תורת החישוביות – תרגול הכנה
לוגיקה ותורת הקבוצות

מה יש כאן?

בקורס תורת החישוביות נניח ידע בסיסי **בתורת הקבוצות ובלוגיקה**, והכרות עם מושגים בסיסיים כמו **א"ב, מילה ושפה**. לטובת מי ששכח חומר זה, או שלא למדו מעולם, ניסינו לרכז כאן מספר הגדרות ומונחים שישמשו אותנו.

חלק 1 מכיל חזרה על סימונים בסיסיים בתורת הקבוצות, ובוודאי מוכר לרובכם. חלק 2 דן בשפות. חלק 3 דן בעוצמות של קבוצות, חלק 4 מתמקד בקבוצות בנות מניה, חלק 5 דן בשפות סופיות, וחלק 6 מציג מונחים בסיסיים בלוגיקה.

מה לקרוא?

הקורס **לוגיקה ותורת הקבוצות** הוא כיף וקל, אבל למי שבכל זאת לא למד אותו מומלץ לעבור על חלקים 1, 3, 4 (קבוצות) ו־6 (לוגיקה). מי שלא למד **אוטומטים ושפות פורמאליות**, מומלץ לו לקרוא את חלקים 2 ו־5.

1 קבוצות

<u>הגדרה (לא פורמלית)</u>: אוסף של איברים ללא חשיבות לסדר או חזרות נקרא <u>קבוצה</u>.

- תסומן בסוגריים מסולסלים: $\{1,2\} = \{2,1\} = \{1,2,2\}$
- איברים בקבוצה יכולים להיות קבוצות בעצמם.

$$\begin{aligned} A &= \{\{1,2,3\},\{4,5\}\} \\ B &= \{1,2,3,4,5\} \end{aligned}$$

- עבור קבוצה סופית X נסמן ב־$|X|$ את מספר האיברים ב־X.

$$|A| = 2 \quad |B| = 5 \quad |\{1,2,2\}| = 2$$

<u>הגדרה:</u>
קבוצה ללא איברים תקרא <u>הקבוצה הריקה</u>, ותסומן ב־$\emptyset$.
<u>דרכים לסימון קבוצה:</u>

- רשימת איברים: $\{1,3,8\}$
- חוקיות: $\{0,2,4,6,\ldots\}$
- קבוצות מוכרות: $\mathbb{N}$, $\mathbb{N}^+$, $\emptyset$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{C}$.
- תכונה משותפת: $\{p \in \mathbb{N} \mid p \text{ is a prime number}\}$ – קבוצת המספרים הראשוניים.

סימונים בסיסיים

שייכות: $x\in A$. אבר x שייך לקבוצה A.

אחרת, $x\notin A$.

הכלה: $B\subseteq A$ כל אבר ב־B שייך גם ל־A.

במקרה כזה B היא תת־קבוצה של A.

שיוויון: $A=B$. מתקיים $B\subseteq A$ וגם $A\subseteq B$.

אחרת, $A\neq B$.

פעולות בסיסיות בין קבוצות

איחוד: $A\cup B=\{x\mid x\in A$ או $x\in B\}$

חיתוך: $A\cap B=\{x\mid x\in A$ וגם $x\in B\}$

הפרש: $A\setminus B=\{x\mid x\in A$ וגם $x\notin B\}$

קבוצת החזקה

קבוצת החזקה: $\mathcal{P}(A)=\{S\mid S\subseteq A\}$ - קבוצת כל תתי הקבוצות של A.

דוגמה

$\mathcal{P}(\{1,2\})=\{\emptyset,\{1\},\{2\},\{1,2\}\}$.

2 שפות

א"ב Σ היא קבוצה של אותיות.

בקורס זה נתעניין כמעט תמיד רק בקבוצות א"ב סופיות. בפרט, פעמים רבות נתעניין בא"ב הבינארי $\Sigma=\{0,1\}$.

מילה w מעל א"ב Σ היא אוסף סופי סדור של אפס או יותר אותיות מתוך הא"ב. למשל: $0,01,0010101$ וגם ε (המילה הריקה, המורכבת מאפס אותיות) הן מלים מעל הא"ב $\{0,1\}$.

