

מתמטיקה דיסקרטית (בדידה)

חלק חמישי

מסמך זה הוא החמישי והאחרון בסדרת מסמכים הבאים להציג לקורא את עקרונות הקומבינטוריקה ותורת הקבוצות, כפי שהם מתוארים בקורס "מתמטיקה דיסקרטית".

מסמך זה ממשיך מהנקודה בה הסתיים המסמך הרביעי. במסמך זה נדון ברלציות שקילות, מחלקות שקילות, קבוצות מנה ועוצמות.

ידע קודם הנדרש להבנת המסמך הוא לפחות מתמטיקה בהיקף של בגרות 5 יחידות, וכן הבנה של קומבינטוריקה ותורת הקבוצות, כפי שהוצגו במסמכים הקודמים בסדרה זו. אנא שלחו הערות, תיקונים והצעות אל המחבר.

מסמך זה הורד מהאתר <http://underwar.livedns.co.il>. אין להפיץ מסמך זה במדיה כלשהי, ללא אישור מפורש מאת המחבר. מחבר המסמך איננו אחראי לכל נזק, ישיר או עקיף, שיגרם עקב השימוש במידע המופיע במסמך, וכן לנכונות התוכן של הנושאים המופיעים במסמך. עם זאת, המחבר עשה את מירב המאמצים כדי לספק את המידע המדויק והמלא ביותר.

כל הזכויות שמורות לניר אדר

Nir Adar

Email: underwar@hotmail.com

Home Page: <http://underwar.livedns.co.il>

רלציית שקילות

רלציה תקרא רלצית שקילות אם היא רפלקסיבית, סימטרית וטרנזיטיבית.
 R רפלקסיבית אם לכל x מתקיים $(x, x) \in R$
 R סימטרית אם לכל x, y , כך ש $(x, y) \in R$ מחייב כי $(y, x) \in R$
 R טרנזיטיבית אם לכל x, y, z מתקיים $(x, y) \in R, (y, z) \in R \Rightarrow (x, z) \in R$

מחלקת שקילות

בהנתן יחס E מעל A ואיבר $x \in A$, נגדיר את מחלקת השקילות של x המסומנת על ידי $[x]$ באופן הבא:
 $[x] = \{y \mid (x, y) \in E\}$

דוגמא

A_1 - קבוצת האנשים בעולם.

$E_1 = \{(x, y) \mid x, y \text{ live in the same country}\}$

A_2 - כל המילים בעולם.

$E_2 = \{(x, y) \mid x, y \text{ starts with the same letter}\}$

A_3 - קבוצת המספרים הטבעיים.

$E_3 = \{(x, y) \mid x, y \text{ has the same module in diving by 3}\}$

עבור E_1 - מהי מחלקת השקילות של x הגר בישראל?

$[x] = \{\text{כל תושבי ישראל}\}$

עבור E_2 - מהי מחלקת השקילות של המילה "אבא"?

$[x] = \{\text{כל המילים המתחילות ב-א}\}$

עבור E_3 :

$[0] = \{0, 3, 6, 9, \dots\}$

$[1] = \{1, 4, 7, 10, \dots\}$

$[2] = \{2, 5, 8, 11, \dots\}$

$[3] = \{0, 3, 6, 9, \dots\}$

$[4] = \{1, 4, 7, 10, \dots\}$

ניתן לראות כי:

$[0] = [3] = [6] = \dots$

$[1] = [4] = [7] = \dots$

$[2] = [5] = [8] = \dots$

$[0] \cap [1] = \emptyset$

$[1] \cap [2] = \emptyset$

$[0] \cap [2] = \emptyset$

מתקיים:

$[0] \cup [1] \cup [2] = N$

למה 1

יהיו $x, y \in A$ ו E רלצית שקילות ב A .

א. $[x] = [y]$ אם ורק אם $x E y$.

ב. $[x] \cap [y] = \emptyset$ אם $[x] \neq [y]$.
 • מחלקת שקילות היא לא קבוצה ריקה (היא מתאפיינת על ידי איבר מסויים)

הגדרה

הקבוצה A/E מוגדרת כך:

$$A/E = \{[x] \mid x \in A\}$$

היא נקראת קבוצת המנה של A לפי E .

למה 2

לכל $B_1, B_2 \in A/E$, או $B_1 \cap B_2 = \emptyset$ או $B_1 = B_2$.

