} \end{cases}$$

(g מתקבל מ- f על-ידי "החלפת" הערכים שמקבלים j_0 ו- $n+1$).
קל לראות, ש- g גם היא ח.ח.ע., ושהתמונה של g שווה לתמונה של f. על g חלה, אבל, אפשרות א, ולכן התמונה של g היא כל $\mathbf{N}_{n+1}$ (לפי מה שכבר הוכחנו). לכן גם התמונה של f היא כל $\mathbf{N}_{n+1}$. במלים אחרות: f היא על $\mathbf{N}_{n+1}$.

הערה:
טענת העזר שקולה, בעצם, לחצי מהטענה הכלולה בתכונה (4) (ii) של טבלה ג.2.

מסקנה 1: $\mathbf{N}_n$ אינה אקויפוטנטית עם שום קבוצה חלקית-ממש שלה.

מסקנה 2: אם $\mathbf{N}_n \sim \mathbf{N}_k$, אז $n = k$.

הוכחה:
אם $k < n$, אז $\mathbf{N}_k$ קבוצה חלקית-ממש של $\mathbf{N}_n$, ונקבל סתירה עם מסקנה 1. בדומה, לא ייתכן, ש- $n < k$. לכן $k = n$.

הוכחת המשפט:
אם $A \sim \mathbf{N}_n$ ו- $A \sim \mathbf{N}_k$, אז $\mathbf{N}_n \sim \mathbf{N}_k$. לכן $n = k$ לפי מסקנה 2.

הערה:
(4) (i) של טבלה ג.2 נובעת בקלות ממסקנה 1 ומהגדרת קבוצה סופית (הוכיחו!).

ג.3 סדר על עוצמות

לאחר שהגדרנו מתי שתי עוצמות הן שוות, השלב הטבעי הבא הוא לנסות לסדר אותן, באופן שנוכל לקבוע, מי גדולה יותר ומי קטנה יותר (ממש כשם שהדבר נעשה לגבי קבוצות סופיות). הקו המנחה יהיה שוב ניתוח המושג של "קבוצה גדולה יותר" בתחום המוכר של קבוצות סופיות. הבה נחזור אפוא לאולם הריקודים שלנו. הפעם נניח אבל, שבהיכנסנו לאולם *לא* כל הנוכחים מרקדים, אלא חלקם יושבים על הספסל בהמתנה. נניח עוד, שכל חובשי הספסל הם גברים. מה יש בחדר יותר: גברים או נשים? התשובה המיידית היא: גברים, ושוב אין כל צורך בספירה בשביל להגיע למסקנה זו. די לנו בכך, שיש פונקציית שקילות בין קבוצות הנשים בחדר ובין קבוצה חלקית-ממש לקבוצת הגברים (או פונקציה ח.ח.ע. מקבוצת הנשים אל קבוצת הגברים, שאיננה על).

ניסיון לא זהיר להכליל עקרון זה לקבוצות כלשהן יביא, מן הסתם, ל"הגדרה" הבאה: "קבוצה A היא קטנה ממש מקבוצה B אם קיימת פונקציה ח.ח.ע. מ- A על קבוצה חלקית-ממש של B". ברם, לפי זה נקבל, למשל, ש- N הינה קטנה-ממש מעצמה (כי N אקויפוטנטית, כזכור, ל- $\mathrm{N}_{\mathrm{even}}$, החלקית לה ממש), בעוד יחס סדר חזק אמור להיות אי-רפלקסיבי! הלקח הינו, שהכללה של מושגים מהתחום הסופי אל התחום האינסופי צריכה להיעשות בזהירות מופלגת. לא כל עקרון, שהוא "מובן מאליו" בתחום הסופי, נשאר נכון לגבי קבוצות אינסופיות.

עם זאת, מה שעדיין נראה אינטואיטיבית כנכון, ללא ספק, הוא העיקרון הבא, אותו נהפוך להגדרה:

הגדרה:

יהיו a ו- b עוצמות, כך ש- $a=|A|$ ו- $b=|B|$. נאמר ש- $a \le b$ ("a קטנה או שווה ל- b"), אם קיימת פונקציה ח.ח.ע. מ- A ל- B.

בהגדרה זו יש בעייתיות מסוימת, האופיינית כמעט לכל ההגדרות, הקשורות בעוצמות. הבה נסבירה אפוא בפרוטרוט, ונראה איך מתגברים עליה. מה שמתרחש כאן הוא, שכדי להגדיר מושג הקשור בעוצמות ($a \le b$, במקרה הזה), אנו משתמשים בקבוצות *מייצגות* עבור עוצמות אלה (כאן: קבוצות A ו- B כך ש- $|A|=a$ ו- $|B|=b$) ומגדירים את המושג באמצעותן. הבעיה היא, שלעוצמה אחת יש מייצגים רבים, וחייבים אנו להיות בטוחים, שההגדרה אינה תלויה במייצגים שבחרנו. שוו, למשל, בנפשכם מצב, בו יש קבוצות A_1, A_2, B_1 ו- B_2, כך ש- $|A_1|=a$, $|A_2|=a$, $|B_1|=b$, $|B_2|=b$, יש פונקציה ח.ח.ע. מ- A_1 ל- B_1, אך *אין* פונקציה ח.ח.ע. מ- A_2 ל- B_2. במצב כזה, שמעון, שהיה

מסתמך על A_1 ו- B_1, היה מגיע למסקנה ש- $a \le b$. לעומתו לוי, שהיה מסתמך על A_2 ו-B_2, היה מגיע למסקנה ההפוכה – ושניהם היו צודקים לפי ה"הגדרה" למעלה! במצב עניינים כזה היינו אומרים, שהיחס $\le$ ***אינו מוגדר היטב***, כיוון שה"הגדרה" שניתנה תלויה במייצגים. המשימה הראשונה לכן, בכל פעם שנותנים הגדרה כזו (עקרונית: עוד *לפני* שנותנים הגדרה כזו!), היא להראות, שמצב כזה אינו נוצר, ושהמושג שהוגדר – אכן הוגדר היטב.

לגבי $\le$, אי-תלות כזו מובטחת בטענה הבאה:

טענה:

היחס $\le$ על עוצמות מוגדר היטב: אם $|A_1| = |A_2|$, $|B_1| = |B_2|$ וקיימת פונקציה ח.ח.ע. f מ- A_1 אל B_1, אז קיימת גם פונקציה ח.ח.ע. מ- A_2 אל B_2.

הוכחה:

כיוון ש- $|A_1| = |A_2|$, אז קיימת פונקציה ח.ח.ע. F מ- A_1 על A_2. בדומה, קיימת פונקציה ח.ח.ע. G מ- B_1 על B_2. F ו- G הן כמובן הפיכות, והפונקציות ההפוכות, F^{-1} ו- G^{-1}, אף הן חד-חד-ערכיות. עתה, $G \circ f \circ F^{-1}$ היא פונקציה מ- A_2 ל- B_2, והיא ח.ח.ע., כיוון שהיא הרכבה של פונקציות חד-חד-ערכיות.

הערות:

1. רעיון ההוכחה מודגם על-ידי הדיאגרמה הבאה, שבה חצים עבים רציפים מייצגים פונקציות, שקיומן מובטח ישירות על-ידי הנתונים:

$$\begin{tikzcd}
A_1 \arrow[r, shift right, "F"'] \arrow[d, "f"'] & A_2 \arrow[l, shift right, "F^{-1}"'] \arrow[d, dashed, "?"] \\
B_1 \arrow[r, shift right, "G"'] & B_2 \arrow[l, shift right, "G^{-1}"']
\end{tikzcd}$$

ברור מהדיאגרמה, שאפשר "ללכת" מ- A_2 ל- B_2 במסלול:

$$\begin{tikzcd}
A_1 \arrow[d, "f"'] & A_2 \arrow[l, "F^{-1}"'] \\
B_1 \arrow[r, "G"'] & B_2
\end{tikzcd}$$

לכן טבעי לשער, ש- $G \circ f \circ F^{-1}$ היא הפונקציה המבוקשת.
דיאגרמות מסוג זה יכולות להיות לעזר רב במציאת הוכחות ובהבנתן.

2. ניסוח אחר של הטענה האחרונה הוא: אם $|A_1| = |A_2|$, $|B_1| = |B_2|$, ו- $|A_1| \leq |B_1|$, אז $|A_2| \leq |B_2|$.
3. לגבי מספרים טבעיים, היחס $\leq$, כמו שהוגדר כאן, והיחס $\leq$, המוכר לנו, הם זהים.

נביא עתה אפיונים נוספים ליחס $\leq$ על עוצמות:

משפט:

תהיינה a ו- b עוצמות. נניח $a = |A|$, $b = |B|$. אז:

(א) $a \leq b$ אם"ם A אקויפוטנטית עם קבוצה חלקית כלשהי של B.

(ב) $a \leq b$ אם"ם $A = \varnothing$ או יש פונקציה מ- B על A.

הוכחה:

(א) נובע מיידית מההגדרות והעובדה, שאם f פונקציה ח.ח.ע. מ- A ל- B, אז $A \sim f(A) \subseteq B$.

(ב) ($\Leftarrow$): נניח $a \leq b$ ו- $A \neq \varnothing$ אז יש פונקציה ח.ח.ע. מ- A ל- B, ויש איבר $a_0 \in A$. נגדיר:

$$g = \lambda x \in B.\ \text{if } x \in f(A) \text{ then } (\iota z \in A.\ f(z) = x) \text{ else } a_0$$

(השימוש באופרטור ι (מפרק א.5) בהגדרת g מוצדק כאן, כיוון ש- f ח.ח.ע.).

מיידי, כשלכל $y \in A$ מתקיים ש- $y = g(f(y))$, ולכן $y \in g(B)$. לכן g על A.

($\Rightarrow$): אם $A = \varnothing$, אז $\varnothing$ היא פונקציה ח.ח.ע. מ- A ל- B ($\varnothing$ היא פונקציה מ- $\varnothing$ אל כל קבוצה, והיא ח.ח.ע. באופן טריביאלי!).

אם קיימת פונקציה g מ- B על A, אז לכל $x \in A$ הקבוצה $g^{-1}(\{x\})$ אינה ריקה. נבחר אפוא לכל x איבר b_x ב- $g^{-1}(\{x\})$. אז $g(b_x) = x$. נגדיר עתה $f: A \to B$ על-ידי שנתאים לכל $x \in A$ את b_x (רשמית: $f = \{<x, b_x> \mid x \in A\}$). f זו הינה ח.ח.ע., כיוון ש:

$$\begin{aligned} f(x) = f(y) &\Rightarrow b_x = b_y \\ &\Rightarrow g(b_x) = g(b_y) \\ &\Rightarrow x = y \end{aligned}$$

%%

הערה:

בהוכחת כיוון ה"אם" ($\Rightarrow$) בחלק ב' של המשפט האחרון, השתמשנו באופן מפורש ב*אקסיומת הבחירה*: את b_x הרי לא הגדרנו במפורש (בעזרת סימון-למדא, למשל),

ולא נתנו שום כלל איך "לבחור" אותו. עתה, אקסיומת הבחירה מבטיחה, שאם $\{B_x | x \in A\}$ היא קבוצה של קבוצות לא ריקות, אז קיימת פונקציה f מ- A אל $\bigcup_{x \in A} B_x$ כך ש- $\forall x \in A. f(x) \in B_x$. במקרה הנוכחי $B_x = g^{-1}(\{x\})$, $\bigcup_{x \in A} B_x = B$ והאקסיומה היא שסיפקה, למעשה, את ה- f בה השתמשנו.

%%

טענה:

(1) תהיינה a ו- b עוצמות. אז $a \le b$ אם"ם קיימות קבוצות A ו- B, כך ש- $|A| = a$, $|B| = b$, ו- $A \subseteq B$.

(2) נניח a ו- b עוצמות ו- $|B| = b$. אז $a \le b$ אם"ם יש $A \subseteq B$ כך ש- $|A| = a$.

הוכחה: תרגיל.

נעבור עתה לבדוק את השאלה אם היחס $\le$ על עוצמות הינו אכן (כמו שהסימון מרמז) יחס סדר חלקי.

טענה:

היחס $\le$ על עוצמות הינו רפלקסיבי וטרנסיטיבי.

הוכחה:

רפלקסיביות: תהי a עוצמה, ונניח $|A| = a$. כיוון ש- $A \subseteq A$ ו- $A \sim A$, הרי $a \le a$ לפי המשפט הקודם.

טרנסיטיביות: נניח a, b, c עוצמות כך ש- $a \le b$ ו- $b \le c$. נניח $|A| = a$, $|B| = b$ ו- $|C| = c$. אז יש פונקציה ח.ח.ע. f מ- A ל- B ופונקציה ח.ח.ע. g מ- B ל- C. עתה, $g \circ f$ הינה פונקציה ח.ח.ע. מ- A ל- C. לכן $a \le c$.

מה בקשר לתכונה השלישית, אנטי-סימטריות? ובכן, בניגוד לרפלקסיביות ולטרנסיטיביות, ההוכחה שלה אינה טריביאלית כלל ועיקר! זהו התוכן, למעשה, של המשפט הבא, שהינו אחד המשפטים המרכזיים של תורת הקבוצות:

משפט קנטור-ברנשטיין-(שרודר):

היחס $\le$ על עוצמות הוא אנטי-סימטרי: אם a ו- b עוצמות כך ש- $a \le b$ ו- $b \le a$, אז $a = b$.

ניסוחים שקולים:

(א) אם A ו- B קבוצות, כך ש- $|A| \leq |B|$ ו- $|B| \leq |A|$, אז $|A| = |B|$.

(ב) אם A ו- B קבוצות, כך ש- A אקויפוטנטית עם קבוצה חלקית של B, ו- B אקויפוטנטית עם קבוצה חלקית של A, אז A ו- B אקויפוטנטיות.

(ג) אם A ו- B קבוצות, וקיימות פונקציות ח.ח.ע. $f: A \to B$ ו- $g: B \to A$, אז קיימת פונקציה ח.ח.ע. h מ- A על B.

העובדה, שארבעת הניסוחים אכן שקולים, מיידית מההגדרות של שוויון עוצמות, של היחס $\leq$ בין עוצמות ושל אקויפוטנטיות בין קבוצות. את הוכחת המשפט עצמו אפשר למצוא בנספח לפרק זה.

מסקנה:

היחס $\leq$ על עוצמות הינו יחס סדר חלקי.

הוכחה:

מיידי מהמשפט האחרון ומהטענה שקדמה לו.

%%

הערה:

בעיה, שמתעוררת באופן טבעי בנקודה זו, היא: האם היחס $\leq$ בין עוצמות הוא יחס סדר ***מלא*** (דהיינו: האם לכל שתי עוצמות a ו- b מתקיים, ש- $a \leq b$ או $b \leq a$)? התשובה הינה חיובית, אך ההוכחה (הנעזרת באקסיומת הבחירה) חורגת ממה שאפשר להביא בקורס זה. בהמשך לא נסתמך לכן על עובדה זו.

%%

כדי להדגים את הכוח של משפט קנטור-ברנשטיין, נוכיח את המשפט הבא (נזכיר לקוראים ש- $|(0,1)| = \aleph$):

משפט:

אם A היא קבוצה חלקית של $\mathbf{R}$, המכילה קטע פתוח (דהיינו: $(a,b) \subseteq A \subseteq \mathbf{R}$ עבור מספרים ממשיים a,b כלשהם כך ש- $a < b$), אז $|A| = \aleph$.