אורך של מילה w יסומן $|w|$.

שפה L מעל א"ב Σ היא קבוצה של מלים מעל הא"ב Σ.

שרשור של שתי מילים w_1,w_2, שיסומן w_1w_2, הוא מילה בודדת המורכבת מאותיות w_1 ומיד לאחריהן אותיות w_2.

שרשור של שתי שפות, L_1,L_2, הוא שפה המוגדרת:

$$L_1L_2=\{w_1w_2\mid w_1\in L_1,\ w_2\in L_2\}$$

סגור־קלייני של א"ב Σ, שיסומן Σ^*, הוא שפת כל המלים מעל הא"ב Σ.

נסמן ב־Σ^n את קבוצת כל המלים מעל הא"ב Σ שאורכן n בדיוק. אז מתקיים:

$$\Sigma^0=\{\varepsilon\}$$
$$\Sigma^n=\left\{wv\mid w\in\Sigma^{n-1},\ v\in\Sigma\right\}$$
$$\Sigma^*=\bigcup_{n\geq 0}\Sigma^n$$

ניתן להפעיל את האופרטור "סגור־קלייני" גם על שפה, ולא רק על א"ב. בהינתן שפה L, השפה L^* מכילה את כל המלים שהן שרשורים של מספר סופי של מלים ב־L.

3 עָצמות

נחזור לדיון בקבוצות. עבור קבוצות סופיות "גודל" של קבוצה הוא פשוט מספר האברים שלה. נרצה להגדיר מושג של "גודל" גם עבור קבוצות אינסופיות. מושג זה ייקרא עצמה של קבוצה.

הגדרה כזו אינה משימה טריוויאלית. למשל, קבוצת המספרים **הטבעיים הזוגיים** מוכלת בקבוצת המספרים **הטבעיים**, לכן קבוצת הזוגיים בוודאי אינה "גדולה" מקבוצת הטבעיים. אבל האם היא קטנה ממנה ממש? בהגדרות שלנו, נראה שהקבוצות הללו הן שוות עצמה.

<u>תזכורת:</u>

פונקציה $f:A\to B$ תקרא <u>חד־חד־ערכית</u> (חח"ע) אם לכל $a,a'\in A$ מתקיים $f(a)\neq f(a')$.

פונקציה $f:A\to B$ תקרא <u>על</u> אם לכל $b\in B$ קיים $a\in A$ כך ש־$f(a)=b$. האבר a הנ"ל לא חייב להיות יחיד.

<u>סימונים והגדרות</u>

תהינה A,B קבוצות.

$A\sim B$ – A ו־B <u>שוות עצמה</u> – קיימת $f:A\to B$ חח"ע ועל.

$A\preceq B$ – העצמה של B <u>גדולה או שווה</u> מהעצמה של A – קיימת $f:A\to B$ חח"ע. באופן שקול, קיימת $g:B\to A$ על.

$A\prec B$ – העצמה של B <u>גדולה ממש</u> מהעצמה של A – מתקיים $A\preceq B$ וגם $A\not\sim B$.

<u>טענות</u>

1. אם $A\sim B, B\sim C$ אז $A\sim C$.
2. אם $A\preceq B, B\preceq C$ אז $A\preceq C$.
3. אם $A\preceq B$ וגם $B\preceq A$ אז $A\sim B$ (קנטור, שרדר, ברנשטיין).

<u>תרגילים</u>

1. הוכיחו כי $\mathbb{Z}\sim\mathbb{N}$.
2. הוכיחו $\mathbb{R}\sim(0,1)$ (כאשר $(0,1)$ קטע פתוח ב־$\mathbb{R}$).
3. הוכיחו כי $\mathbb{Q}\sim\mathbb{N}$.

<u>משפט (קנטור)</u>

לכל קבוצה A מתקיים $A\prec\mathcal{P}(A)$.

4 קבוצות בנות מניה

קבוצה A תקרא **בת מניה** (ב"מ) אם $A\preceq\mathbb{N}$ (כלומר קיימת $f:A\to\mathbb{N}$ חח"ע).

תזכורת: A בת מניה אם"ם קיימת $g:\mathbb{N}\to A$ על. פונקציה כזו תקרא **מניה** של A.