קבוצה Π היא חלוקה של קבוצה A אם מתקיימים התנאים הבאים:
 א. אם כל איבר של Π הוא תת קבוצה לא ריקה ב- A .
 ב. בעבור כל $x \in A$ קיים בדיוק איבר אחד $S \in \Pi$ עבורו $x \in S$.

טענה

א. A/E היא חלוקה של קבוצה A .
 ב. אם Π היא חלוקה של קבוצה A אזי היחס הבא הוא יחס שקילות.
 $E = \{(x, y) \mid (\exists S, S \in \Pi), x \in S \text{ and } y \in S\}$

ומכאן: $A/E = \Pi$.

למה 3

E רלציית שקילות מעל A . איחוד כל מחלקות השקילות ייתן את הקבוצה A :

$$\bigcup_{x \in A} [x] = A$$

דוגמא

1.

A קבוצת השלמים בין 0 ל-100.

$$R = \{(x, y) \mid x \equiv y \pmod{10}\}$$

רפלקסיביות: כן: $x \equiv x \pmod{10}$

סימטריות: כן: $x \equiv y \pmod{10} \Rightarrow y \equiv x \pmod{10}$

טרנזיטיביות: כן: $x \equiv y \pmod{10}, y \equiv z \pmod{10} \Rightarrow x \equiv z \pmod{10}$

לכן זוהי רלציית שקילות. כעת נגדיר מי הן מחלקות השקילות, ונמצא את קבוצת המנה.
 מחלקות השקילות מאופיינות על ידי השאריות בחלוקה ב-10. לכן קבוצת המנה היא:

$$A/R = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9]\} = \{[x] \mid 0 \leq x \leq 9, x \in N\}$$

2.

A קבוצה, B תת קבוצה של A.

$$R = \{(x, y) \mid x = y \text{ or } x, y \in B\}$$

רפלקסיביות: כן: כי $x=x$.סימטריות: כן: xRy אם $x=y$ אז ברור ש yRx כי הם שווים.אם $x \neq y$ אזי x, y שייכים ל B ולכן גם y, x שייכים ל B ולכן yRx .טרנזיטיביות: כן: xRy, yRz אם כולם זהים ברור כי xRz אם x, y, z לא זהים כולם, אזי הם שייכים ל B, ולכן xRz .

איפיון מחלקות השקילות:

מחלקת שקילות אחת היא B וכל איבר ב A מהווה מחלקת שקילות.

$$A/R = \begin{cases} \{[x] \mid x \in A \setminus B\} & B = \emptyset \\ \{[x] \mid x \in A \setminus B\} \cup \{B\} & B \neq \emptyset \end{cases}$$

נשים לב לכתיבה: $\{[x] \mid x \in A \setminus B\} \cup \{B\}$. הכתיבה $\{[x] \mid x \in A \setminus B\} \cup B$ היא טעות במקרה זה. הסבר בעזרת דוגמא:

$$A = \{1, 2, 3, 4, 5\}$$

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

$$\{[x] \mid x \in A \setminus B\} \cup \{B\} = \{\{3\}, \{4\}, \{5\}, \{1, 2\}\}$$

$$\{[x] \mid x \in A \setminus B\} \cup B = \{\{3\}, \{4\}, \{5\}, 1, 2\}$$

הביטוי השני הוא כבר לא חלוקה למחלקות שקילות!

3.

מה מספר רלציות השקילות בקבוצה סופית A?

הגדרת קבוצת מנה מגדירה רלציה ולהפך. השאלה היא למעשה כמה חלוקות אפשריות.

נניח כי $|A|=n$. מספר הרלציות הוא מספר האפשרויות לחלק את האלמנטים לתתי קבוצות כך שבכל קבוצה אלמנט אחד לפחות, ואין אלמנט המופיע ביותר מקבוצה אחת.