הוכחה:

נשתמש בשתי למות, שאת הוכחתן ראינו בפרק ג.1 (ראה טבלה ג.1):

למה 1:

$(a,b) \sim (0,1)$ לכל $a,b \in \mathbf{R}$ כך ש- $a < b$.

למה 2:

$\mathbf{R} \sim (-1,1)$.

עתה, מלמה 1 נובע, ש- $(0,1) \sim (-1,1)$, ולכן, מלמה 2, $\mathbf{R} \sim (0,1)$. לכן, שוב מלמה 1, $(a,b) \sim \mathbf{R}$ עבור כל קטע (a,b) כך ש- $a < b$. לכן $|\mathbf{R}| = |(a,b)|$ עבור כל קטע (a,b) כזה. עתה, אם $(a,b) \subseteq A \subseteq \mathbf{R}$, אז $|(a,b)| \le |A| \le |\mathbf{R}|$. אבל כיוון ש- $|(a,b)| = |\mathbf{R}|$, אנו מקבלים ש- $|A| \le |\mathbf{R}|$ ו- $|\mathbf{R}| \le |A|$. לכן, לפי משפט קנטור-ברנשטיין, $|A| = |\mathbf{R}|$. נותר עוד לכן להראות ש- $|\mathbf{R}| = א$. אבל כיוון ש- $(0,1) \subseteq [0,1) \subseteq \mathbf{R}$, נובע ממה שהראינו, שגם $|\mathbf{R}| = |[0,1)|$, כלומר: $|\mathbf{R}| = א$.

מסקנה:

ל- $\mathbf{R}$ ולכל קטע עליו (סופי או אינסופי, פתוח, סגור, או חצי פתוח חצי סגור) יש אותה עוצמה: א.

הערות:

(1) ממה שהראינו נובע בפרט, ש- $|[0,1)| = |(0,1)|$. לכן יש פונקציה ח.ח.ע. מ- $(0,1)$ על $[0,1)$. אין זה כה פשוט אבל להציג פונקציה כזו ישירות, ללא שימוש במשפט קנטור-ברנשטיין!

(2) אם נבדוק את הוכחת המשפט האחרון יתברר לנו, שהשתמשנו בעיקרון השימושי הבא:

אם $A \subseteq B \subseteq C$ ו- $|A| = |C|$, אז $|A| = |B| = |C|$

לעיקרון זה אפשר לקרוא ***"עיקרון הסנדוויץ'"*** עבור עוצמות, והוא מסקנה מיידית ממשפט קנטור-ברנשטיין.

כמו בכל מקרה בו מוגדר יחס סדר חלקי $\le$, ניתן לגזור ממנו יחס סדר חזק:

הגדרה:

יהיו a ו- b עוצמות. $a < b$ אם $a \le b$, אך $a \ne b$.

ברור ש- $|A| < |B|$, אם קיימת פונקציה ח.ח.ע. מ- A אל B, אך לא מ- A על B (ולפי קנטור-ברנשטיין, גם לא פונקציה ח.ח.ע. מ- B אל A). כמו כן ברור, ש- $<$ הוא יחס סדר *חזק* על עוצמות.

דוגמאות:

(1) **לגבי מספרים טבעיים, היחס $<$, כמו שהוגדר כאן, והיחס $<$ המוכר לנו מקודם, הם זהים.**

(2) **אם n טבעי, אז $n < \aleph_0$.**

הוכחה:

כיוון ש- $\{0,1, \ldots, n-1\} \subseteq \mathbf{N}$, $n = |\{0, \ldots, n-1\}| \le |\mathbf{N}| = \aleph_0$. לא יתכן אבל ש- $n = \aleph_0$ (כלומר ש- $\mathbf{N} \sim \{0,1, \ldots, n-1\}$), כי $\mathbf{N}$ אינסופית (הוכחנו!), בעוד $\{0, \ldots, n-1\}$ הינה סופית.

(3) **$\aleph_0 < \aleph$.**

הוכחה:

$\mathbf{N} \subseteq \mathbf{R}$. לכן: $\aleph_0 = |\mathbf{N}| \le |\mathbf{R}| = \aleph$. כיוון שהראינו בפרק הקודם ש- $\aleph \neq \aleph_0$, נובע מזה, ש- $\aleph_0 < \aleph$.

דוגמה (3) אינה מקרית. היא מקרה פרטי של המשפט הבא:

משפט:

(1) **אם a עוצמה אינסופית, אז $\aleph_0 \le a$.**

(2) **אם a עוצמה אינסופית ו- $a \neq \aleph_0$, אז $\aleph_0 < a$.**

הוכחה:

(1) בפרק הקודם ראינו, שכל קבוצה אינסופית מכילה קבוצה בת-מניה. מכאן, שאם a אינסופית ו- $a = |A|$, אז יש קבוצה $B \subseteq A$ כך ש- $|B| = \aleph_0$. לכן $a = |A| \ge |B| = \aleph_0$. את הכיוון ההפוך (ש- $\aleph_0 \le a \Leftarrow a$ אינסופית) נשאיר לקורא.

(2) מיידי מ- (1).

מסקנה:

אם a עוצמה כך ש- $a < \aleph_0$, אז a סופית (כלומר: $a \in \mathbf{N}$).

עד כה הכרנו שתי עוצמות אינסופיות בלבד: $\aleph_0$ ו- $\aleph$. המשפטים, שהוכחנו עד כה, עלולים ליצור את הרושם, שאלו הן כל העוצמות האינסופיות. המשפט הבא הוא משפט מפתח המראה, *שאין הדבר כך* !

משפט קנטור:

$|A| < |P(A)|$ לכל קבוצה A.

הוכחה:

$\lambda x \in A.\{x\}$ היא פונקציה ח.ח.ע. מ- A אל $P(A)$. לכן $|A| \le |P(A)|$. נותר להראות, ש- $|A| \ne |P(A)|$. בשביל זה מספיק להראות, שלא תיתכן פונקציה מ- A על $P(A)$. תהי אפוא F פונקציה מ- A אל $P(A)$, ונראה ש- F לא על $P(A)$. לצורך זאת נתבונן בקבוצה הבאה:

$$\mathbf{C}_F = \{x \in A \mid x \notin F(x)\}$$

ברור ש- $C_F \in P(A)$. עתה, לו היתה F על $P(A)$, כי אז היה $a \in A$, כך ש- $F(a) = C_F$. אבל אז היינו מקבלים ש:

$$\begin{aligned} a \in F(a) &\Leftrightarrow a \in C_F \\ &\Leftrightarrow a \in \{x \in A \mid x \notin F(x)\} \\ &\Leftrightarrow a \notin F(a) \end{aligned}$$

קיבלנו ש- $a \in F(a) \Leftrightarrow a \notin F(a)$, וזו סתירה לוגית. מכאן ש- F אינה יכולה להיות על $P(A)$.

הסבר נוסף להוכחה:

הוכחת משפט קנטור נותנת דרך קונסטרוקטיבית איך, בהינתן $F: A \to P(A)$, אפשר לבנות איבר ב- $P(A)$, שאינו בתמונה של F. נדגים זאת עם $A = \{1,2\}$. במקרה זה $P(A) = \{\varnothing,\{1\},\{2\},\{1,2\}\}$, ויש 16 פונקציות ב- $A \to P(A)$. ניקח שתיים כדוגמה:

$$F_1 = \lambda x \in A.\ \text{If } x = 1 \text{ then } \{1\} \text{ else } \{1,2\}$$
$$F_2 = \lambda x \in A.\ \text{If } x = 1 \text{ then } \{2\} \text{ else } \{1,2\}$$

עתה, $C_{F_1} = \varnothing$ (כי $1 \in F_1(1) = \{1\}$ ו- $2 \in F_1(2) = \{1,2\}$), בעוד $C_{F_2} = \{1\}$ (כי $1 \notin F_2(1) = \{2\}$, בעוד $2 \in F_2(2) = \{1,2\}$). ואכן: $\varnothing$ אינו בתמונה של F_1 (שהיא $\{\{1\},\{1,2\}\}$), ו- $\{1\}$ אינו בתמונה של F_2 (שהיא $\{\{2\},\{1,2\}\}$).

מסקנות ממשפט קנטור:

(1) אין עוצמה מקסימלית.

(2) $\aleph_0 = |\mathbf{N}| < |P(\mathbf{N})| < |P(P(\mathbf{N}))| < |P(P(P(\mathbf{N})))| < \ldots$

מהמסקנה השנייה ברור, שיש אינסוף עוצמות אינסופיות. אלה, אגב, אינן כולן. אם נגדיר, למשל, $P^n(\mathbf{N}) = \overbrace{P(P(\ldots P}^{n \text{ פעמים}}(\mathbf{N}))\ldots)$ (P מופעל n פעמים על $\mathbf{N}$) ו- $\mathbf{N}_\infty = \bigcup_{n=0}^{\infty} P^n(\mathbf{N})$, אז לכל n $\mathbf{N}_\infty \supseteq P^{n+1}(\mathbf{N})$, ולכן $|\mathbf{N}_\infty| \geq |P^{n+1}(\mathbf{N})| > |P^n(\mathbf{N})|$, לפי משפט קנטור. $|\mathbf{N}_\infty|$ היא לכן עוצמה הגדולה מכל אלה בסדרה למעלה, ולפי מסקנה (1) גם היא אינה מקסימלית!

*נספח:
הוכחת משפט קנטור-ברנשטיין

משפט עזר:

נניח כי $f : A \to D$ היא פונקציה ח.ח.ע., וש- $D \subseteq A$. אז $A \sim D$.

הוכחת משפט העזר:

נגדיר:

$$A^* = \{x \in D \mid \exists\, n \in \mathbf{N}\ \exists a \in A - D.\ x = f^n(a)\}$$
$$F = \lambda x \in A.\ \text{If}\ \ x \in A^*\ \ \text{then}\ \ f(x)\ \ \text{else}\ x$$

במלים: A^* מכילה את כל הנקודות, הנמצאות על "מסלול" מהצורה:

$$x = f^0(x), f(x), f^2(x), f^3(x), \ldots$$

המתחיל בנקודה הנמצאת ב- $A - D$ ($f^n(x)$ מוגדר לכל $n \geq 0$, כי $D \subseteq A$ ו- $f : A \to D$, ולכן $f : A \to A$). בפרט $A - D \subseteq A^*$ (המקרה $n = 0$ בהגדרת A^*). אינטואיטיבית, מה ש- F עושה הוא להזיז "ימינה" במסלול כל נקודה הנמצאת על מסלול כזה, ולהשאיר במקומן את הנקודות האחרות.

נראה עתה ש- F היא פונקציית שקילות מ- A על D.

(א) $F : A \to D$

ברור ש- A היא התחום של F. נראה ש- $F(x) \in D$ לכל $x \in A$. ואכן, אם $x \in A^*$, אז $F(x) = f(x) \in D$ (כי $f : A \to D$). אם $x \notin A^*$, אז $x \in D$ (כי $A - D \subseteq A^*$), ולכן $F(x) = x \in D$ גם במקרה זה.

(ב) F היא על D

יהי $y \in D$. נראה, שקיים $x \in A$ כך ש- $y = f(x)$.

(i) אם $y \in A^*$, אז מהגדרת A^* והעובדה ש- $y \notin A - D$ (כי $y \in D$), נובע, שיש $a \in A - D$ ו- $n \geq 1$ כך ש- $y = f^n(a)$. עתה, $f^{n-1}(a) \in A^*$, שוב מהגדרת A^*. לכן, אם נקח $x = f^{n-1}(a)$ נקבל:

$$F(x) = f(x) = f(f^{n-1}(a)) = f^n(a) = y$$

(ii) אם $y \notin A^*$ אז $F(y) = y$, ולכן נוכל במקרה זה לקחת $x = y$.

(ג) F ח.ח.ע.

נניח $F(x_1) = F(x_2)$, כאשר $x_1, x_2 \in A$. נראה ש- $x_1 = x_2$.

(i) נניח $x_1 \in A^*$, $x_2 \notin A^*$. אז מהנתון $F(x_1) = F(x_2)$ והגדרתה של F נובע אז, ש- $f(x_1) = x_2$. במקרה זה קיימים אבל $a \in A - D$ ו- $n \in \mathbf{N}$, כך ש- $x_1 = f^n(a)$. מכאן ש- $x_2 = f(x_1) = f^{\,n+1}(a)$, ולכן גם $x_2 \in A^*$ זוהי סתירה לנתון. מקרה זה הינו לכן בלתי אפשרי.

(ii) נניח $x_1 \notin A^*$, $x_2 \in A^*$. נקבל כאן שוב סתירה, בדיוק כמו במקרה הקודם.

(iii) נניח $x_1 \in A^*$ וגם $x_2 \in A^*$. אז מ- $F(x_1) = F(x_2)$ נובע כאן ש- $f(x_1) = f(x_2)$, ולכן $x_1 = x_2$ (כי f ח.ח.ע.).

(iv) נניח $x_1 \notin A^*$ וגם $x_2 \notin A^*$. אז הנתון $F(x_1) = F(x_2)$ פירושו $x_1 = x_2$, כי $F(x_1) = x_1$ ו- $F(x_2) = x_2$ במקרה זה.

הוכחת משפט קנטור-ברנשטיין:

נניח ש- $f : A \to B$ ו- $g : B \to A$ הן פונקציות ח.ח.ע. תהי $D = g[B]$. אז $D \subseteq A$ ו- $g \circ f$ היא פונקציה ח.ח.ע. מ- A ל- D. לפי משפט העזר, $A \sim D$. כיוון ש- g פונקציית שקילות מ- B על D, גם $B \sim D$. משתי השקילויות נובע, כי $A \sim B$ (ולכן יש פונקציית שקילות מ- A על B).

ג.4 פעולות על עוצמות

אחרי שהכללנו בפרק הקודם את יחס הסדר של N לעוצמות כלשהן, נכליל בפרק זה כמה מהפעולות הבסיסיות על מספרים טבעיים: חיבור, כפל וחזקה. המפתח להכללות יהיה תכונה מס' (8) בטבלת התכונות הבסיסיות של קבוצות סופיות (טבלה ג.2).

נפתח בחיבור:

הגדרה:

יהיו a ו- b עוצמות. אז $a + b = |A \cup B|$, כאשר A ו- B הן קבוצות, כך ש- $|A| = a$, $|B| = b$ ו- $A \cap B = \varnothing$.

כמו שקורה בכל ההגדרות הקשורות בעוצמות, יש קודם כל להצדיק את ההגדרה ולהראות, שחיבור עוצמות אכן מוגדר היטב. בשביל זה יש, ראשית חוכמה, להראות, שהתוצאה הסופית, $a + b$, אינה תלויה במייצגים A ו- B (השווה עם הדיון אחרי הגדרת הסדר על עוצמות בפרק הקודם, ועם הטענה, שבאה אחרי הדיון הנ"ל). זאת עשינו כבר, למעשה, בפרק קודם, במסגרת הלמה, אותה הוכחנו מיד אחרי ההגדרה של קבוצות בנות-מניה (בפרק ג.2). ברם, בניגוד למה שקורה עם הטענה המקבילה במקרה של $\leq$ (ולמה שיקרה בהגדרות של כפל וחזקה), הלמה הנ"ל ***אינה*** מספיקה בשביל להראות, שחיבור עוצמות מוגדר היטב! מה שהיא מראה הוא, ***שאם*** $a + b$ מוגדר, אז הוא מוגדר היטב (כלומר, באופן יחיד). עדיין לא ברור אבל, שכל שתי עוצמות ניתן אכן לחבר! בשביל זה יש להראות את הדבר הבא:

טענה 1:

אם a ו- b עוצמות, אז ***יש*** קבוצות A ו- B כך ש- $|A| = a$, $|B| = b$ ו- $A \cap B = \varnothing$.