<u>סימון</u>

אם $A\sim\mathbb{N}$, נאמר כי <u>עצמת A היא $\aleph_0$</u>.

<u>סיווג של קבוצות מוכרות</u>

סופית		אינסופית
בת־מניה		לא בת־מניה
ב"מ סופית	ב"מ אינסופית ($\aleph_0$)	אינסופית לא ב"מ
$\emptyset, \{1,2\}$	$\mathbb{Z}\sim\mathbb{Q}\sim\mathbb{N}\sim$ראשוניים	$\{0,1\}^{\mathbb{N}}\sim\mathcal{P}(\mathbb{N})\sim\mathbb{R}$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$

<u>משפט</u>

איחוד בן מניה של קבוצות בנות מניה הוא בן מניה.

תרגיל

נזכיר כי $\{0,1\}^*$ היא שפת כל המילים הבינאריות (הסופיות!). הוכיחו כי $\{0,1\}^*$ היא בת מניה.

פתרון

לכל מילה ב־$\{0,1\}^*$ יש אורך סופי, לכן אפשר להציג את $\{0,1\}^*$ כך: $\{0,1\}^* = \cup_{n\in\mathbb{N}} \{0,1\}^n$.

כל קבוצה מהצורה $\{0,1\}^n$ היא סופית – מכילה את כל הסדרות הבינאריות באורך n, ולכן גודלה 2^n. בפרט, כל קבוצה כזו היא בת מניה.

הקבוצה $\{0,1\}^*$ היא לכן איחוד בן מניה ($\mathbb{N}$) של קבוצות בנות מניה ($\{0,1\}^n$), ולפי המשפט $\{0,1\}^*$ בת מניה.

הערה

טיעון דומה מראה כי לכל Σ סופית מתקיים ש־Σ^* היא בת מניה.

משהשתכנענו ש־Σ^* היא בת מניה, נציע מניה שלה, שתקרא סדר לקסיקוגרפי: נמנה את המילים לפי אורכן, ובתוך כל קבוצה של מילים באורך נתון נמנה את המילים בסדר מילוני. כלומר, $w_1 < w_2$ אם $|w_1| < |w_2|$ או אם $|w_1| = |w_2|$ אבל w_1 באה לפני w_2 בסדר מילוני רגיל (דהיינו, כשמשווים אות־אות). נמספר את המילים ב־Σ^* כ־$w_0, w_1, w_2, \ldots$.

לכסון וקבוצות שאינן בנות מניה

ראינו מספר טכניקות כדי להראות שקבוצה היא בת מניה. נראה כעת דוגמה להוכחה שקבוצה אינה בת מניה.

תרגיל

תהי A קבוצת כל הסדרות הבינאריות האינסופיות. הוכיחו כי A אינה בת מניה.

פתרון – באמצעות לכסון

נניח בשלילה כי קיימת ל־A מניה, כלומר קיימת $f : \mathbb{N} \to A$ על. כדי להגיע לסתירה, נבנה סדרה $b \in A$ כך שלכל $n \in \mathbb{N}$ מתקיים $f(n) \neq b$.

נסמן את האבר ה־i של $a \in A$ ב־a_i. ספציפית, את האבר ה־i של תמונת f על $n \in \mathbb{N}$ נסמן $f(n)_i$.

נגדיר את $b = b_0 b_1 b_2 \cdots$ על־ידי $b_i = 1 - f(i)_i$.

שכנעו עצמכם כי b מוגדר היטב ומקיים $b \in A$.

לכל $i \in \mathbb{N}$ מתקיים $f(i)_i \neq b_i$, ולכן גם $f(i) \neq b$. מכאן ש־f אינה על A, והגענו לסתירה.