כלומר, הבעיה שקולה לחלוקה של n אלמנטים שונים לתאים זהים, כך שאין תא ריק ואין הגבלה על מספר התאים.

$$p(n) = \sum_{k=0}^{n-1} \binom{n-1}{k} p(k), p(0) = 1$$

עוצמותהקדמה לעוצמות

עבור קבוצות סופיות, בעלות אותו גודל, ניתן לבנות התאמה חז"ע בין שתי הקבוצות. גודל במקרה זה הוא מספר האיברים בכל קבוצה. הבעיה מתחילה כשאנחנו עוברים לקבוצות אין סופיות. נעביר את ההגדרה הזו עבור גודל לקבוצות אין סופיות:

הגדרה

שתי קבוצות A ו- B הן בעלות עוצמה שווה, בעלות אותה קרדינליות, אם קיימת ביניהם התאמה חז"ע, כלומר אם קיימת פונקציה $f: A \rightarrow B$ שהיא פונקציה של A על B וחז"ע. נאמר ש $A \sim B$ ונקודות ונסמן $A \sim B$, (רצליה E המוגדרת כך: $E = \{(A, B) \mid B \sim A\}$ קיימת פונקציה חז"ע ועל M ל- B) $\{ (A, B) \mid B \sim A \}$ מחלקות השקילות נקראות "מספרים קרדינלים" (עוצמות). כל קבוצה שהמספר הקרדינלי שלה הוא מספר סופי, היא קבוצה סופית.

הגדרה

קבוצה A תיקרא סופית אם קיים $n \in \mathbb{N}$ כך שקיימת התאמה חז"ע בין A לבין $\{1, 2, \dots, n\}$. הקבוצה A תיקרא אין סופית אם לא קיים n כזה.

טענה

הקבוצה \mathbb{N} היא אינסופית.

הגדרה (הגדרת קבוצה אינסופית לפי תכונה)

קבוצה A היא אינסופית אם קיימת $f: A \rightarrow A$ חז"ע כך $f(A) \subset A$. קיימת פונקציה $f: A \rightarrow A$ לעצמה שהיא חז"ע אבל לא על. קבוצה A היא סופית אם איננה סופית.

- שתי ההגדרות הנ"ל לקבוצה אין סופית שקולות.

מסקנה

עבור 2 קבוצות אינסופיות A ו- B , אם $|A| = |B|$ אזי קיימת פונקציה f חז"ע מ- A ל- B שאיננה על.

משפט

- אם A היא קבוצה אינסופית, אזי מתקיימות הטענות הבאות:
1. כל קבוצה B המקיימת $A \subseteq B$ היא קבוצה אינסופית.
 2. כל קבוצה B שעבורה קיימת פונקציה חז"ע $f: A \rightarrow B$ היא אינסופית.
 3. כל קבוצה B שעבורה קיימת פונקציה על $f: A \rightarrow B$ היא אינסופית.
 4. הקבוצה $P(A)$ היא אינסופית.
 5. לכל קבוצה לא ריקה B , הקבוצה $A \times B$ היא אינסופית.
 6. עבור כל קבוצה B , הקבוצה $A \cup B$ היא אינסופית.
 7. לכל קבוצה לא ריקה B , הקבוצה A^B (קבוצת הפונקציות מ B ל A) היא אינסופית.

הגדרה

העוצמה של קבוצת הטבעיים היא:

$$|N| = \aleph_0$$

כל הקבוצות שיש ביניהן לטבעיים פונקציה חד חד ערכית ועל, עוצמתן תהיה גם \aleph_0 .

הגדרה

קבוצה A תיקרא בת מניה אם $|A| = \aleph_0$.

משפט קנטור שריידר ברנשטיין

לכל 2 קבוצות A ו B :
אם קיימת פונקציה $f: A \rightarrow B$ שהיא 1:1 וגם קיימת פונקציה $g: B \rightarrow A$ שהיא 1:1, אזי קיימת התאמה חז"ע בין A ל B .

טענה

$$|N| = |Q^*|, Q^* = \left\{ \frac{m}{n} \mid m, n \in N, n \neq 0 \right\}$$

נוכיח על ידי משפט קנטור שריידר ברנשטיין:

$$\forall n \in N, f(n) = \frac{n}{1}, f: N \xrightarrow{1:1} Q^*$$

$$\forall \frac{m}{n} \in Q^*, g\left(\frac{m}{n}\right) = 2^n \cdot 3^m, G: Q^* \xrightarrow{1:1} N$$

כיצד מוכיחים שקבוצה A היא בת מניה?

1. מציגים התאמה חז"ע בין A לקבוצה שידוע שהיא בת מניה.
2. מציגים פונקציה חז"ע מ A לקבוצה כלשהי בת מניה ופונקציה חז"ע מקבוצה בת מניה כלשהי ל A ומשתמשים במשפט CSB.
3. מציגים מניה של אברי A שמקיימת:
 - א. לפני כל איבר נמצא מספר סופי של איברים.
 - ב. כל איבר נמצא במקום כלשהו במניה.