הוכחה:

כיוון ש- a ו- b עוצמות, אז קיימות קבוצות A' ו- B', כך ש- $|A'| = a$, ו- $|B'| = b$. נגדיר $A = A' \times \{0\}$, $B = B' \times \{1\}$. ברור ש- $A \cap B = \varnothing$. כמו כן, $\lambda x \in A'. <x,0>$ הינה פונקציית שקילות מ- A' על A. לכן $a = |A'| = |A|$. באופן דומה נראה גם, ש- $b = |B'| = |B|$.

מסקנה מהלמה (בפרק ג.2) ומהטענה: חיבור כל שתי עוצמות מוגדר היטב.

דוגמאות:

(1) אם $n, m \in \mathbf{N}$, אז $n+m$ הוא בדיוק תוצאת החיבור הרגיל.

(2) $\aleph_0+\aleph_0=\aleph_0$.

הוכחה:

$\mathbf{N}=\mathbf{N}_{\mathrm{odd}}\cup\mathbf{N}_{\mathrm{even}}$ ו- $\mathbf{N}_{\mathrm{odd}}\cap\mathbf{N}_{\mathrm{even}}=\varnothing$. לכן

$$\aleph_0=|\mathbf{N}|=|\mathbf{N}_{\mathrm{odd}}|+|\mathbf{N}_{\mathrm{even}}|=\aleph_0+\aleph_0$$

(כזכור, $\aleph_0=|\mathbf{N}_{\mathrm{odd}}|=|\mathbf{N}_{\mathrm{even}}|$, כיוון ש- $\mathbf{N}\sim\mathbf{N}_{\mathrm{odd}}\sim\mathbf{N}_{\mathrm{even}}$).

מסקנה: $|\mathbf{Z}|=\aleph_0$.

הוכחה:

$\mathbf{Z}=\mathbf{N}\cup\{-n\mid n\in\mathbf{N}^+\}$ ו- $\mathbf{N}\cap\{-n\mid n\in\mathbf{N}^+\}=\varnothing$. לכן:

$$|\mathbf{Z}|=|\mathbf{N}|+|\{-n\mid n\in\mathbf{N}^+\}|$$

ברור אבל, ש- $|\{-n\mid n\in\mathbf{N}^+\}|=\aleph_0$ (למה?). לכן $|\mathbf{Z}|=\aleph_0+\aleph_0=\aleph_0$.

(3) $\aleph+\aleph=\aleph$.

הוכחה:

$(0,2)=(0,1)\cup[1,2)$ ו- $(0,1)\cap[1,2)=\varnothing$. לכן:

$$\aleph=|(0,2)|=|(0,1)|+|[1,2)|=\aleph+\aleph.$$

תרגיל:

$\aleph=\aleph_0+\aleph$. (רמז: כדאי להשתמש במשפט על עוצמת קבוצות חלקיות של $\mathbf{R}$ המכילות קטע פתוח).

נעבור עתה לכפל עוצמות.

הגדרה:

יהיו a ו- b עוצמות. אז $a\cdot b=|A\times B|$, כאשר A ו- B קבוצות, כך ש- $a=|A|$, $b=|B|$.

טענה 2:

כפל עוצמות מוגדר היטב.

הוכחה:

במקרה זה יש להוכיח רק אי תלות במייצגים (כי לכל עוצמה a יש קבוצה A כך ש- $a = |A|$). כלומר: עלינו להראות, שאם $A \sim A'$ ו- $B \sim B'$, אז $A \times B \sim A' \times B'$.
תהי אפוא f פונקציית שקילות מ- A על A', ו- g פונקציית שקילות מ- B על B'.
אז $\lambda x \in A, y \in B. <f(x), g(y)>$ היא פונקציית שקילות מ- $A \times B$ על $A' \times B'$ ($\lambda x \in A', y \in B'. <f^{-1}(x), g^{-1}(y)>$ היא הפונקציה ההפוכה – בדוק!).

דוגמאות:

(1) בגלל (8) מטבלה ג.2, $m \cdot n$ הוא בדיוק הכפל הרגיל כאשר $m,n \in \mathbf{N}$.

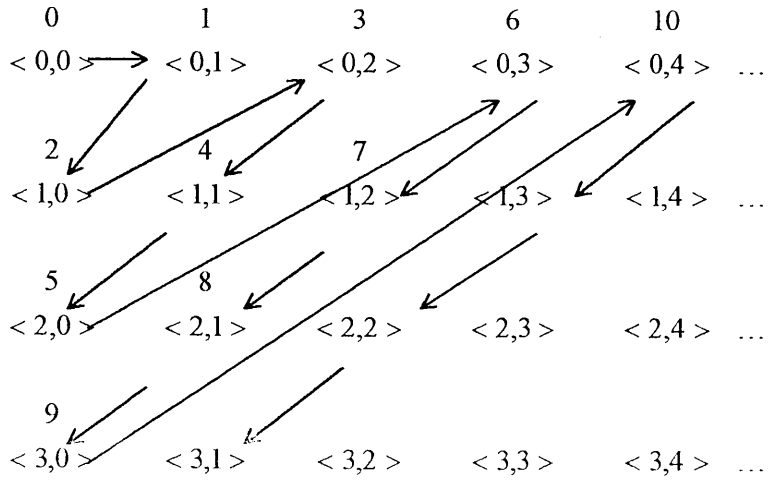
(2) $\aleph_0 \cdot \aleph_0 = \aleph_0$.

הוכחה:

לפי הגדרה, $\aleph_0 \cdot \aleph_0 = |\mathbf{N} \times \mathbf{N}|$. עתה, $\lambda n \in \mathbf{N}, k \in \mathbf{N}.\ 2^n \cdot 3^k$ היא פונקציה ח.ח.ע. מ- $\mathbf{N} \times \mathbf{N}$ אל $\mathbf{N}$, בעוד $\lambda n \in \mathbf{N}. <n,0>$ היא פונקציה ח.ח.ע. בכיוון ההפוך. לפי משפט קנטור-ברנשטיין נקבל לכן ש- $\aleph_0 = |\mathbf{N}| = |\mathbf{N} \times \mathbf{N}|$.

הערה:

הוכחה זו היא קצרה, אך לא מספקת פונקציית שקילות קונקרטית בין $\mathbf{N} \times \mathbf{N}$ ו- $\mathbf{N}$. פונקציה כזו ניתנה בטבלה ג.1. היא מתקבלת על-ידי התבוננות בדיאגרמה הבאה:



הדיאגרמה מגדירה פונקציה $F: \mathbf{N} \to \mathbf{N} \times \mathbf{N}$, כך ש- $F(0) = <0,0>$, $F(1) = <0,1>$, $F(2) = <1,0>$, $F(3) = <0,2>$, ..., $F(7) = <1,2>$, ... ברור ש-

F זו אכן ח.ח.ע. ועל. לגבי הפונקציה ההפוכה, $F^{-1}: \mathbf{N} \times \mathbf{N} \to \mathbf{N}$, מתקיים: $F^{-1}(<0,0>) = 0$, $F^{-1}(<0,1>) = 1$, $F^{-1}(<1,0>) = 2$, ..., $F^{-1}(<1,2>) = 7$, ... לא קשה להיווכח, שאכן:

$$F^{-1} = \lambda m \in \mathbf{N}, k \in \mathbf{N}. \frac{(m+k)(m+k+1)}{2} + m$$

(3) $\aleph = \aleph_0 \cdot \aleph$. ואכן: $\lambda x \in [0,1), z \in \mathbf{Z} \cdot x + z$ היא פונקציית שקילות מ- $[0,1) \times \mathbf{Z}$ על $\mathbf{R}$. לכן $\aleph = |\mathbf{R}| = |[0,1) \times \mathbf{Z}| = \aleph_0 \cdot \aleph$.

נעבור לבסוף לחזקה של עוצמות.

הגדרה:

יהיו a ו- b עוצמות. אז $a^b = |B \to A|$, כאשר A ו- B קבוצות, כך ש- $|A| = a$ ו- $|B| = b$.

הערות:

(1) כשמדובר בחזקות, הסימון A^B (במקום $B \to A$) נוח אולי יותר. בסימון זה – $|A^B| = |A|^{|B|}$.

(2) שוב, ל- $n,m \in \mathbf{N}$ m^n היא החזקה הרגילה, לפי (8) של טבלה ג.2.

טענה 3:

חזקה של עוצמות מוגדרת היטב.

הוכחה:

עלינו להוכיח, שאם $A \sim A'$ ו- $B \sim B'$, אז $A \to B \sim A' \to B'$.
מהנתונים קיימת פונקציה F ח.ח.ע. מ- A על A', ופונקציה G ח.ח.ע. מ- B על B'. תהי $H = \lambda f \in A \to B.\ G \circ f \circ F^{-1}$. ברור ש- $H : (A \to B) \to (A' \to B')$. נראה ש- H פונקציית שקילות. בשביל זה די להראות ש- $H' = \lambda g \in A' \to B'.\ G^{-1} \circ g \circ F$ הינה הפוכה ל- H. ואכן, $H' : (A' \to B') \to (A \to B)$, ואם $g \in A' \to B'$, אז:

$$\begin{aligned}(H \circ H')(g) &= H(H'(g)) \\ &= H(G^{-1} \circ g \circ F) \\ &= G \circ (G^{-1} \circ g \circ F) \circ F^{-1} \\ &= (G \circ G^{-1}) \circ g \circ (F \circ F^{-1}) \\ &= i_{B'} \circ g \circ i_{A'} \\ &= g\end{aligned}$$

לכן $H \circ H' = i_{A' \to B'}$. באופן דומה מראים ש- $H' \circ H = i_{A \to B}$.

הערה:
כדי להבין כיצד מגיעים להגדרה זו של H, כדאי להתבונן שוב בדיאגרמה בפרק הקודם, המופיעה אחרי הוכחת העובדה, שהיחס $\le$ בין עוצמות מוגדר היטב (וכמו כן לעיין בהוכחה של העובדה הנ"ל).

דוגמה:
אם $|E| = a$, אז $|P(E)| = 2^a$, או ביתר קיצור: $|P(E)| = 2^{|E|}$.

הוכחה:
ראינו בעבר, ש- $P(E) \sim E \to \{0,1\}$ (ראה טבלה ג.1 בפרק ג.1). לכן:

$$|P(E)| = |E \to \{0,1\}| = |\{0,1\}|^{|E|} = 2^a$$

עיקר העניין והתועלת בפעולות על המספרים הטבעיים היא העובדה, שיש חוקים פשוטים המקשרים ביניהם. טבלה ג.3 בעמוד הבא מרכזת את העובדות החשובות ביותר הקשורות לפעולות החיבור, הכפל וההזקה של מספרים טבעיים, ומסתבר שהן נשארות נכונות גם לגבי עוצמות כלשהן!

משפט:
כל התכונות המופיעות בטבלה ג.3 נכונות לעוצמות a,b,c,d כלשהן.

הוכחת המשפט:
הבה נתחיל ב- (1) כדוגמה. ההוכחה מתחילה בתרגום הטענות על עוצמות לטענות בדבר קבוצות, שאינן מזכירות כלל את מושג העוצמה. כך, למשל, משמעות $(1)_{(i)}$ היא, שאם ניקח קבוצות A ו- B כך ש- $|A| = a$, $|B| = b$ ו- $A \cap B = \varnothing$, אז ל- $A \cup B$ ול- $B \cup A$ תהיה אותה עוצמה, דהיינו $A \cup B \sim B \cup A$. באופן דומה, $(1)_{(ii)}$ פירושו, שאם $|A| = a$ ו- $|B| = b$, אז $A \times B \sim B \times A$. כיוון שהטענות כאן הן עבור כל עוצמה a וכל עוצמה b, ולכל קבוצה יש עוצמה כלשהי, הרי $(1)_{(i)}$ פירושו, שאם $A \cap B = \varnothing$, אז $A \cup B \sim B \cup A$, ו- $(1)_{(ii)}$ פירושו, שלכל A, B $A \times B \sim B \times A$. עתה $(1)_{(i)}$ נכון פשוט משום *שלכל* A ו- B (לא רק כאלו שחיתוכן ריק) מתקיים אפילו ש- $A \cup B = B \cup A$ (וממילא $A \cup B \sim B \cup A$). $(1)_{(ii)}$ נכון כיוון שהראינו בפרק ג.1, ש- $\lambda x \in A, y \in B.\ \langle y,x \rangle$ היא פונקציית שקילות מתאימה (טבלה ג.1).

טבלה ג.3: התכונות היסודיות של הפעולות על עוצמות

(1)	(i) $a+b=b+a$ (ii) $a\cdot b=b\cdot a$	
(2)	(i) $(a+b)+c=a+(b+c)$ (ii) $(a\cdot b)\cdot c=a\cdot(b\cdot c)$	
(3)	$a\cdot(b+c)=a\cdot b+a\cdot c$	
(4)	(i) $a+0=a$ (ii) $a\cdot 0=0$ (iii) $a\cdot 1=a$ (iv) $a^0=1$ (v) $a^1=a$ (vi) $0^a=0$ $(a\neq 0)$ (vii) $1^a=1$	
(5)	$a^c\cdot b^c=(a\cdot b)^c$	
(6)	$a^b\cdot a^c=a^{b+c}$	
(7)	$(a^b)^c=a^{b\cdot c}$	
(8)	(i) $a\le b\wedge c\le d\Rightarrow a+c\le b+d$ (ii) $a\le b\wedge c\le d\Rightarrow a\cdot c\le b\cdot d$ (iii) $a\le b\wedge c\le d\Rightarrow a^c\le b^d$ (פרט למקרה $a=c=b=0$, $d\neq 0$)	
(9)	$2^a>a$	

טבלה ג.4: תכונות מקבילות של קבוצות

(1)	(i) $A \cup B = B \cup A$ (ii) $A \times B \sim B \times A$
(2)	(i) $(A \cup B) \cup C = A \cup (B \cup C)$ (ii) $(A \times B) \times C \sim A \times (B \times C)$
(3)	$A \times (B \cup C) = (A \times B) \cup (A \times C)$ (יחד עם: $B \cap C = \varnothing \Rightarrow (A \times B) \cap (A \times C) = \varnothing$)
(4)	(i) $A \cup \varnothing = A$ (ii) $A \times \varnothing = \varnothing$ (iii) $A \times \{\varnothing\} \sim A$ (iv) $\varnothing \to A = \{\varnothing\}$ (v) $\{\varnothing\} \to A \sim A$ (vi) $A \to \varnothing = \varnothing \ (A \neq \varnothing)$ (vii) $A \to \{\varnothing\} = \{\lambda x \in A.\, \varnothing\}$
(5)	$(C \to A) \times (C \to B) \sim C \to (A \times B)$
(6)	$(B \to A) \times (C \to A) \sim B \cup C \to A$ if $B \cap C = \varnothing$
(7)	$C \to (B \to A) \sim B \times C \to A$ וזה שקול ל: $C \to (B \to A) \sim C \times B \to A$
(8)	(i) $A \prec B \wedge C \prec D \Rightarrow A \cup C \prec B \cup D$ if $B \cap D = \varnothing,\ A \cap C = \varnothing$ (ii) $A \prec B \wedge C \prec D \Rightarrow A \times C \prec B \times D$ (iii) $A \prec B \wedge C \prec D \Rightarrow C \to A \prec D \to B$ (פרט למקרה $A = C = B = \varnothing$, $D \neq \varnothing$)
(9)	$A \prec P(A) \wedge \neg(A \sim P(A))$

באופן דומה ניתן לתרגם כל טענה על עוצמות בטבלה ג.3 לטענה על קבוצות, שאינה מזכירה כלל את מושג העוצמה. תרגום זה ניתן (לכל הטענות בטבלה ג.3) בטבלה ג.4. התרגום הוא מיידי מההגדרות, ולכן ניתן להבין את הקשר בין טבלה ג.3 וטבלה ג.4 בקלות, בתנאי שנשים לב לנקודות הבאות:

- במקומות בהם הטענה של עוצמות נובעת באופן מיידי מטענה חזקה יותר בדבר שוויון קבוצות, מובאת בטבלה ג.4 הזהות על קבוצות. $(1)_{(i)}$ הוא דוגמה לכך.
- בתור קבוצה שעוצמה 1 בחרנו כאן (באופן אקראי) ב- $\{\varnothing\}$.
- בסעיף (7) הסתמכנו (במעבר "וזה שקול ל-...") על $(1)_{(ii)}$ (ועל טענה 3 מפרק זה).
- בסעיף (9) הסתמכנו כבר על כך, ש- $|P(A)| = 2^{|A|}$.
- הסימון $A \prec B$ פירושו, שיש פונקציה ח.ח.ע. מ- A ל- B. למעשה, משמעותו היא בדיוק כמו של $|A| \le |B|$, אך הוא אינו מזכיר "עוצמות".