איור הפתרון:

	0	1	2	3	$\cdots$
$f(0)$	$f(0)_0$	$f(0)_1$	$f(0)_2$	$f(0)_3$	$\cdots$
$f(1)$	$f(1)_0$	$f(1)_1$	$f(1)_2$	$f(1)_3$	$\cdots$
$f(2)$	$f(2)_0$	$f(2)_1$	$f(2)_2$	$f(2)_3$	$\cdots$
$f(3)$	$f(3)_0$	$f(3)_1$	$f(3)_2$	$f(3)_3$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
$b =$	$1 - f(0)_0$	$1 - f(1)_1$	$1 - f(2)_2$	$1 - f(3)_3$	$\cdots$

הערה חשובה

באמצעות טיעון דומה ניתן להראות כי קיים מספר לא בן מניה של **שפות**. נניח כי $L_0, L_1, \ldots$ היא מניה של כל השפות מעל Σ ונבנה שפה $L = \{w_i | w_i \notin L_i\}$. כלומר, כל מילה $w_i \in \Sigma^*$ נמצאת ב־L אם ורק אם היא אינה נמצאת ב־L_i. מכאן שלכל i מתקיים $L \neq L_i$ (שכן הן נבדלות במילה w_i), ולכן L אינה מופיעה במניה שהצענו – סתירה. מכאן שיש מספר לא בן מניה של שפות.

הטענה שמספר השפות אינו בן מניה ניתנת להסקה בקלות גם ממשפט קנטור: אוסף כל השפות מעל Σ הוא בדיוק אוסף כל תת הקבוצות של Σ^*, כלומר הוא $\mathcal{P}(\Sigma^*)$, ועל פי משפט קנטור עצמתו גדולה ממש מעצמת Σ^*.

באופנים דומים ניתן להראות שיש גם מספר לא בן מניה של פונקציות $f : \Sigma^* \longrightarrow \{0,1\}$.

המחשב אינו כל יכול

כדוגמה למה שנלמד בקורס, נראה שלא כל פונקציה אפשר לחשב. לצורך הדיון, נתעניין רק בתוכניות מחשב בשפת c שמקבלות קלט בינארי, כלומר מילה ב־$\{0,1\}^*$, ולכל קלט כזה עוצרות ומוציאות פלט 0 או 1. נזהה כל תוכנית עם פונקציה מהצורה $f:\{0,1\}^*\rightarrow\{0,1\}$ שאותה היא מחשבת.

אם נחשוב על תוכנית c בתור קובץ טקסט בודד, קל לראות שקבוצת כל תוכניות ה־c האפשריות היא בת־מניה. (ניתן להסתכל על כל תוכנית c בתור מילה מעל א"ב סופי, שמורכב מכל סימני הטקסט שניתן להקליד בקובץ.)

מכיוון שיש מספר **לא בן מניה** של פונקציות כנ"ל, אך רק מספר **בן מניה** של תוכניות c, אז **משיקולי ספירה** בהכרח קיימת פונקציה שאין **אף תוכנית c המסוגלת לחשב אותה** (למעשה, יש אינסוף פונקציות כאלו). כלומר, יש **יותר** פונקציות מאשר תוכניות בשפת c.

כלומר, ראינו כי יש אינסוף פונקציות שאי־אפשר לחשב, ואולם לא ראינו ולו פונקציה אחת מפורשת שכזו. זהו החיסרון הגדול שטיעון ספירה – הוא אינו קונסטרוקטיבי.

5 אינדוקציה ו־Σ^*

ראינו שלא את כל הפונקציות מהצורה $f:\{0,1\}^*\rightarrow\{0,1\}$ אפשר לחשב. לעומת זאת, אם נגביל את אורך מילת הקלט, נוכל לחשב כל פונקציה, ובקלות.

<u>טענה:</u>

כל פונקציה מהצורה $f:\Sigma^n\longrightarrow\Sigma$, עבור n קבוע, ניתנת לחישוב על־ידי תוכנית בשפת c. (נניח לצורך העניין כי $\sum=\{0,1\}$.)

<u>הסבר אינטואיטיבי:</u>

מכיוון שהתחום $\sum^n$ הוא סופי (נניח למשל $n=3$), ניתן לכתוב תוכנית מן הצורה:

```
if (input == 000) return 0;
if (input == 001) return 1;
if (input == 010) return 1;
...
```

כאשר ערכי ה־return נקבעים כמובן בהתאם לפונקציה הספציפית שברצוננו לחשב.