טענה

Z בת מניה.

$0, 1, 2, \dots, -1, -2, -3, \dots$ זהו לא פתרון טוב!!!

פתרון טוב:

$Z \quad 0 \quad 1 \quad -1 \quad 2 \quad -2 \quad 3 \quad -3$

$N \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6$

נשים לב שזוהי למעשה התאמה חד חד ערכית.

בשלב ה- k של המניה סופרים את k ואת $-k$.

כל שלב ספירה הוא סופי, ולפני כל איבר יש מספר סופי של שלבים ולכן ניתן למנות אותו לאחר מספר סופי של שלבים.

- אם קיימת מניה עם חזרות, קיימת גם מניה בלי חזרות. מעבר ממניה עם חזרות למניה בלי חזרות בצורה פשוטה: מתקדמים לפי הסדר שקבענו. אם האיבר הנוכחי כבר נספר, לא נספור אותו שוב. אחרת נספור אותו.

טענה

Q^* - הרציונליים החיוביים - בת מניה. $a, b \in N, \frac{a}{b}$

אם נצליח לספור את החיוביים, נוכל לספור גם את השליליים.
ניצור טבלה:

	1	2	3	4	5	...
1	1/1	1/2	1/3	1/4	1/5	
2	2/1	2/2	2/3	2/4	2/5	
3	3/1	3/2	3/3	3/4	3/5	
4	4/1	4/2	4/3	4/4	4/5	
5	5/1	5/2	5/3	5/4	5/5	
...						

ישנם מספרים שמופיעים כמה פעמים - למשל - כל האלכסון הראשי.

בשלב ה- $k, k > 1$, נספור את כל המספרים מהצורה $\frac{a}{b}$ כך ש- $a+b=k$. (יש $k+1$ מספרים כאלו).

כל מספר מהצורה $\frac{a}{b}$ יספר בשלב ה- $a+b$. קיים שלב כזה! זוהי ספירה עם חזרות.

טענה

איחוד של מספר סופי או מספר בן מניה של קבוצות בנות מניה הוא בן מניה.
נבנה טבלה בה בעמודה יהיו הקבוצות השונות ובתוך הטבלה יהיו האיברים השונים של הקבוצות.
נעבור על האלכסונים בצורה דומה לזו שעברנו בדוגמא הקודמת.

טענה

אם A ו- B בנות מנייה, אזי $A \times B$ בת מנייה.

דוגמא

Σ קבוצה סופית של אותיות. קבוצת המילים הסופיות מעל Σ היא בת מניה.

- כמה מילים באורך k כלשהו קיימות? Σ^k .
- בשלב ה- k נספור את כל המילים באורך k .
- כל שלב הוא סופי ולכן משל.

דוגמא

Σ קבוצה בת מניה של אותיות. קבוצת המילים הסופיות מעל Σ היא בת מניה. עבור כל n יש אין סוף אפשרויות לאותיות לכן אי אפשר להשתמש בדרך פתרון הקודמת. פתרון:

- בשלב ה- k , $k \geq 1$, נספור את כל המילים באורך קטן שווה k שהאותיות בהן הן מהקבוצה $\{a_0, a_1, \dots, a_{k-1}\}$

כמה מילים כאלו יש? $\sum_{i=1}^k k^i$.

נוכיח שכל מילה נספרת בספירה זו. תהיי מילה $k_1 k_2 \dots k_r$. נסתכל על האות שבה האינדקס הוא מקסימלי. יהי s האינדקס. המילה תיספר בשלב שהוא המקסימום בין r ל- $s+1$

טענה

אם B בת מניה ו- A קבוצה סופית, אזי B^A היא בת בניה. B^A זוהי קבוצת כל הפונקציות מ- A ל- B .

בשלב ה- k נספור את כל הפונקציות מ- A לקבוצה $\{b_1, \dots, b_k\}$.

יש $k^{|A|}$ פונקציות כאלו.

בהינתן פונקציה $f: A \rightarrow B$, יהיו $f(a_1), \dots, f(a_n)$ ערכי הפונקציה.

יהיו $b_{1j} = f(a_j), 1 \leq j \leq n$

נביט על הערך המקסימלי מבין $b_{11}, b_{12}, \dots, b_{1n}$. יהי r המקסימלי שבהם. לכן f נספרת בשלב ה- r .

טענה

לכל קבוצה אין סופית A יש תת קבוצה בת מניה.