כדאי לציין, שאת סעיפי (8) בטבלה ג.4 ניתן להחליף בטענות נוחות יותר להוכחה על סמך משפט שהוכחנו, והוא: $a \le b$ אם"ם קיימות קבוצות B ו- A כך ש- $b = |B|$, $a = |A|$ ו- $A \subseteq B$. מזה נובע בקלות, ש:

$(8)_{(i)}$ בטבלה ג.3 נובע מ: $A \subseteq B \wedge C \subseteq D \wedge B \cap D = \varnothing \Rightarrow A \cup C \subseteq B \cup D$

$(8)_{(ii)}$ בטבלה ג.3 נובע מ: $A \subseteq B \wedge C \subseteq D \Rightarrow A \times C \subseteq B \times D$

$(8)_{(iii)}$ בטבלה ג.3 נובע מ: $A \subseteq B \wedge C \subseteq D \Rightarrow C \to A \prec D \to B$

(פרט למקרה: $B = C = \varnothing$, $D \neq \varnothing$).

בצורה זו $(8)_{(i)}$ ו- $(8)_{(ii)}$ הופכים לטריביאליים.

נעבור עתה לדון בהוכחות של הטענות בטבלה ג.4. ראשית נעיר, שכל השוויונות שם הם טריביאליים, ועל רובם (אם לא כולם) עמדנו בעבר. לכן לא נוכיח כאן. היוצא מן הכלל היחיד הוא אולי $4_{(iv)}$, שגם הוא טריביאלי, אבל אין זה אולי טריביאלי להבין, שזה טריביאלי. נסביר אפוא: הקבוצה הריקה $\varnothing$ היא קבוצה של זוגות (ריקה, כמובן), ולכן הינה יחס בין כל שתי קבוצות. כיחס היא מקיימת באופן ריק את תנאי החד-ערכיות, ולכן היא *פונקציה חלקית* מכל קבוצה לכל קבוצה. לבסוף, היא *פונקציה* מ- $\varnothing$ לכל קבוצה A, כיוון שהיא מתאימה משהו מ- A לכל איבר ב- $\varnothing$ (גם זה נכון באופן ריק, כמובן). לכן $\varnothing \in \varnothing \to A$. ברור, שאין שום פונקציה אחרת ב- $\varnothing \to A$, ולכן $\varnothing \to A = \{\varnothing\}$.

אשר ל- (9), אין הוא אלא משפט קנטור.

לגבי הסעיפים ב- (7)-(2) העוסקים באקויפוטנציות, יש צורך בשביל הוכחתם לתת פונקציות שקילות מתאימות. טבלה ג.5 בעמוד הבא מציגה פונקציית שקילות כזו בכל מקרה ומקרה, יחד עם הפונקציה ההפוכה לה. העובדה, ששתי הפונקציות הן אכן הפוכות זו לזו (ובין הקבוצות המתאימות) היא כמעט עניין של חישוב טהור, דומה לזה שעשינו בפרק ב.4 לגבי פונקציית Curry (Cu) וההפוכה שלה (U). החישובים למקרים של (5) ו- (6) מובאים כנספח לפרק זה. מומלץ לעשות אותם תחילה כתרגילים. (אשר ל- (7), הפונקציות Cu ו- U הן בדיוק מה שנדרש להוכחתו, ולכן (7) כבר הוכח למעשה בפרק ב.4!).

לבסוף, לגבי (8) יש (אם מוכיחים אותו ישירות) לתת פונקציות ח.ח.ע. מתאימות בכל אחד משלושת הסעיפים, בהנחה, שנתונות פונקציה ח.ח.ע. F מ- A ל- B ופונקציה ח.ח.ע. G מ- C ל- D (ועם ההנחות הנוספות ב- (i) וב- (iii)). טבלה ג.5 כוללת בסופה גם פונקציות כאלו.

הערות חשובות לטבלה ג.5:

(א) בטבלה נעשה שימוש בפונקציות ההטל π_1 ו- π_2 על זוגות. כדאי לחזור על תכונותיהן היסודיות לפני ההוכחות. במיוחד חשוב ש- $\pi_1(<x,y>) = x$, $\pi_2(<x,y>) = y$, וש- $z = <\pi_1(z), \pi_2(z)>$, כאשר z הינו זוג. כמו כן, נעשה בטבלה שימוש בפונקציות מצומצמות (F/X), וכדאי לחזור גם על תכונות פונקציות כאלה.

(ב) כמו שנרמז בתוך הטבלה, הפונקציה ב- $(2)_{(ii)}$ היא הגדרה רשמית של הפונקציה f מ- $(A \times B) \times C$ ל- $A \times (B \times C)$, שאינטואיטיבית היינו מגדירים כך:

$$f(<<x,y>, z>) = <x, <y,z>> \quad (\text{עבור } x \in A,\ y \in B,\ z \in C)$$

צורת הגדרה מהסוג שתיארנו הרגע ידועה כהגדרה בעזרת pattern matching. היא אפשרית כאן, בגלל שלכל איבר w ב- $(A \times B) \times C$ קיימים $x \in A$, $y \in B$ ו- $z \in C$ *יחידים* כך ש- $w = <<x,y>, z>$.

טבלה ג.5: פונקציות מתאימות לטבלה ג.4

סעיף		פונקציה מתאימה	פונקציה הפוכה
(1)	(ii)	$\lambda x \in A,\ y \in B.\ \langle y,x\rangle$	$\lambda y \in B,\ x \in A.\ \langle x,y\rangle$
(2)	(ii)	$\lambda z \in (A \times B) \times C.$ $\langle \pi_1(\pi_1(z)), \langle \pi_2(\pi_1(z)), \pi_2(z)\rangle\rangle$ $[\ f(\langle\langle a,b\rangle, c\rangle) = \langle a, \langle b,c\rangle\rangle\ ]$	$\lambda z \in A \times (B \times C).$ $\langle\langle \pi_1(z), \pi_1(\pi_2(z))\rangle, \pi_2(\pi_2(z))\rangle$ $[\ g(\langle a,\langle b,c\rangle\rangle) = \langle\langle a,b\rangle, c\rangle\ ]$
(4)	(iii)	$\lambda z \in A \times \{\varnothing\}.\ \pi_1(z) \quad [f(\langle x,\varnothing\rangle) = x\ ]$	$\lambda x \in A.\ \langle x, \varnothing\rangle$
	(v)	$\lambda f \in \{\varnothing\} \to A.\ f(\varnothing)$	$\lambda x \in A.\ \lambda y \in \{\varnothing\}.\ x$
(5)		$\lambda f \in C \to A,\ g \in C \to B.\ \lambda x \in C.$ $\langle f(x), g(x)\rangle$	$\lambda g \in C \to A \times B.$ $\langle \lambda y \in C.\ \pi_1(g(y)), \lambda y \in C.\ \pi_2(g(y))\rangle$
(6)		$\lambda f \in B \to A,\ g \in C \to A.\ \lambda x \in B \cup C.$ If $x \in B$ then $f(x)$ else $g(x)$	$\lambda h \in B \cup C \to A.\ \langle h/B, h/C\rangle$
(7)		$Cu: (C \times B \to A) \to (C \to (B \to A)) =$ $\lambda f \in C \times B \to A.\ \lambda x \in C.\ \lambda y \in B.\ f(x,y)$	$U: (C \to (B \to A) \to (C \times B \to A)) =$ $\lambda g \in C \to (B \to A).\ \lambda x \in C, y \in B.\ (g(x))(y)$
(8)		נניח ש- $G: C \to D$, $F: A \to B$ הן פונקציות ח.ח.ע.:	
	(i)	$\lambda x \in A \cup C.$ If $x \in A$ then $F(x)$ else $G(x)$	
	(ii)	$\lambda x \in A, y \in C.\ \langle F(x), G(y)\rangle$	
	(iii)	$\lambda h \in C \to A.\ \lambda z \in D. \begin{cases} F(h(G^{-1}(z))) & z \in G(C) \\ b_0 & z \notin G(C) \end{cases}$ (כאשר b_0 איבר כלשהו של B)	

(ג) כאמור, את (8) ניתן להחליף בדברים קלים יותר להוכחה (ומה שיש בטבלה הוא יותר בגדר תרגיל). למעשה, את $(8)_{(i)}$ ו- $(8)_{(ii)}$ כבר הוכחנו, ול- $(8)_{(iii)}$ נתנו ניסוח פשוט יותר. לגבי ניסוח זה די להראות, שאם $A \subseteq B$ ו- $C \subseteq D$, אז:

$$H = \lambda h \in C \to A.\ \lambda z \in D.\ \text{If } z \in C \text{ then } h(z) \text{ else } b_0$$

היא פונקציה ח.ח.ע. מ- $C \to A$ ל- $D \to B$, כאשר b_0 איבר כלשהו של B. ואכן, נניח ש- $h_2, h_2 \in C \to A$ ונניח: $H(h_1) = H(h_2)$ אז:

$$\lambda z \in D.\ \text{If } z \in C \text{ then } h_1(z) \text{ else } b_0 = \lambda z \in D.\ \text{If } z \in C \text{ then } h_2(z) \text{ else } b_0$$

ולכן:

$$\begin{aligned} &\forall z \in D.\ \ z \in C \Rightarrow h_1(z) = h_2(z) \\ &\Rightarrow \forall z \in C.\ h_1(z) = h_2(z) \quad (\text{כי } C \subseteq D) \\ &\Rightarrow h_1 = h_2 \end{aligned}$$

הערות:

1. H היא אכן פונקציה מ- $C \to A$ ל- $D \to B$, בגלל ש- $A \subseteq B$ ו- $C \subseteq D$.
2. אם B ריקה, אז לא נוכל למצוא b_0 כנדרש, ו- H למעלה אינה מוגדרת היטב. במקרה זה אבל $A = \varnothing$. אם בנוסף $C \neq \varnothing$, אז $C \to A = \varnothing$, ולכן $\varnothing$ הינה פונקציה ח.ח.ע. מ- $C \to A$ לכל קבוצה, כולל $D \to B$. אם $C = \varnothing$ ו- $D = \varnothing$, אז $A \to B = C \to D = \{\varnothing\}$. לבסוף, אם $A = B = C = \varnothing$ ו- $D \neq \varnothing$, אז $A \to C = \{\varnothing\}$, בעוד $D \to B = \varnothing$, ואין אז לכן פונקציה מ- $C \to A$ אל $D \to B$.

גישה שונה במעט להוכחת $a \le b \wedge c \le d \Rightarrow a^c \le b^d$ היא לפרק זאת לשני חלקים הבאים, שהוכחת כל אחד קלה יותר. את הפרטים נשאיר לקורא:

(א) $a \le b \Rightarrow a^c \le b^c$

(ב) $c \le d \Rightarrow b^c \le b^d$ (פרט למקרה $b = c = 0$ ו- $d \neq 0$).

דוגמאות לשימושים בחוקי הפעולות

(א) אם $n \subset \mathrm{N}$, אז

$$a \cdot n = \overbrace{a + a + \ldots + a}^{n \text{ פעמים}}$$

$$a^n = a \cdot a \cdot a \cdot \ldots \cdot a$$

הוכחה:

$$a \cdot n = a(1 + 1 + \ldots + 1) = a \cdot 1 + a \cdot 1 + \ldots + a \cdot 1 = a + a + \ldots + a$$

$$a^n = a^{1+1+\ldots+1} = a^1 \cdot a^1 \cdot \ldots \cdot a^1 = a \cdot a \cdot a \cdot \ldots \cdot a$$

%%

הערה:

בפרט נכון הדבר ל- $a \in \mathbf{N}$, ואנו רואים אפוא, שלמספרים הטבעיים פעולות הכפל והחזקה שהגדרנו, אכן זהות לאלה הידועות. זוהי הוכחה לכך, ללא הסתמכות על תכונה מס' (8) בטבלה ג.2 (טבלת התכונות של קבוצות סופיות), ולכן קיבלנו כאן *הוכחה* לנוסחאות שם! (תכונה מס' (8) הנ"ל סיפקה אומנם *מוטיבציה* להגדרות שלנו, אך מאז ***לא*** הסתמכנו עליה בהוכחות).

%%

(ב) $\aleph_0 \cdot n = \aleph_0$ כאשר $n \in \mathbf{N}^+$

$\aleph \cdot n = \aleph$ כאשר $n \in \mathbf{N}^+$

הוכחה ראשונה:

$\aleph_0 \cdot n = \aleph_0 + \aleph_0 + \dots + \aleph_0 = \aleph_0$ (כי $\aleph_0 + \aleph_0 = \aleph_0$).

הוכחה שנייה:

$\aleph_0 = \aleph_0 \cdot 1 \le \aleph_0 \cdot n \le \aleph_0 \cdot \aleph_0 = \aleph_0$ (כי $1 \le n \le \aleph_0$). לכן $\aleph_0 \cdot n = \aleph_0$.

ההוכחות לגבי $\aleph$ דומות (על סמך הנוסחאות $\aleph + \aleph = \aleph$ ו- $\aleph \cdot \aleph_0 = \aleph$, אותן כבר הוכחנו).

(ג) $\aleph_0^n = \aleph_0$ כש- $n \in \mathbf{N}^+$.

הוכחה:

אינדוקציה על n[7].

(ד) $\aleph_0 + n = \aleph_0$ כש- $n \in \mathbf{N}$.

