אימות חומרה־תוכנה

אלי דיין[1]

6 בדצמבר 2013

[1] <eliyahud@post.tau.ac.il>

תקציר

מסמך זה יביא את סיכומי השיעורים מהקורס אימות חומרה תוכנה, שהועבר על ידי פרופ' אלכסנדר רבינוביץ' בסמסטר א' בשנה"ל תשע"ד.

תוכן עניינים

1 מבוא **3**

1.1 אימות על קצה המזלג 3

1.2 מבנה הקורס 4

2 אוטומטים סופיים על מחרוזות אינסופיות **6**

2.1 תזכורת 6

2.2 בעיית הריקנות (Emptyness Problem) 7

2.3 התנהגות אינסופית של אוטומטים סופיים 7

2.4 סוגים נוספים של אוטומטים 10

2.5 ביטויים ω־רגולריים 12

2.6 סגירות של NBA 13

2.7 משפט רמזי 14

2.8 סיכום 14

3 לוגיקה מונדית **15**

3.1 לוגיקה מסדר ראשון 15

3.2 לוגיקה מסדר שני 16

3.3 לוגיקת מחרוזות 16

3.4 הצרנות 16

3.5 לוגיקה של מחרוזות 18

3.6 עוד מבנים 18

3.7 שקילות בין MLO לאוטומט Büchi 19

3.8 גרסת סדר־ראשון של MSO 20

3.9 הקשר לביטויים רגולריים 20

3.10 פער לא־אלמנטרי בתמציתיות בין MLE לאוטומטים 21

3.11 סיכום 22

4 לוגיקת זמן (Temporal Logic) **23**

4.1 הגדרה ללוגיקת זמן בסיסית 23

4.2 לוגיקות זמן שקולות 24

4.3 עוד לוגיקות זמן 24

4.4 דוגמאות להצרנות 25

4.5 משפט Kamp 26

4.5.1 משפט Kamp 26

4.5.1.1 מ-$\mathcal{TL}$ ל-$\mathcal{FOMLO}$ 26
4.5.1.2 משפט Kamp 26
4.5.2 הוכחת משפט Kamp 27
4.5.2.1 על ההוכחה 27
4.5.2.2 נוסחאות $\forall\overrightarrow{\exists}$ 27
4.5.2.3 מנוסחאות $\forall\overrightarrow{\exists}$ לנוסחאות $\mathcal{TL}\left(\mathbf{Until},\mathbf{Since}\right)\vee$ . . . 29
4.5.2.4 הרחבה קנונית 29
4.5.2.5 שקילות בהרחבה הקנונית 29
4.5.2.6 הוכחת משפט Kamp 29
4.6 משפט Stavi 33

פרק 1

מבוא

1.1 אימות על קצה המזלג

ניתן לקרוא לקורס באנגלית Automata Logic & Games. אנחנו נעסוק ב־Validators.

ניתן לחלק את עולם ה־Validators ל־2 תתי עולמות, כפי שמתואר באיור 1.1. בתוכנה, בדרך כלל עובדים עם Testing & Debugging. בחומרה, עושים אימות פורמלי, כי בדרך כלל שגיאות בחומרה עולות הרבה כסף. גם פרוטוקולי תקשורת משתמשים באימות פורמלי.

בשביל אימות פורמלי, אנחנו צריכים שפת אפיון (*Specification Language*) ושפת מימוש (*Implementation Language*), כך שלשתיהן תחביר (*Syntax*) וסמנתיקה (*Semantics*). אנחנו נרצה להגיע למצב שבו "Program meets Specification".

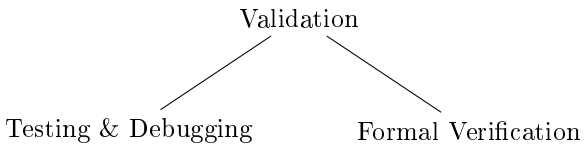
דוגמה 1 (מחלק משותף גדול ביותר (gcd)): תנאי מקדים (Precondition):

$$\{x_1 > 0 \wedge x_2 > 0\}$$

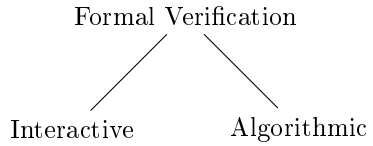
תנאי סיום (Postcondition):

$$\{z \mid x_1 \wedge z \mid x_2 \wedge z > 0 \wedge \forall y \left((y \mid x_1 \wedge y \mid x_2) \rightarrow y \mid z\right)\}$$

למעשה, במקרה זה, מדובר בזוג נוסחאות לוגיות.



איור 1.1: חלוקת עולם ה־Validators



איור 1.2: חלוקת עולם האימות הפורמלי

שפת האפיון מגדירה יחס R בין הקלט לפלט, כך שהיחס מתקיים כאשר גם הפלט וגם הקלט תקינים. שפת המימוש מגדירה פונקציה f, כך ש־$\forall x.\,(x, f\,(x)) \in R$.

אם שפת המימוש (או שפת התיכנות) היא שפה חזקה (כלומר שקולה למכונת טיורינג), אזי אין אלגוריתם לווידוא פורמלי (כי למשל אי אפשר להכריע את בעיית העצירה). כך גם לגבי שפת האפיון.