נבנה קבוצה $B: B = \{b_i \mid i \in \mathbb{N}\}$.

יהי $b_0 \in A$ ותהי $B_0 = \{b_0\}$.

יהי $b_1 \in A/B_0$ ותהי $B_1 = \{b_0, b_1\}$.

נניח $B_i \subset A$ כאשר $B_i = \{b_0, b_1, \dots, b_i\}$.

יהי $b_{i+1} \in A/B_i$ ותהי $B_{i+1} = B_i \cup \{b_{i+1}\}$.

כל אחת מהקבוצות B_i היא סופית. איחוד כל איברי קבוצות B_i הוא אינסופי. המניה היא הסדר בו בחרנו איברים מ- A . הקבוצה הזו היא עם עוצמה שווה לזו של הטבעיים.

משפט

לכל קבוצה אינסופית A יש תת קבוצות אמיתיות (תת קבוצה ממש) בעלות עוצמה שווה ל- A .

כיוון

הצורה היחידה שניתן להוכיח זאת היא לקחת תת קבוצה M ולהוכיח שקיימת בינה לבין A פונקציה חז"ע ועל.
אם ניקח את A ונוציא ממנה רק איבר אחד, נקבל קבוצה בעלת אותה עוצמה.

הוכחה

תהי $B \subseteq A$ בת מניה $B = \{b_i \mid i \in \mathbb{N}\}$, ותהי $B' = \{b_i \mid i \in \mathbb{N}, i \geq 1\}$.
נבנה העתקה בין שתי הקבוצות שהיא התאמה חז"ע.
נבנה g חד חד ערכית ועל.

$$g: A \rightarrow A \setminus \{b_0\}$$

$A \setminus \{b_0\}$ היא תת קבוצה אמיתית של A . אם נצליח למצוא g כמבוקש נראה כי ל- A ול- $A \setminus \{b_0\}$ יש אותה עוצמה.
נגדיר את g :

$$g(x) = \begin{cases} x & x \in A \setminus B \\ b_{i+1} & x \in B (\Rightarrow x = b_i) \end{cases}$$

מסקנה חשובה

אם ניקח קבוצה אינסופית ונוציא ממנה מספר סופי של איברים, נשמור על עוצמת הקבוצה.

מסקנה ללא הוכחה

אם ניקח קבוצה מעוצמה גבוהה, ונוציא מספר איברים מעוצמה נמוכה יותר, העוצמה תישמר.

קבוצות שאינן בנות מניה - שיטת הליכסון של קנטור

יהי A קבוצת כל המילים הבינריות האינסופיות.
נניח ש- A בת מניה. כלומר יש מניה מהטבעיים אל הקבוצה הזו.
תהי $f: \mathbb{N} \rightarrow A$ שהיא חז"ע ועל.

$$f(0) = b_{00}b_{01}b_{02}\dots$$

$$f(1) = b_{10}b_{11}b_{12}\dots$$

...

$$f(i) = b_{i0}b_{i1}b_{i2}\dots$$

נרצה להראות מילה בינרית שלא רשומה בצורה הזו. (נראה שהפונקציה איננה על).
נבנה את המילה y :

$$y = y_0y_1y_2\dots$$

$$y_i \neq b_{ii}$$

מילה זו שונה מהמילה הראשונה של הפונקציה בביט הראשון. שונה מהמילה השנייה בביט השני, שונה מהמילה השלישית בביט השלישי וכך הלאה.

כל מילה לא תואמת, לכן המילה הזו לא התקבלה.

העוצמה של קבוצת המילים הבינריות האינסופיות נקראת עוצמת רצף. היא זהה לעוצמה של קבוצת המספרים הממשיים.

סימון לעוצמת רצף: $|A| = \aleph$

עוצמת רצף

מספרים ממשיים:

נסתכל על הקטע $[0,1]$.

נטען כי קבוצת המספרים בקטע היא איננה בת מניה.

כל מספר בקטע בין 0 ל 1 יכול להיות מיוצג בצורה הבאה: $0.x_1x_2x_3\dots$ כאשר $0 \leq x_i \leq 9$.

נניח שקיימת $g: N \rightarrow [0,1]$. נכתוב אותה:

$$g(0) = 0.x_{00}x_{01}x_{02}\dots$$

$$g(1) = 0.x_{10}x_{11}x_{12}\dots$$

...

$$g(i) = 0.x_{i0}x_{i1}x_{i2}\dots$$

נבנה את המספר y :

$$y = y_0y_1y_2\dots$$

$$y_i \neq x_{ii}$$

המספר הזה שוב לא יתקבל.