הוכחה:

תרגיל.

(ה) אם $a \le \aleph$, אז $\aleph + a = \aleph$.

הוכחה:

$\aleph = \aleph + 0 \le \aleph + a \le \aleph + \aleph = \aleph \Leftarrow 0 \le a \le \aleph$

מסקנה: $\aleph + \aleph_0 = \aleph$, ו- $\aleph + n = \aleph$ ל- $n \in \mathbf{N}$.

[7] למעשה, גם בשביל הוכחה 1 של (ב) יש צורך באינדוקציה כדי להראות ש- $\aleph_0 + \aleph_0 + \dots + \aleph_0 = \aleph_0$ (העובדה שמדובר במספר סופי של מחוברים היא קריטית לצורך זה!). גם הוכחת (א) היא למעשה באינדוקציה.

(ו) $\mathbf{N} \to P(\mathbf{N}) \sim P(\mathbf{N})$

הוכחה:

$$|\mathbf{N} \to P(\mathbf{N})| = |P(\mathbf{N})|^{|\mathbf{N}|} = \left(2^{\aleph_0}\right)^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = |P(\mathbf{N})|$$

(ז) $P(\mathbf{N}) \times P(\mathbf{N}) \sim P(\mathbf{N})$

הוכחה:

$$|P(\mathbf{N}) \times P(\mathbf{N})| = |P(\mathbf{N})| \cdot |P(\mathbf{N})| = 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0} = |P(\mathbf{N})|$$

(ח) אם $n \in \mathbf{N}$ ו- $n \geq 2$, אז $\aleph_0^{\aleph_0} = n^{\aleph_0} = 2^{\aleph_0}$.

הוכחה:

$2^{\aleph_0} \leq \aleph_0 \leq n \leq 2$. לכן: $2^{\aleph_0} \leq n^{\aleph_0} \leq \aleph_0^{\aleph_0} \leq \left(2^{\aleph_0}\right)^{\aleph_0}$.

אבל $\left(2^{\aleph_0}\right)^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$. לכן כל האי-שוויונות בשרשרת האחרונה הם למעשה שוויונות.

מסקנה: $(\mathbf{N} \to \mathbf{N}) \sim (\mathbf{N} \to \{0,1\})$.

הערה:

דוגמאות (ו), (ז) והמסקנה ב- (ח) מדגימות היטב את הכוח הרב שבשימוש בחוקי עוצמות. להוכיח עובדות אלו ישירות (על-ידי בניית פונקציות שקילות) אינו דבר של מה בכך – ואילו כאן ניתנת הוכחה של שורה אחת בדיוק... (למעשה, עצם ***גילוי*** העובדות הללו התאפשר בעיקר בגלל השימוש בעוצמות!).

נשתמש עתה בדוגמה (ח) כדי להוכיח את המשפט הבא:

משפט:

$\aleph = 2^{\aleph_0}$ (ולכן $|\mathbf{R}| = 2^{\aleph_0}$).

הוכחה:

נראה ש- $2^{\aleph_0} \leq \aleph \leq 10^{\aleph_0}$. כיוון ש- $2^{\aleph_0} = 10^{\aleph_0}$ לפי דוגמה (ח), נקבל ש- $\aleph = 2^{\aleph_0}$. עתה $|(0,1)| = \aleph$, ולכל מספר בקטע הזה מתאים פיתוח עשרוני אינסופי יחיד. פיתוח זה אינו בעצם אלא פונקציה מ-$\mathbf{N}^+$ ל- $\{0,1,\ldots,9\}$: אם $x \in (0,1)$, אז $x = 0.x_1x_2x_3\ldots$, ו- $f_x = \lambda i \in \mathbf{N}^+ . x_i$ היא פונקציה כזו. יתר על כן, אם $x \neq y$, אז $f_x \neq f_y$ (כי $x \neq y$ אם"ם הם שונים באיזו ספרה בפיתוח). על כן, $\lambda x \in (0,1). f_x$ היא פונקציה ח.ח.ע. מ- $(0,1)$ אל $N^+ \to \{0,1,\ldots,9\}$ ומכאן $\aleph = |(0,1)| \leq |N^+ \to \{0,\ldots,9\}| = 10^{\aleph_0}$.

מצד שני, נוכל להגדיר פונקציה $G:(N^+\to\{1,2\})\to(0,1)$ על-ידי:

$$G(f)=0.f(1)f(2)f(3)\dots$$

הפונקציה נותנת פיתוחים עשרוניים אינסופיים (ללא אפסים כלל) וברור שהיא ח.ח.ע..

לכן:

$$2^{\aleph_0}=\left|N^+\to\{1,2\}\right|\le\left|(0,1)\right|=\aleph$$

קיבלנו אכן, ש- $\aleph\le 10^{\aleph_0}=2^{\aleph_0}$ ו- $2^{\aleph_0}\le\aleph$. לכן $\aleph=2^{\aleph_0}$.

מסקנה 1: $\mathbf{R}\sim P(\mathbf{N})$.

מסקנה 2: $\aleph\cdot\aleph=\aleph$.

הוכחה:

$\aleph=2^{\aleph_0}=2^{\aleph_0+\aleph_0}=2^{\aleph_0}\cdot 2^{\aleph_0}=\aleph\cdot\aleph$.

מסקנה 3: $\mathbf{R}\times\mathbf{R}\sim\mathbf{R}$.

הוכחה:

$|\mathbf{R}|=\aleph=\aleph\cdot\aleph=|\mathbf{R}\times\mathbf{R}|$.

תרגילים:

(א) $\mathbf{R}^n\sim\mathbf{R}$ לכל $n\in\mathbf{N}^+$.

(ב) $\mathbf{N}\to\mathbf{R}\sim\mathbf{R}$.

על השערת הרצף

העוצמה האינסופית הקטנה ביותר היא $\aleph_0$. מבין כל העוצמות האינסופיות האחרות, אותן הכרנו עד עתה, הקטנה ביותר היא $\aleph=2^{\aleph_0}$. שאלה המתבקשת לכן היא: האם באמת אין שום עוצמה ביניהן? ההשערה שהתשובה היא חיובית – כלומר: שאין עוצמה a בין $\aleph_0$ ו- $2^{\aleph_0}$ (או: כל קבוצה חלקית אינסופית של $\mathbf{R}$ היא ב"מ, או שוות-עוצמה עם $\mathbf{R}$) – ידועה בשם ***השערת הרצף*** (CH). קנטור עשה מאמצים נואשים להוכיחה, אך ללא הצלחה. היום אנו יודעים למה: מעבודותיהם של גדל (1940) וכוהן (1963) ***ידוע*** לנו, שמערכת האקסיומות המקובלת של תורת הקבוצות אינה מספיקה בשביל להוכיח או להפריך השערה זו. לעומת זאת, ***לא ידוע*** לנו אם היא נכונה או לא, וספק אם אי-פעם נדע (יש כאלה שסוברים, שזוהי שאלה חסרת משמעות. זה מכניס אותנו אבל רחוק לתחום הפילוסופיה של המתמטיקה, ואין באפשרותנו לדון בסוגיות כאלה במסגרת קורס זה).

על חיסור וחילוק

לסיום פרק זה נעשה דיון קצר בשאלה הבאה: הרחבנו את פעולות החיבור, הכפל והחזקה לעוצמות כלשהן. מדוע, כך תמה אולי הקורא, לא ניסינו להכליל גם את החיסור והחילוק? התשובה היא, שהדבר לא ניתן להיעשות (לעוצמות אינסופיות) בצורה פרודוקטיבית. ניקח לדוגמה את החיסור. במספרים הטבעיים זוהי פעולה הפוכה לחיבור במובן הבא: אם $a \geq b$, אז:

$$x = a - b \Leftrightarrow b + x = a$$

כלומר: אם $a \geq b$, אז $a - b$ הוא ה- x ה*יחיד* כך ש- $b + x = a$. ברם, כשעוברים לעוצמות אינסופיות, שוב אין בהכרח למשוואה $b + x = a$ פתרון יחיד. למשל: למשוואה $\aleph_0 + x = \aleph_0$ יש הפתרונות הבאים: $0,1,2,\ldots$ ואפילו $\aleph_0$ עצמו. כל אחד מהם זכאי באותה מידה לתואר "$\aleph_0 - \aleph_0$". בהמשך נראה (ולא קשה להוכיח זאת כתרגיל כבר עכשיו), שלכל a אינסופי יש למשוואה $a + x = a$ לפחות את הפתרונות $x = 0,1,2,\ldots$ ו- $x = \aleph_0$. לכן ברור, שאין משמעות לדבר על "$a - a$".

ניתן להציג את הבעיה עם חיסור גם מנקודת ראות אחרת. הגדרה "טבעית" לחיסור $a - b$ יכלה להיראות כך: $a - b = |A - B|$, כאשר A ו- B קבוצות כך ש- $B \subseteq A$, $a = |A|$ ו- $b = |B|$. ברם, פעולת "חיסור" כזו *אינה* מוגדרת היטב, כיוון שיש בהגדרתה תלות במייצגים. אם נרצה, למשל, לחשב לפיה את $\aleph_0 - \aleph_0$, הרי אם, מצד אחד, ניקח $A = B = \mathbf{N}$, נקבל $0 = |\varnothing| = |\mathbf{N} - \mathbf{N}| = "\aleph_0 - \aleph_0"$. מצד שני, אם ניקח $A = \mathbf{N}$, $B = \mathbf{N}_{even}$, אז נקבל:

$$"\aleph_0 - \aleph_0" = |\mathbf{N} - \mathbf{N}_{even}| = |\mathbf{N}_{odd}| = \aleph_0$$

כיוון ש- $\aleph_0 \neq 0$ (ובגדול), פעולת החיסור אינה מוגדרת היטב (שימו לב, שלגבי קבוצות *סופיות* ההגדרה הנ"ל היא תקפה!).

באופן דומה אפשר להסביר, למה אין כל טעם לדבר על חילוק של עוצמות אינסופיות. כיוון ש- $\aleph_0 \cdot n = \aleph_0$ ו- $\aleph_0 \cdot \aleph_0 = \aleph_0$, הרי "$\aleph_0 / \aleph_0$" היה צריך להיות שווה ל- 1, ל- 2, ל- 3, ... ואפילו ל- $\aleph_0$!

נספח: הוכחת (5) ו- (6) בטבלה ג.5

הוכחת (5):

נסמן:

$$F = \lambda f \in C \to A, g \in C \to B.\ \lambda x \in C.\ <f(x), g(x)>$$

$$G = \lambda h \in C \to (A \times B).\ <\lambda y \in C.\ \pi_1(h(y)), \lambda y \in C.\ \pi_2(h(y))>$$

ברור ש- $F:((C\to A)\times(C\to B))\to(C\to A\times B)$

ו- $G:(C\to(A\times B))\to((C\to A)\times(C\to B))$.

(i) נניח $<f,g>\in(C\to A)\times(C\to B)$, אז:

$$(G\circ F)(<f,g>) = G(F(<f,g>))$$
$$= G(\lambda x\in C.<f(x),g(x)>)$$
$$=<\lambda y\in C.\ \pi_1\underbrace{((\lambda x\in C.<f(x),g(x)>)(y))}, \lambda y\in C.\ \pi_2\underbrace{((\lambda x\in C.<f(x),g(x)>)(y))}>$$
$$=<\lambda y\in C.\ \underbrace{\pi_1(<f(y),g(y)>)}, \lambda y\in C.\ \underbrace{\pi_2(<f(y),g(y)>)}>$$
$$=<\lambda y\in C.f(y), \lambda y\in C.\ g(y)>$$
$$\overset{\eta}{=}<f,g>$$

לכן $G\circ F=i_{(C\to A)\times(C\to B)}$.

(ii) נניח: $h:C\to(A\times B)$, אז:

$$(F\circ G)(h) = F(G(h))$$
$$= F(<\lambda y\in C.\ \pi_1(h(y)), \lambda y\in C.\ \pi_2(h(y))>$$
$$=\lambda x\in C.\ <\underbrace{(\lambda y\in C.\pi_1(h(y)))(x)},\underbrace{(\lambda y\in C.\pi_2(h(y)))(x)}>$$
$$=\lambda x\in C.<\pi_1(h(x)), \pi_2(h(x))>$$
$$=\lambda x\in C.\ h(x)$$ (כי $h(x)$ הינו זוג)
$$\overset{\eta}{=}h$$

לכן $F\circ G=i_{C\to A\times B}$.

הוכחת (6)

נסמן:

$F=\lambda f\in B\to A, g\in C\to A.\ \lambda x\in B\cup C.$ If $x\in B$ then $f(x)$ else $g(x)$

$G=\lambda h\in B\cup C\to A.<h/B, h/C>$

אנו מניחים: $B\cap C=\varnothing$.

(i) נניח $h \in B \cup C \to A$, אז:

$$
\begin{aligned}
(F \circ G)(h) &= F(G(h)) \\
&= F(h/B,\ h/C) \\
&= \lambda x \in B \cup C.\ \text{If } x \in B \text{ then } (h/B)(x) \text{ else } (h/C)(x) \\
&= \lambda x \in B \cup C.\ \text{If } x \in B \text{ then } h(x) \text{ else } h(x) \quad (\text{כי } x \notin B \Rightarrow x \in C) \\
&= \lambda x \in B \cup C.\ h(x) \\
&\overset{\eta}{=} h
\end{aligned}
$$

לכן $F \circ G = i_{B \cup C \to A}$.

(הערה: בשביל כיוון זה אין צורך להניח ש- $B \cap C = \varnothing$!).

(ii) נניח $<f,g> \in (B \to A) \times (C \to A)$, אז:

$$
\begin{aligned}
(G \circ F)(<f,g>) &= G(F(<f,g>)) \\
&= G(\lambda x \in B \cup C.\ \text{If } x \in B \text{ then } f(x) \text{ else } g(x)) \\
&= <(\lambda x \in B \cup C.\ \text{If } x \in B \text{ then } f(x) \text{ else } g(x))\ /\ B, \\
&\qquad (\lambda x \in B \cup C.\ \text{If } x \in B \text{ then } f(x) \text{ else } g(x))\ /\ C> \\
&= <(\lambda x \in B.\ \text{If } x \in B \text{ then } f(x) \text{ else } g(x)), \\
&\qquad \lambda x \in C.\ \text{If } x \in B \text{ then } f(x) \text{ else } g(x)> \\
&= <\lambda x \in B.\ f(x),\ \lambda x \in C.\ g(x)>
\end{aligned}
$$

(הרכיב השני – כיוון שאם $x \in C$, אז $x \notin B$, ולכן ה- "else" תופס. זהו המקום היחיד בחישוב, בו משתמשים בנתון $B \cap C = \varnothing$!).

$$\overset{\eta}{=} <f,g>$$

לכן $G \circ F = i_{(B \to A) \times (C \to A)}$.

ג.5 קבוצות בנות מניה ותכונותיהן

בפרק זה נדון בעיקר בתכונותיהן של הקבוצות האינסופיות הפשוטות ביותר: הקבוצות בנות המניה. נזכיר, שקבוצה היא בת-מניה (ב"מ), אם עוצמתה היא $\aleph_0$. נזכיר כמו כן, שבפרק ג.3 ראינו, שאם a עוצמה אינסופית, אז $a \leq \aleph_0$, וש- $a < \aleph_0$ אם"ם a היא סופית (כלומר: $a \in \mathbf{N}$). התכונות של קבוצות בנות-מניה, שנוכיח בפרק זה, מסוכמות בטבלה ג.6 בעמוד 203.