<u>טענה:</u>

כל פונקציה מהצורה $f:\cup_{0\leq i\leq n}\Sigma^i\longrightarrow\Sigma$ עבור n קבוע, ניתנת לחישוב על ידי תוכנית בשפת c.

<u>הוכחה - באינדוקציה:</u>

מקרה הבסיס הוא מקרה פרטי של הטענה הקודמת.

צעד האינדוקציה: תהי f פונקציה כלשהי מן הצורה $f:\cup_{0\leq i\leq n}\Sigma^i\longrightarrow\Sigma^1$. נוכיח כי קיימת תוכנית c המחשבת את f. "נחלק" את f לשני חלקים, בהתאם למילת הקלט.

החלק הראשון: $f:\cup_{0\leq i\leq n-1}\Sigma^i\longrightarrow\Sigma$ ניתן לחישוב על־ידי תוכנית c על־פי הנחת האינדוקציה. נסמן תוכנית זו p_1.

החלק השני: $f:\Sigma^n\longrightarrow\Sigma$, ניתן גם הוא לחישוב על־ידי תוכנית c על־פי הטענה הקודמת. נסמן תוכנית זו p_2.

התוכנית p לחישוב הפונקציה f תפעל כך:

```
if (input's length < n) return p_1(input);
else return p_2(input);
```

חשוב להדגיש, שעל אף שה"הוכחה" שלעיל מראה שהטענה נכונה עבור כל n טבעי, היא **איננה** מראה שניתן לחשב כל פונקציה מן הצורה $f:\Sigma^*\longrightarrow\Sigma$. הרי ראינו **משיקולי ספירה** שקיימות פונקציה מצורה זו שלא ניתנות לחישוב.

<u>שימו לב:</u>

האינדוקציה מאפשרת לנו להוכיח את הטענה עבור כל n טבעי. היא **אינה** מאפשרת מעבר ל־$n=\infty$.

6 לוגיקה

נרצה לתאר באופן פורמאלי אמיתות של טענות שתלויות במספר סופי של טענות בסיסיות. למשל, "השמש זורחת וגם יורד גשם", "היום יום שלישי או יום רביעי", וכו'. הטענות הבסיסיות, "השמש זורחת" וכו', תקראנה פסוקים אטומיים, ומהן נרכיב פסוקים "גדולים יותר". בנוסף, נגדיר השמה, שהיא פונקציה שנותנת ערך אמת לכל פסוק אטומי. לפי כללים לוגיים מוכרים נסיק מהו ערך האמת של הפסוק כולו.

סימונים

פסוקים אטומיים יסומנו ב־$p_1, p_2, \ldots$.

קשרים יסומנו או: $\vee$, וגם: $\wedge$, לא: $\neg$.

השמה היא פונקציה $v : \{p_1, p_2, \ldots\} \to \{T, F\}$.

ערך האמת של פסוק α תחת השמה v יסומן $\bar{v}\left(\alpha\right)$. זהו אבר מ־$\{T, F\}$, שנקבע לפי v ו־α בהתאם לכללים לוגיים פשוטים שלא נציג כאן באופן פורמאלי.

נאמר שהשמה v **מספקת** פסוק α אם $\bar{v}\left(\alpha\right) = T$.

תרגיל

יהי פסוק $\alpha = p_1 \wedge \left(p_2 \vee \neg p_3\right)$, ותהי v ההשמה הנותנת ערך T לכל p_i. מהי $\bar{v}\left(\alpha\right)$?

CNF

מבנה ספציפי של פסוקים לוגיים הוא CNF. נאמר שפסוק הוא פסוק CNF אם:

הפסוק כולו הוא "וגם" של הרבה פסוקים אחרים, שיכונו **פסוקיות.**,

וכל פסוקית היא "או" של משתנים אטומיים ושלילתם.

דוגמאות

$\left(p_1 \vee p_4\right) \wedge \left(\neg p_1 \vee p_2 \vee \neg p_3\right)$,

$\left(p_7 \vee p_4\right) \wedge \neg p_4$.

הערות

- השמה מספקת פסוק CNF אם"ם היא מספקת כל פסוקית בו.
- לכל פסוק יש פסוק בצורת CNF ששקול לוגית אליו (כלומר מקבל אותו ערך אמת עבור כל ההשמות).