ההוכחה במקרה זה לא מושלמת, יש בה בעיה. הבעיה נובעת מהאופי של המספרים הממשיים.

יש מספרים שיש להם יותר מייצוג אחד. המספר $0.3999\dots = 0.4000\dots$. למשל, $0.9999\dots = 1$.

זוהי בעיה של דיוק, לא דיוק לננו במילים הבינריות האינסופיות.

לכן נוסיף דרישה נוספת למספר y .

$$y = y_0y_1y_2\dots$$

$$y_i \neq x_{ii}, y_i \neq \{0,9\}$$

הדרישה נובעת רק מהאופי של המספרים הממשיים.

משחק - הפרדוקס של ראסל

תהי S קבוצה המכילה את כל הקבוצות שאינן מכילות את עצמן. האם S מכילה את עצמה?

אם S מכילה את עצמה, אז היא איננה ב- S , כלומר אינה מכילה את עצמה.

ואם S אינה מכילה את עצמה, אזי S מכילה את עצמה.

טענה

$$|[a,b]| = |(a,b)| = |(a,b]|$$

נפצל למספר חלקים.
טענה: עוצמת הקטע $[0,a]$ היא עוצמת הרצף.

$$f : [0,1] \rightarrow [0,a]$$

$$f(x) = ax$$

טענה: עוצמת הקטע $[x,x+a]$ היא רצף.

$$f : [0,a] \rightarrow [x,x+a]$$

$$f(y) = x + y$$

מסקנה שכבר הוכחנו ברגע זה: עוצמת כל קטע כלשהו על המספרים הממשיים היא עוצמת רצף.

עכשיו נרצה לעבור לקטע אינסופי.

$$f : (0,1) \rightarrow (1,\infty)$$

$$f(x) = \frac{1}{x}$$

מכאן העוצמה של הקטע $(0,1)$ זהה לעוצמה של הקטע $(1,\infty)$.
ברור וטריויאלי כי $|(0,2)| = |(0,\infty)|$. ומכאן $|(-2,2)| = |(-\infty,\infty)|$ שזה זהה לפי הטענה ההתחלתית ל $|(-\infty,\infty)| = |(0,1)|$.

טענה

A, B קבוצות אינסופיות.
 $B > A$ אם קיימת פונקצייה על $f : B \rightarrow A$ אבל לא קיימת פונקצייה על $g : A \rightarrow B$.

משפט קנטור

עבור כל קבוצה A , מתקיים שקבוצת החזקה של A , $|p(A)| > |A|$.

מכאן נובע שיש מספר אינסופי של עוצמות.
עוצמת קבוצת החזקה של הטבעיים היא עוצמת רצף, כי $2^{\aleph_0} -$ זהו מזכיר סידרה בינרית, שזו עוצמת רצף.

הוכחה

עבור קבוצות סופיות, ההוכחה ברורה.
 נניח שהקבוצה A היא קבוצה אינסופית.
 נרצה לראות כי $|p(A)| > |A|$. נרצה להראות שיש פונקציה על מ $p(A)$ ל A .
 נבנה פונקציה:
 יהי z כלשהו שייך ל A .

$$f : P(A) \rightarrow A$$

$$f(x) = \begin{cases} z & |X| \neq 1 \\ v & |X| = 1, X = \{v\} \in A \end{cases}$$

נראה שלא קיימת פונקציה על מ $P(A)$ ל A .
 נניח קיום פונקציה כזו, $g : A \rightarrow p(A)$ על.
 נגדיר קבוצה חדשה S , תת קבוצה של A : $S = \{x \mid x \in A, x \notin g(x)\}$
 התשובה של $g(x)$ זהו איבר מקבוצת החזקה. x איבר ב A . $g(x)$ זהו איבר בקבוצת החזקה (זוהי תת קבוצה של A) ולכן לא התכונה שייך או לא שייך לקבוצה.
 S שייכת לקבוצת החזקה של S . ולכן יש איבר של A שמועתק לתוך S .
 ואז אם a שייך ל S , לפי הגדרת S הוא איננו שייך ל S .
 אם a איננו שייך ל S , לפי ההגדרת הוא שייך ל S .
 סתירה. פירושה ש g לא על. משל.

EOF