משפט 1:

נניח A ב"מ. אם $B \subseteq A$, או אם יש פונקציה ח.ח.ע. מ- B אל A, או אם יש פונקציה מ- A על B, אז B סופית או ב"מ.

הוכחה:

כל התנאים פירושם הוא, ש- $|B| \leq |A|$ (פרק ג.3). כיוון ש- $|A| = \aleph_0$, $|B| \leq \aleph_0$. מכאן, שאו ש- $|B| = \aleph_0$, או ש- $|B| < \aleph_0$. במלים אחרות: או ש- B ב"מ, או ש- B סופית.

%%

הערה:

את העובדה, שאם יש פונקציה מ- A על B, אז $|B| \leq |A|$, הוכחנו בשעתו על סמך אקסיומת הבחירה. ברם: אם A ב"מ, אז אין צורך באקסיומה זו. ניתן אז לבנות פונקציה ח.ח.ע. מ- B ל- A בצורה מפורשת. ואכן, אם F היא פונקציית שקילות מ- $\mathbf{N}$ על A, ו- f פונקציה מ- A על B, אז $\lambda x \in B.\ F(\mu n \in \mathbf{N}.\ f(F(n)) = x)$ היא פונקציה ח.ח.ע. מ- B ל- A.

%%

משפט 2:

אם A אינסופית ו- B סופית או ב"מ, אז $|A \cup B| = |A|$.

הוכחה:

ברור ש- A ו- $B - A$ הן קבוצות זרות זו לזו, שאיחודן שווה ל- $A \cup B$. לכן:

$$|A \cup B| = |A| + |B - A| \qquad \text{(I)}$$

כיוון ש- $B - A \subseteq B$, $B - A$ היא סופית או ב"מ. לכן:

$$\aleph_0 + |B - A| = \aleph_0 \qquad \text{(II)}$$

כמו כן, מהעובדה ש- A אינסופית נובע שקיימת קבוצה C חלקית ל- A, שהינה בת מניה. כיוון ש- $A - C$ ו- C הן זרות זו לזו ואיחודן הוא A, $|A| = |A - C| + |C|$. לכן:

$$|A| = |A - C| + \aleph_0 \qquad \text{(III)}$$

מ- (I)-(III) נקבל:

$$\begin{aligned} |A \cup B| &\overset{\text{(I)}}{=} |A| + |B - A| \\ &\overset{\text{(III)}}{=} \left(|A - C| + \aleph_0\right) + |B - A| \\ &= |A - C| + \left(\aleph_0 + |B - A|\right) \\ &\overset{\text{(II)}}{=} |A\text{-}C| + \aleph_0 \\ &\overset{\text{(III)}}{=} |A| \end{aligned}$$

מסקנה 1:

אם a עוצמה אינסופית, אז $a + \aleph_0 = a$ ו- $a + n = a$ לכל $n \in \mathbf{N}$. במלים אחרות:

$$a \geq \aleph_0 \wedge b \leq \aleph_0 \Rightarrow a + b = a$$

מסקנה 2:

אם A אינסופית, $B \subseteq A$ סופית או ב"מ, ו- $A - B$ אינסופית, אז $|A| = |A - B|$.

הוכחה:

תמיד $|A| = |A - B| + |B|$ כאשר $B \subseteq A$. אבל לפי משפט 2, אם $A - B$ אינסופית, ו- B סופית או ב"מ, אז: $|A - B| + |B| = |A - B|$. לכן $|A| = |A - B|$ במקרה זה.

תרגיל:

אם A אינסופית ו- B סופית, אז $|A| = |A - B|$.

טבלה ג.6: עובדות על קבוצות סופיות או בנות מניה

(1)	(i)	$a \le \aleph_0 \Rightarrow a \in \mathbf{N} \vee a = \aleph_0$
	(ii)	$a < \aleph_0 \Rightarrow a \in \mathbf{N}$
(2)		נניח A ב"מ.
	(i)	אם $B \subseteq A$, אז B סופית או ב"מ.
	(ii)	אם יש פונקציה ח.ח.ע. מ- B ל- A, אז B סופית או ב"מ.
	(iii)	אם יש פונקציה מ- A על B, אז B סופית או ב"מ.
(3)		אם A ב"מ, $B \neq \varnothing$ סופית או ב"מ, אז $A \times B$ ב"מ.
(4)		איחוד סופי או ב"מ של קבוצות סופיות או ב"מ הוא סופי או ב"מ.
(5)		אם A אינסופית ו- B סופית או ב"מ, אז $A \cup B \sim A$ $(a \ge \aleph_0 \Rightarrow a + \aleph_0 = a + n = a)$
(6)		אם A אינסופית, B סופית או ב"מ ו- $A - B$ אינסופית, אז $A - B \sim A$. מסקנות:
	(i)	אם $\lvert A\rvert \ge \aleph_0$ ו- B סופית, אז $A - B \sim A$.
	(ii)	אם $\lvert A\rvert > \aleph_0$ ו- B ב"מ, אז $A - B \sim A$.

מסקנה 3:

אם A אינסופית ולא ב"מ, ו- $B \subseteq A$ סופית או ב"מ, אז $|A - B| = |A|$.

הוכחה:

בנתונים אלה, לא ייתכן ש- $A - B$ סופית, כי אחרת

$$|A| = |A - B| + |B| \leq \aleph_0 + \aleph_0 = \aleph_0$$

וזה סותר את הנתון, ש- A אינסופית ולא ב"מ. מכאן ש- $A - B$ אינסופית, ולכן $|A - B| = |A|$ לפי מסקנה 2.

משפט 3:

אם A היא ב"מ, ו- B קבוצה לא ריקה, שהיא סופית או ב"מ, אז $A \times B$ היא ב"מ.

הוכחה:

מיידי מכך ש- $\aleph_0 \cdot \aleph_0 = \aleph_0$ וש- $\aleph_0 \cdot n = \aleph_0$.$\forall n \in \mathbf{N}^+$.

מסקנה 4:

(א) קבוצת המספרים הרציונליים היא ב"מ.

(ב) קבוצת המספרים האירציונליים היא קבוצה שעוצמתה א.

הוכחה:

(א) ראינו ש- $\mathbf{Z}$ ב"מ ולכן גם $\mathbf{Z}\text{-}\{0\}$ ב"מ (למה?). לפי משפט 3 נובע לכן, ש- $\mathbf{Z} \times \mathbf{Z}\text{-}\{0\}$ היא ב"מ. עתה, $\lambda x \in \mathbf{Z}, y \in \mathbf{Z}\text{-}\{0\}.\ x/y$ היא פונקציה מ- $\mathbf{Z} \times (\mathbf{Z}\text{-}\{0\})$ על $\mathbf{Q}$. לפי משפט 1 נובע מזה, ש- $\mathbf{Q}$ סופית או בת-מניה. ברור, שאינה סופית. מכאן שהיא ב"מ.

(ב) המדובר בקבוצה $\mathbf{R}\text{-}\mathbf{Q}$, וידוע ש: $|\mathbf{R}| = \aleph > \aleph_0$. ממסקנה 3 והחלק הראשון של המסקנה הנוכחית נובע לכן, ש- $|\mathbf{R}\text{-}\mathbf{Q}| = |\mathbf{R}| = \aleph$.

הערה:

מהמסקנה האחרונה נובע, שיש הרבה יותר מספרים אי-רציונליים מרציונליים!

משפט 4:

איחוד סופי או ב"מ של קבוצות סופיות או ב"מ הוא סופי או ב"מ:

$$(|I| \leq \aleph_0 \wedge \forall i \in I.\, |A_i| \leq \aleph_0) \Rightarrow \left|\bigcup_{i \in I} A_i\right| \leq \aleph_0$$

הוכחה:

נבחר לכל $i \in I$ פונקציה f_i מ- **N** על A_i (אפשרי כי $|A_i| \le \aleph_0$).

נגדיר: $G = \lambda i \in I, n \in \mathbf{N}.\, f_i(n)$. G הינה פונקציה מ- $I \times \mathbf{N}$ אל $\bigcup_{i \in I} A_i$. עתה, אם $x \in \bigcup_{i \in I} A_i$, אז קיים $\ell \in I$, כך ש- $x \in A_\ell$. כיוון ש- f_ℓ היא פונקציה מ- **N** על A_ℓ, יש $n \in \mathbf{N}$ כך ש- $x = f_\ell(n)$. לכן $x = G(\ell, n)$. מכאן ש- G היא פונקציה מ- $I \times \mathbf{N}$ על $\bigcup_{i \in I} A_i$. לכן:

$$\left|\bigcup_{i \in I} A_i\right| \le |I \times \mathbf{N}| = |I| \cdot |\mathbf{N}| \le \aleph_0 \cdot \aleph_0 = \aleph_0$$

הערות:

(1) ההוכחה הנ"ל מניחה, ש- $A_i \neq \varnothing$ לכל $i \in I$ (היכן?). השלימי אותה למקרה, שהנחה זו אינה מתקיימת!

(2) אם בנוסף להנחות של המשפט ידוע גם, ש- $\bigcup_{i \in I} A_i$ אינסופית (למשל: אם A_i אינסופית לאיזה i, או אם $\forall i \in I.\, A_i \subset A_{i+1}$, או אם ידוע, שלכל $n \in \mathbf{N}$ קיים $i \in I$ כך ש- $|A_i| \ge n$), אז $\left|\bigcup_{i \in I} A_i\right| = \aleph_0$.

נביא עתה מספר מסקנות של משפט 4, החשובות במיוחד למדעי המחשב:

משפט 5:

יהי נתון א"ב סופי (או אפילו בן-מניה), שיש בו a סימבולים ($1 \le a \le \aleph_0$). אז קבוצת כל המלים (או ה"מחרוזות") הסופיות, שאפשר להרכיב בעזרתו היא ב"מ. הדבר נכון גם לקבוצות המשפטים, המאמרים והספרים, שאפשר ליצור בעזרת א"ב כזה.

הוכחה:

כל מלה בת k אותיות אפשר לראות כפונקציה מ- $\{1, 2, \ldots, k\}$ אל L – קבוצת הסימבולים בא"ב הנתון. (לדוגמה: אם L היוה הא"ב העברי, אז את המלה "שלום" אפשר לראות כפונקציה f מ- $\{1,2,3,4\}$ אל L, שבה "ש" $= f(1)$, "ל" $= f(2)$, "ו" $= f(3)$, ו- "ם" $= f(4)$). עתה, קבוצת המלים, שאפשר, באופן עקרוני, לבנות בא"ב L היא $\bigcup_{i \in \mathbf{N}^+} \alpha_i$, כאשר α_i היא קבוצת המלים המורכבות מ- i אותיות בדיוק (יש לשים

לב, ש- α_i, למשל, כוללת פה מלים כמו "ףףףף"!). לאור ההבחנה שלנו, α_i (לכל $i \in \mathbf{N}^+$) היא שוות-עוצמה עם $L \to \{1,2,\ldots,i\}$. לכן:

$$|\alpha_i| = |L|^i = a^i \le \aleph_0{}^i = \aleph_0$$

לפי משפט 4 אנו מקבלים, שגם $\left|\bigcup_{i\in\mathbf{N}^+}\alpha_i\right| \le \aleph_0$. מצד שני, הפונקציה המתאימה לכל $k \in \mathbf{N}^+$ את $sss\ldots s$ (k פעמים הסימבול "s", כש- "s" איבר כלשהו של L) היא ח.ח.ע.,

ולכן $\left|\bigcup_{i\in\mathbf{N}^+}\alpha_i\right| \ge \aleph_0$. סך-הכל $\left|\bigcup_{i\in\mathbf{N}^+}\alpha_i\right| = \aleph_0$.

כדי לקבל את קבוצת המשפטים, שניתן ליצור מ- L, עלינו להוסיף סימבול אחד חדש לשפה: "רווח" (או "space"), שתפקידו להפריד בין המלים. משפט פוטנציאלי בשפה בה מדובר הוא פשוט מחרוזת סופית בשפה המורחבת ("זהו משפט", למשל, הינו מחרוזת בת 8 סימבולים). כיוון שעל-ידי הוספת סימבול אחד לא"ב סופי או ב"מ מקבלים א"ב אחר, שאף הוא סופי או ב"מ, גם אוסף המשפטים הוא ב"מ (לפי מה שהראינו על מלים).

לבסוף, כדי לקבל מאמרים או ספרים, יש להוסיף עוד אי-אלו סימני פיסוק. שוב נקבל, שכל ספר אינו אלא מלה (ארוכה למדי...) בא"ב מורחב, שהוא עדיין סופי או ב"מ. לכן גם מספר הספרים הוא ב"מ.

מסקנה:

בשפה המבוססת על א"ב סופי (או ב"מ) יש לכל היותר $\aleph_0$ מלים, $\aleph_0$ משפטים, $\aleph_0$ ספרים אפשריים וכו'.

הוכחה:

ההבדל בין שפות ובין הקבוצות, שבהן דן המשפט הקודם, הוא, שבשפה מסוימת לא כל מחרוזת אפשרית היא גם מלה תקנית (המחרוזת "ףףףף", לדוגמה, אינה מלה בשפה העברית). בדומה, לא כל משפט אפשרי הוא משפט תקין מבחינה תחבירית, וכנ"ל עם ספרים. עם זאת, קבוצת המלים התקניות היא בכל מקרה קבוצה חלקית לקבוצת המחרוזות האפשריות, וזו הינה ב"מ לפי המשפט הקודם. לכן גם היא עצמה סופית או ב"מ. אותו שיקול תופס גם לגבי קבוצת המשפטים בשפה ולגבי קבוצת הטקסטים התקינים בה.

דוגמה:

קבוצת התכניות החוקיות, שאפשר לכתוב בשפות כמו: SCHEME, PASCAL או C++, היא ב"מ.

מהדוגמה האחרונה נובעת מסקנה חשובה מאוד:

מסקנה:

קיימות פונקציות מ- N ל- N, ששום תכנית ב- SCHEME אינה יכולה לחשב. הדבר נכון גם לכל שפת תכנות אחרת.

הוכחה:

$|\mathbb{N}\to\mathbb{N}|=\aleph_0^{\aleph_0}=2^{\aleph_0}>\aleph_0$, בעוד קבוצת התכניות ב- SCHEME (למשל) היא ב"מ, וממילא קבוצת הפונקציות, שאפשר לחשב בעזרתן, היא סופית או ב"מ (למה?). כיוון שכל הפונקציות הקבועות $\lambda n \in \mathbb{N} \cdot k$ $(k \in \mathbb{N})$ הן חשיבות ב- SCHEME, הקבוצה הנ"ל איננה סופית, ולכן היא ב"מ.

הערה:

למעשה, קבוצת הפונקציות החשיבות ב- SCHEME זהה לקבוצת הפונקציות החשיבות ב- PASCAL, או בכל שפת תכנות אחרת. ההוכחה לכך ניתנת בקורס במודלים חישוביים (או בקורס בתורת הרקורסיה).

תרגילים:

נניח A ב"מ. אז הקבוצות הבאות גם הן ב"מ:

(א) $\mathrm{List}(A)$: קבוצת כל הסדרות הסופיות (או "רשימות") של איברי A.

(ב) $P_{fin}(A)$: קבוצת כל תת-הקבוצות הסופיות של A.

%%

הערה על בעיית העצירה:

אחת הבעיות החשובות ביותר לגבי תכניות מחשב היא: האם תכנית מסוימת עוצרת ונותנת פלט עם קלט מסוים, או שמא ממשיכה היא לרוץ לנצח? היה זה מאוד משמח, לו יכולנו לכתוב תכנית אוניברסלית, שתענה מראש על בעיה זו. העובדה, שקבוצת התכניות, שניתן לכתוב בשפת מחשב נתונה, היא ב"מ, מאפשרת לנסח את הספציפיקציה של תכנית כזו באופן מדויק: אם $g_1,g_2,g_3,\ldots$ היא מניה אפקטיבית של כל התכניות עם קלט אחד מ- N, אז מה שאנו רוצים היא תכנית H, שמקבלת שני קלטים: n ו- k, ומחזירה 1 אם g_n עוצרת עם הקלט k, 0 אם לא. עתה, בעזרת שיטת

האלכסון של קנטור (ראה הוכחת משפט קנטור) אפשר להראות, שתכנית כזו היא בלתי אפשרית. אכן, לו היתה אפשרית היינו יכולים לכתוב תכנית P, שעושה את הדבר הבא: היא מקבלת קלט טבעי n ומעבירה את n ו- n כקלטים ל- H. אם מה ש- H מחזירה הוא 0, P תחזיר 1. אם מה ש- H מחזירה הוא 1, P תרוץ לנצח.[8] ברור ש- P היא תכנית שמחכה לקלט אחד מ- $\mathbf{N}$, לכן $P = g_\ell$ לאיזה $\ell \in \mathbf{N}$. עתה, אם נכניס את ℓ עצמו כקלט ל- P, אז P תעצור אםם g_ℓ עוצרת על ℓ (כי $P = g_\ell$), אםם $H(\ell,\ell) = 1$ (מתכונת H), אםם P **לא** עוצרת על ℓ (מהגדרת P). זוהי סתירה!

%%

[8] חסרים פה כמה פרטים טכניים, כמובן, שמושלמים בקורס ב"מודלים חישוביים".

ג.6 עקרונות קומבינטוריים כלליים

בפרק זה נתאר מספר עקרונות קומבינטוריים כלליים, שנשתמש בהם בעיקר בחלק הבא, העוסק בקומבינטוריקה של קבוצות סופיות. עם זאת, העקרונות, שנדון בהם בפרק זה, נכונים לכל הקבוצות, סופיות ואינסופיות כאחת. רשימת העקרונות מסוכמת בטבלה ג.7 בעמוד הבא. הטבלה כוללת מספר פעולות חדשות על עוצמות: C, P ו- E, אותן נגדיר בפרק זה. בחלק אחר אנו רק חוזרים על תכונות הידועות לנו כבר (אלה שב- (4)).

נעבור להוכחת התכונות והדגמתן:

(1) את הנוסחה ב- (1)(א) מוכיחים באינדוקציה על n. לגבי $n = 2$ זוהי פשוט הגדרת חיבור עוצמות. נניח נכונות ל- $n \geq 2$, נוכיח ל- $n + 1$. אז:

$$\biguplus_{i=1}^{n+1} A_n = \left(\biguplus_{i=1}^{n} A_i \right) \uplus A_{n+1}$$

לכן, לפי הגדרת חיבור עוצמות והנחת האינדוקציה:

$$\left| \biguplus_{i=1}^{n+1} A_i \right| = \left| \biguplus_{i=1}^{n} A_i \right| + |A_{n+1}| \underset{\substack{\uparrow \\ \text{הנחת אינדוקציה}}}{=} \sum_{i=1}^{n} |A_i| + |A_{n+1}| = \sum_{i=1}^{n+1} |A_i|$$

הוכחת (1)(ב) דומה. כאן המקרה $n = 2$ נובע מהזהות:

$$A_1 \cup A_2 = A_1 \uplus (A_2 - A_1)$$

ולכן:

$$|A_1 \cup A_2| = |A_1| + |A_2 - A_1| \leq |A_1| + |A_2|$$

(אי השוויון האחרון נובע מהעובדה, ש- $A_2 - A_1 \subseteq A_2$).
את שלב האינדוקציה נשאיר לקוראים.

טבלה ג.7: עקרונות קומבינטוריים כלליים

(1)	(א)	$\left\lvert \biguplus_{i=1}^{n} A_i \right\rvert = \sum_{i=1}^{n} \lvert A_i \rvert$
	(ב)	$\left(\forall i \in \{1,\ldots,n\}. \lvert A_i \rvert \le a_i\right) \Rightarrow \left\lvert \bigcup_{i=1}^{n} A_i \right\rvert \le \sum_{i=1}^{n} a_i$
(2)	(א)	$\lvert A_1 \times A_2 \times \ldots \times A_n \rvert = \lvert A_1 \rvert \cdot \lvert A_2 \rvert \ldots \lvert A_n \rvert$
	(ב)	$\left(\forall \alpha \in I. \lvert A_\alpha \rvert = a\right) \Rightarrow \left\lvert \biguplus_{\alpha \in I} A_\alpha \right\rvert = a \cdot \lvert I \rvert$
	(ג)	$\left(\forall \alpha \in I. \lvert A_\alpha \rvert \le a\right) \Rightarrow \left\lvert \bigcup_{\alpha \in I} A_\alpha \right\rvert \le a \cdot \lvert I \rvert$
(3)	(א)	$\left\lvert \bigcup_{i=1}^{n} A_i \right\rvert > \sum_{i=1}^{n} a_i \Rightarrow \exists i \in \{1, \ldots, n\}. \lvert A_i \rvert > a_i$
	(ב)	$\left\lvert \bigcup_{\alpha \in I} A_\alpha \right\rvert > a \cdot \lvert I \rvert \Rightarrow \exists \alpha \in I. \lvert A_\alpha \rvert > a$
(4)	(א)	$\lvert A \to B \rvert = \lvert B \rvert^{\lvert A \rvert}$
	(ב)	$\lvert P(A) \rvert = 2^{\lvert A \rvert}$
(5)	(א)	(i) $C(a, 1) = P(a, 1) = a$ (ii) $P(a, 0) = C(a, 0) = 1$
	(ב)	אם $a \ge b$ אז $C(a, b) \ge 1$. אחרת $C(a, b) = 0$ ו- $P(a, b) = 0$
	(ג)	$P(a, b) = C(a, b) \cdot E(b)$
	(ד)	$P(b, b) \ge E(b) \ge 1$
	(ה)	$C(a, b) \le P(a, b) \le a^b$
	(ו)	$C(a, b) \le 2^a$
	(ז)	אם $a_1 \le a_2$ אז: $P(a_1, b) \le P(a_2, b)$ $C(a_1, b) \le C(a_2, b)$ $E(a_1) \le E(a_2)$

הערה:

בתורת הקבוצות המתקדמת מוכיחים גם, ש:

$$\forall i \in \{1,\dots,n\}.\ |A_i| < a_i \Rightarrow \left|\bigcup_{i=1}^{n} A_i\right| < \sum_{i=1}^{n} a_i$$

אי-שוויון זה אי-אפשר להכליל לאיחוד אינסופי.

(2) את הוכחת (א) באינדוקציה נשאיר לקוראים.

לגבי (ג), תהי A קבוצה כך ש- $|A| = a$.

תהי $I' = \{\alpha \in I \mid A_\alpha \neq \varnothing\}$, אז $\bigcup_{\alpha\in I'} A_\alpha = \bigcup_{\alpha\in I} A_\alpha$. כמו כן, כיוון ש- $|A_\alpha| \le a$ ו- $A_\alpha \neq \varnothing$ לכל $\alpha \in I'$, הרי קיימת לכל $\alpha \in I'$ פונקציה f_α מ- A **על** A_α. נגדיר: $F = \lambda x \in A,\ \alpha \in I'.\ f_\alpha(x)$. ברור, ש- F היא פונקציה מ- $A \times I'$ אל $\bigcup_{\alpha\in I} A_\alpha$. נראה ש- F היא **על** $\bigcup_{\alpha\in I} A_\alpha$. נניח אפוא ש- $x \in \bigcup_{\alpha\in I} A_\alpha$. אז יש $\alpha_0 \in I'$ כך ש- $x \in A_{\alpha_0}$. כיוון ש- f_{α_0} היא פונקציה מ- A על A_{α_0}, יש $y \in A$ כך ש- $x = f_{\alpha_0}(y)$. לכן $x = F(\alpha_0, y)$

עתה, כיוון שיש[9] פונקציה מ- $A \times I'$ על $\bigcup_{\alpha\in I} A_\alpha$, אז

$$\left|\bigcup_{\alpha\in I} A_\alpha\right| \le |A|\cdot|I'| = a\cdot|I'| \le a\cdot|I|$$

הוכחת חלק (ב) דומה מאוד. ההבדלים הם, שבמקרה זה $I' = I$, אם $\alpha = \beta$ $A_\alpha \cap A_\beta \neq \varnothing$, ואת f_α אפשר לבחור כך שתהיה גם ח.ח.ע.. מעובדות אלה נובע, ש- F, אותה הגדרנו בהוכחת סעיף (ג), היא לא רק על $\bigcup_{\alpha\in I} A_\alpha$, אלא גם ח.ח.ע..

ואכן, נניח $F(\alpha_1, x_1) = F(\alpha_2, x_2)$. כיוון ש- $F(\alpha_1,x_1) \in A_{\alpha_1}$ ו- $F(\alpha_2,x_2) \in A_{\alpha_2}$, הרי $A_{\alpha_1} \cap A_{\alpha_2} \neq \varnothing$, ולכן $\alpha_1 = \alpha_2$. מכאן, שהשוויון $F(\alpha_1, x_1) = F(\alpha_2, x_2)$ אינו אלא $f_{\alpha_1}(x_1) = f_{\alpha_1}(x_2)$. כיוון ש- f_{α_1} ח.ח.ע., $x_1 = x_2$. קיבלנו, שאם $F(\alpha_1, x_1) = F(\alpha_2, x_2)$, אז $<\alpha_1, x_1> = <\alpha_2, x_2>$, כלומר: F ח.ח.ע..

---

[9] אלא אם כן $A_\alpha = \varnothing$ לכל $\alpha \in I$, אבל במקרה זה הטענה הינה טריביאלית.

דוגמאות:

(א) $\mathbf{R} = \biguplus_{i\in\mathbf{Z}} [i, i+1)$. האיחוד פה הוא אכן איחוד זר, כי $[i, i+1) \cap [j, j+1) = \varnothing$

אם $i \neq j$ ו- j, i הם שלמים. כמו כן, $|[i, i+1)| = א$ לכל $i \in \mathbf{Z}$. לכן לפי (2)(ב), $א = |\mathbf{R}| = א \cdot |\mathbf{Z}| = א \cdot \aleph_0$ (זו אינה עובדה חדשה, כמובן).

(ב) במטריצה בת 20 שורות, כשבכל שורה יש 5 מקומות, יש לפי (2)(ב) $20 \cdot 5 = 100$ מקומות (כאן $|I| = 20$, $a = 5$). לפי (2)(ג) מספר המספרים הרשומים במטריצה הוא קטן או שווה ל- 100 (כי אותו מספר יכול, כמובן, להופיע ביותר משורה אחת).

(ג) אם נציב ב- (2)(ג) $a = \aleph_0$ ונניח ש- I סופית או בת-מניה, נקבל ש- $\left|\bigcup_{\alpha\in I} A_\alpha\right| \le \aleph_0 \cdot |I| = \aleph_0$. במלים אחרות: האיחוד של מספר סופי או בן-מניה של קבוצות סופיות או בנות מניה הוא קבוצה סופית או ב"מ. עובדה זו ידועה לנו מהפרק הקודם (וההוכחה שם, אם נבדוק, היא מקרה פרטי של ההוכחה כאן).

(ד) מ-(2)(ב) נובע מיידית, שאם F פירוק של A, ו- $|X| = a$ לכל $X \in F$, אז $|A| = |F| \cdot a$. בפרט: אם R יחס שקילות על A, ו- $|X| = a$ לכל $X \in A/R$, אז $|A| = a \cdot |A/R|$. אם, לעומת זאת, $|X| \le a$ לכל $X \in A/R$, אז לפי (2)(ג) $|A| \le a \cdot |A/R|$.

(3) (א) אם נפעיל על (1)(ב) את העקרון הלוגי, ש- $(\neg\psi \Rightarrow \neg\varphi) \Leftrightarrow (\varphi \Rightarrow \psi)$, נקבל:

$$\neg\left(\left|\bigcup_{i=1}^{n} A_i\right| \le \sum_{i=1}^{n} a_i\right) \Rightarrow \exists i \in \{1,\ldots,n\}.\neg\left(\left|A_i\right| \le a_i\right)$$

נסתמך עתה, באופן חד-פעמי, על העובדה הכללית, שלכל שתי עוצמות a ו- b מתקיים ש- $\neg(a \le b)$ אם"ם $a > b$[10], ונקבל בדיוק את (3)(א). (3)(ב) נובע באופן דומה מ- (2)(ג).

מ- (3)(ב), לדוגמה, נובע, שאם ננסה לחלק 71 אנשים ל- 7 קבוצות, הרי לפחות אחת מקבוצות אלה תכלול למעלה מ- 10 אנשים (כלומר: לפחות 11). בדוגמה זו $|I| = 7$ ו- $a = 10$.

[10] עובדה זו הינה טריביאלית בשלב זה, אם אחת מהעוצמות a או b הינה סופית או ב"מ – וזהו המקרה השימושי באמת. הטענה נכונה, כזכור, באופן כללי, אם כי לא הוכחנו זאת.

שני העקרונות ב- (3) ידועים *מעקרונות שובך-יונים*, כי שניהם מהווים הכללה ישירה של עקרון שובך היונים בצורתו הפשוטה ביותר, והיא: שאם ננסה לחלק $n+1$ עצמים (או יותר) ל- n קבוצות, הרי תהיה לפחות קבוצה אחת, שבה יהיו שניים (או יותר) מהעצמים. עקרון פשוט זה מתקבל מ- (3)(א) אם נציב $a_i = 1$ לכל $1 \le i \le n$, ומ-(3)(ב) אם נציב $a = 1$ (השם "שובך יונים" נובע מהדימוי הספרותי, לפיו אם ננסה לפזר $n+1$ יונים בשובך שבו n תאים, הרי יהיה לפחות תא אחד, בו יהיו שתי יונים או יותר). עקרונות אלו מהווים, למרות פשטותם, כלי נשק חזק בפתרון בעיות לא מעטות. הבה נביא דוגמה.

תרגיל:

הוכח שבכל קבוצה A, שיש בה 501 מספרים טבעיים בין 1 ל- 1000, יש שני מספרים, שאחד מהם מתחלק בשני.

פתרון:

כל מספר טבעי k אפשר לפרק באופן יחיד למכפלה מהצורה $k = 2^{\ell} \cdot m$, כש- m מספר אי-זוגי. כיוון שיש רק 500 מספרים אי-זוגיים בין 1 ל- 1000, יהיו לפי עקרון שובך היונים (הפשוט) לפחות שני מספרים n_1 ו- n_2 ב- A, שיש להם אותו רכיב אי-זוגי, דהיינו $n_1 = 2^{\ell_1} \cdot m$ ו- $n_2 = 2^{\ell_2} \cdot m$, כש- m אי-זוגי. עתה n_1 מתחלק ב- n_2 או n_2 מתחלק ב- n_1 (בהתאם, אם $\ell_1 \ge \ell_2$ או $\ell_2 \ge \ell_1$). (פורמלית, I היא כאן קבוצת המספרים האי-זוגיים בין 1 ל- 1000, ולכל $i \in I$, $A_i = \{n \in A \mid \exists \ell \in \mathbf{N}. n = 2^{\ell} \cdot i\}$. אז $A = \bigcup_{i \in I} A_i$, ולכן $\left|\bigcup_{i \in I} A_i\right| = 501$, בעוד $a = 1$ ו- $|I| = 500$).

נעבור עתה להגדיר את הפעולות C, P ו- E המוזכרות ב- (5) של טבלה ג.7.

הגדרה:

(א) $\mathrm{In}(A, B)$ היא קבוצת הפונקציות הח.ח.ע. מ- B ל- A.

(ב) $P_b(A)$ היא קבוצת הקבוצות החלקיות ל- A, שעוצמתן b:

$$P_b(A) = \{X \in P(A) \mid |X| = b\}$$

(ג) $\mathrm{Eq}(A, B)$ היא קבוצת פונקציות השקילות מ- B ל- A.

הערה:

ברור ש: $A \to B \supseteq \mathrm{In}(A, B) \supseteq \mathrm{Eq}(A, B)$, $P_b(A) \subseteq P(A)$ וש- $\mathrm{Eq}(A, B) = \varnothing$ אם $|A| \ne |B|$.

הגדרה:

יהיו a ו- b עוצמות.

(א) $P(a, b)$ היא $|\mathrm{In}(A, B)|$ כש- A ו- B קבוצות, כך ש- $|A| = a$ ו- $|B| = b$.

(ב) $C(a, b)$ (או $\binom{a}{b}$) היא $|P_b(A)|$, כאשר A קבוצה כך ש- $|A| = a$.

(ג) $E(a)$ היא $|\mathrm{Eq}(A, B)|$, כאשר A ו- B קבוצות, כך ש- $|A| = a$ ו- $|B| = a$.

משפט:

הפעולות P, C ו- E מוגדרות היטב.

הוכחה:

צריך להוכיח, שאם $A \sim A'$ ו- $B \sim B'$, אז:

(א) $\mathrm{In}(A, B) \sim \mathrm{In}(A', B')$

(ב) $\mathrm{Eq}(A, B) \sim \mathrm{Eq}(A', B')$

(ג) $P_b(A) \sim P_b(A')$

תהי אפוא F פונקציית שקילות מ- A על A', G פונקציית שקילות מ- B על B'.

לגבי (א): ראינו בהוכחה קודמת, שבנתונים אלו $H = \lambda f \in B \to A.F \circ f \circ G^{-1}$ היא פונקציית שקילות מ- $B \to A$ על $B' \to A'$. כיוון ש- $\mathrm{In}(A, B) \subseteq B \to A$, כל שצריך להראות הוא, שהתמונה לפי H של $\mathrm{In}(A, B)$ היא בדיוק $\mathrm{In}(A', B')$. ואכן, אם $f \in \mathrm{In}(A, B)$, אז $H(f) = F \circ f \circ G^{-1}$ היא פונקציה ח.ח.ע. (כי היא הרכבה של פונקציות ח.ח.ע.). לכן $H(f) \in \mathrm{In}(A', B')$. מצד שני, אם $g \in \mathrm{In}(A', B')$, אז קל לברר, ש- $g = H(F^{-1} \circ g \circ G)$ וש- $F^{-1} \circ g \circ G \in \mathrm{In}(A,B)$.

הוכחת (ב) כמעט זהה.

לבסוף, לגבי (ג), די אם נראה ש- $F(X)$. $\lambda X \in P_b(A)$. $F(X)$) – התמונה של X לפי F) היא פונקציית שקילות בין $P_b(A)$ ל- $P_b(A')$. זוהי, קודם כל, אכן פונקציה מ- $P_b(A)$ אל $P_b(A')$, כי לכל $X \in P_b(A)$ מתקיים ש- $F(X) \in P(A')$ ו- $|F(X)| = |X| = b$ (כי F ח.ח.ע.). שנית, קל לראות, ש- $F^{-1}(Y)$. $\lambda Y \in P_b(A')$ היא פונקציה הפוכה, כיוון שכאשר F פונקציית שקילות, אז לכל $X \subseteq A$ ו- $Y \subseteq B$ מתקיים, ש- $F(F^{-1}(Y)) = Y$ ו- $F^{-1}(F(X)) = X$.

כאשר מדובר במספרים טבעיים, הרי $C(n, k)$ הוא בדיוק מה שמסומן בדרך-כלל ב- $\binom{n}{k}$ ומוגדר בתור מספר תת-הקבוצות בנות k איברים, שיש לקבוצה בת n איברים ("מספר האפשרויות לבחור k עצמים מתוך קבוצה בת n איברים"). $P(n, k)$ הוא מספר ה"חליפות" של k עצמים מתוך n ("מספר האפשרויות לבחור k עצמים שונים מתוך קבוצה בת n איברים עם חשיבות לסדר"), ו- $E(n)$ הוא מספר ה"תמורות" של קבוצה בת n איברים ("תמורה" של קבוצה אינה אלא פונקציית שקילות מהקבוצה על עצמה). למעשה, המשפט האחרון מוכיח, שכל הפעולות הנ"ל על k ו- n מוגדרות היטב, דבר שלא נעשה כלל בתיכון!

משפט:

לכל שתי עוצמות a,b מתקיים $P(a,b) = C(a,b).\, E(b)$.

הוכחה:

תהיינה A ו- B קבוצות כך ש- $|A| = a$ ו- $|B| = b$.

הרעיון האינטואיטיבי של ההוכחה הינו פשוט ביותר ומוכר היטב מקומבינטוריקה תיכונית: אסטרטגיה אפשרית לבניית פונקציה ח.ח.ע. מ- B ל- A היא לבחור תחילה את התמונה שלה (שעוצמתה חייבת להיות כשל B, דהיינו: b) ואחר-כך לבחור פונקציית שקילות מ- B על תמונה זו. את הבחירה הראשונה אפשר לעשות ב- $C(a,b)$ דרכים, ואת השנייה אפשר אחר-כך לעשות ב- $E(b)$ דרכים – ולכן הכפל.

הוכחה פורמלית:

אם $f \in \text{In}(A, B)$, אז f היא פונקציית שקילות מ- B על התמונה שלה, $f(B)$. ממילא $|f(B)| = |B| = b$. לכן $f(B) \in P_b(A)$, בעוד $f \in \text{Eq}(f(B), B)$. מכאן ש-

$$\text{In}(A, B) = \biguplus_{X \in P_b(A)} \text{Eq}(X, B)$$

האיחוד כאן הוא זר, כי ברור שפונקציות, שתמונתן שונה, הינן שונות זו מזו. (ממה שכתבנו נובע, בעצם, רק ש- $\text{In}(A,B) \subseteq \biguplus_{X \in P_b(A)} \text{Eq}(X,B)$. הכיוון ההפוך נובע מכך, שאם $X \subseteq A$ ו- $f \in \text{Eq}(X, B)$, אז f היא פונקציה ח.ח.ע. מ- B ל- A. כלומר:

$\forall X \in P_b(A).\ \text{Eq}(X,B) \subseteq \text{In}(A,B)$. לכן $\bigcup_{X \in P_b(A)} \text{Eq}(X,B) \subseteq \text{In}(A,B)$). עתה, מהגדרת $E(b)$ נובע, שלכל $X \in P_b(A)$, $|\text{Eq}(X,B)| = E(b)$. מכאן, לפי (2)(ב) של טבלה ג.7:

$$P(a,b) = |\text{In}(A,B)| = E(b) \cdot |P_b(A)| = E(b) \cdot C(a,b)$$

הערה:

ההוכחה מדגימה תופעה כללית: שיקולים אינטואיטיביים מהסוג של ההוכחה האחרונה (דהיינו: פיצול ל"מקרים", כשכל "מקרה" כולל מספר שווה של "אפשרויות") מתורגמים בהוכחות פורמליות להסתמכות על (2)(ב) של טבלה ג.7.

המשפט האחרון סיפק, למעשה, את ההוכחה של (5)(ג) מטבלה ג.7. ההוכחה של שאר הסעיפים נובעת בקלות מההגדרות (אולי בעזרת (5)(ג)):

(א) נניח $a = |A|$. ברור ש- $\lambda x \in A.\{x\}$ היא פונקציית שקילות בין A ובין $P_1(A)$. לכן $a = |A| = |P_1(A)| = C(a,1)$. ברור גם, ש- $E(1) = 1$. לכן $P(a,1) = a$ על סמך (ג).

(ב) נניח $b = |B|$, $a = |A|$. אם $b \le a$, אז מהגדרת $\le$ יש פונקציה ח.ח.ע. מ- B אל A, כלומר: $\text{In}(A,B) \neq \varnothing$, ולכן $P(a,b) \neq 0$. מ-(ג) נובע לכן, שגם $C(a,b) \neq 0$, דהיינו: $C(a,b) \ge 1$. לעומת זאת, אם $b \not\le a$, אז לא קיימת קבוצה חלקית של A שעוצמתה היא b, דהיינו: $P_b(A) = \varnothing$, ולכן $C(a,b) = 0$. ממילא גם $P(a,b) = 0$ (לפי (ג)).

(ד) נניח B קבוצה, כך ש- $|B| = b$. אז $E(b) = |\text{Eq}(B,B)|$ ו- $P(b,b) = |\text{In}(B,B)|$. כיוון ש- $\text{Eq}(B,B) \subseteq \text{In}(B,B)$, $P(b,b) \ge E(b)$. ש- $E(b) \ge 1$ נובע מזה, שתמיד (אפילו כש- B ריקה!) $i_B \in \text{Eq}(B,B)$.

(ה) ש- $P(a,b) \le a^b$ נובע מכך ש- $\text{In}(A,B) \subseteq B \to A$. ש- $C(a,b) \le P(a,b)$ נובע מ-(ג) ו-(ד).

(ו) נובע מכך ש- $P_b(A) \subseteq P(A)$.

(ז) נניח $a_1 \le a_2$. אז קיימות קבוצות A_1 ו- A_2 כך ש- $|A_1| = a_1$, $|A_2| = a_2$ ו- $A_1 \subseteq A_2$. מכך ש- $A_1 \subseteq A_2$ נובע, לפי הגדרה, ש- $P_b(A_1) \subseteq P_b(A_2)$. לכן $C(a_1,b) \le C(a_2,b)$. כמו כן $E(a_1) = |\text{Eq}(A_1,A_1)|$, $E(a_2) = |\text{Eq}(A_2,A_2)|$. נגדיר אפוא:

$$H = \lambda f \in \text{Eq}(A_1,A_1).\ \lambda x \in A_2.\ \text{If } x \in A_1 \text{ then } f(x) \text{ else } x$$

ברור ש- $H : \mathrm{Eq}(A_1, A_1) \to (A_2 \to A_2)$ קל לברר, שלכל $f \in \mathrm{Eq}(A_1, A_1)$, $H(f)$ היא פונקציית שקילות מ- A_2 ל- A_2. לכן, בעצם, $H : \mathrm{Eq}(A_1, A_1) \to \mathrm{Eq}(A_2, A_2)$. כמו כן, טריביאלי ש- H ח.ח.ע., כיוון שלכל f ב- $\mathrm{Eq}(A_1, A_1)$ מתקיים ש- $H(f) / A_1 = f$ (ולכן $H(f_1) = H(f_2) \Leftarrow H(f_1) / A_1 = H(f_2)/A_1 \Leftarrow f_1 = f_2$). לכן $E(a_1) = |\mathrm{Eq}(A_1, A_1)| \le |\mathrm{Eq}(A_2, A_2)| = E(a_2)$.

לבסוף, ש- $P(a_1,b) \le P(a_2,b)$ נובע מ- (ג) ושני האי-שוויונות על C ו- E, שכבר הוכחנו.

תרגילים:

לחשב:

(1) $C(\aleph_0, n)$ ו- $P(\aleph_0, n)$ עבור $n \in \mathbf{N}$

(2) $C(\aleph_0, \aleph_0)$ ו- $P(\aleph_0, \aleph_0)$

*(3) $E(\aleph_0)$ ו- $E(\aleph)$

(4) $C(\aleph, \aleph)$ ו- $P(\aleph, \aleph)$

(5) $C(\aleph, \aleph_0)$ ו- $P(\aleph, \aleph_0)$

פתרון לחלק מתרגילים אלו מובא בנספח לפרק זה.

*נספח: משפט על $C(a,a)$ כש- a אינסופית

משפט:

אם $a+a=a$, אז $C(a,a)=2^a$.

הוכחה:

כיוון ש- $a+a=a$, אז יש קבוצות B, C כך ש-

$$|B|=|C|=|B\cup C|=a \quad \text{ו-} \quad B\cap C=\varnothing$$

נגדיר $F=\lambda X\in P(C).\,X\cup B$.

כיוון שלכל $X\in P(C)$ מתקיים ש- $B\subseteq X\cup B\subseteq B\cup C$, אזי לכל X כזה, $a=|B|\leq|X\cup B|\leq|B\cup C|=a$. מכאן, שלכל $X\in P(C)$, $F(X)\in P(B\cup C)$ ו- $|F(X)|=a$, דהיינו: $F(X)\in P_a(B\cup C)$ לכן $F\in P(C)\to P_a(B\cup C)$. נראה ש- F ח.ח.ע.. נניח אפוא, ש- $X_1,X_2\in P(C)$ ו- $F(X_1)=F(X_2)$. נראה, ש- $X_1=X_2$. נראה, למשל, ש- $X_1\subseteq X_2$ (ההוכחה ש- $X_2\subseteq X_1$ דומה). יהי אפוא $y\in X_1$. אז:

$$\begin{aligned}
& y\in X_1\cup B\\
\Rightarrow\ & y\in F(X_1)\\
\Rightarrow\ & y\in F(X_2) && (\text{כי } F(X_1)=F(X_2))\\
\Rightarrow\ & y\in X_2\cup B\\
\Rightarrow\ & y\in X_2 \ \vee\ y\in B
\end{aligned}$$

אבל כיוון ש- $B\cap C=\varnothing$ ו- $y\in X_1\subseteq C$, לא ייתכן ש- $y\in B$ ומכאן ש- $y\in X_2$.
קיבלנו ש- F הינה פונקציה ח.ח.ע. מ- $P(C)$ אל $P_a(B\cup C)$, ולכן

$$C(a,a)=|P_a(B\cup C)|\geq|P(C)|=2^{|C|}=2^a$$

מצד שני, $C(a,a)\leq 2^a$ לכל a לפי (5)(ו) של טבלה ג.7.
סך-הכל קיבלנו: $C(a,a)=2^a$.

מסקנות: $C(\aleph_0,\aleph_0)=2^{\aleph_0}=\text{א}$ ו- $C(\text{א},\text{א})=2^{\text{א}}$.

הערה:

כיוון שלמעשה $a+a=a$ *לכל* a אינסופית (הגם שההוכחה חורגת מקורס זה), המשפט קובע ש- $C(a,a)=2^a$ לכל a אינסופית.