מסקנה 2: אי אפשר לבדוק בצורה אוטומטית שתוכנית היא נכונה.

גם את עולם האימות הפורמלי ניתן לחלק ל־2, כפי שמתואר באיור 1.2. רוב הקורס יעסוק באימות אלגוריתמי. לכן, לא ניתן לטפל בשפות תכנות עשירות, ולכן נתמקד ב־Finite State Systems כשפת מימוש. נתעניין בהתנהגות אינסופית: Infinite Behavios of Finite State Systems.

להלן בעיות נפוצות שנעסוק בהן:

- בעיית הוידוא (Verification):

  הקלט הוא זוג $Program$ ו־$Spec$. הפלט הוא תשובה לשאלה: $Program$ meets $Spec$?

- בעיית הסינתזה (Synthesis):

  הקלט הוא $Spec$. הפלט הוא תוכנית שמקיימת את האפיון.

- בעיית האפיון:

  הקלט הוא תוכנית. הפלט הוא האפיון המתאים ביותר.

- בעיית הקונסיסטנטיות:

  הקלט הוא אפיון. הפלט הוא תשובה לשאלה: "האם האפיון ניתן למימוש?"

- בעיית ה־Debugging:

  הקלט הוא אפיון ותוכנית. הפלט הוא תוכנית קרובה שמקיימת את האפיון.

1.2 מבנה הקורס

1. אוטומטים סופיים על מחרוזות אינסופיות.
2. לוגיקה מונדית מסדר שני.

3. לוגיקת זמן (Temporal Logic).
4. סינתזה (מאוש קשורה למשחקים עם שני שחקנים).

נתעסק הרבה בשאלות הבאות:

1. כוח הביטוי (Expressive Power): מה אפשר ובטא ומה אי אפשר לבטא.
2. תמציתיות (סוג של קומפקטיות).
3. אלגוריתמים לתרגום בין הפורמליזמים השונים.
4. בעיות הכרעה.

פרק 2

אוטומטים סופיים על מחרוזות אינסופיות

2.1 תזכורת

הגדרה 3 (Labeed Transition System): תהי קבוצת מצבים Q, אלפבית Σ. אזי מעברים בין המצבים לפי האותיות נקראים *Labeled Transition System*. ניתן לאפיין אותם בסופיות, בדטרמיניסטיות ובשלמות (כלומר שמכל מצב יש קשת לכל אות - Complete).

ריצה היא סדרה של מצבים כך שיש מעברים חוקיים ביניהם. מריצה אפשר לקבל מחרוזת של אותיות.

בעבר, הגדרנו גם קבוצה I, שהיא אוסף של מצבים התחלתיים, ו־F, שהיא אוסף של מצבים מקבלים. כך יש ריצות שמתחילות ב־I ומסתיימות ב־F. מכל ריצה כזאת מקבלים מחרוזת, שהאוסף שלהן נותן לנו שפה. אמרנו שאוטומטים הם שקולים אם ורק אם הם מגדירים את אותה השפה.

השפות שמתקבלות על ידי אוטומטים סופיים הן סגורות תחת חיתוך, איחוד, הטלה והשלמה. הוכחנו גם שיש אלגוריתם שמקבל שני אוטומטים $\mathcal{A}_1$ ו־$\mathcal{A}_2$, ומחזיר אוטומט שמקבל את חיתוך השפות של $\mathcal{A}_1$ ו־$\mathcal{A}_2$. גם הראנו את האלגוריתם.

משפט 4: כל אוטומט לא דטרמיניסטי שקול לאוטומט דטרמיניסטי.

באופן לוגי, חיתוך שקול לאופרטור $\wedge$, ואפשר לבנות אוטומט של חיתוך שפות בסיבוכיות כפלית. איחוד שקול לאופרטור $\vee$, ואפשר לבנות אוטומט חיבורי לא־דטרמיניסטי, א כפלי אם שומרים על הדטרמיניסטיות. הטלה אפשר לעשות עם אוטומט לא־דטרמיניסטי חיבורי, והיא שקולה ל־$\exists$. השלמה עושים בקלות עבור אוטומט דטרמיניסטי. אם האוטומט הוא לא־דטרמיניסטי, הסיבוכיות היא אקספוננציאלית.

נוכיח: נגדיר את השפות הבאות מעל $\Sigma = \{0,1\}$:

$$\begin{aligned} E_n &= \{\omega\omega \mid |\omega| = n\} \\ L_n &= \Sigma^{2n} \setminus E_n \end{aligned}$$

איור 2.1 מתאר אוטומט ל־L_n. האוטומט הזה הוא בגודל $\mathcal{O}(n)$, והוא לא דטרמיניסטי. נראה שאין אוטומט דטרמיניסטי קטן עבור L_n. אם $|\omega_1| = n = |\omega_2|$, ו־$\omega_1 \neq \omega_2$, אזי

אסור שהן תגענה לאותו המצב. לכן, באוטומט דטרמיניסטי יש לפחות $\mathcal{O}(2^n)$ מצבים. נסמן ב־$q(\omega)$ את המצב שמתקבל מהפעלת המחרוזת ω. אזי אם $\omega_1 \neq \omega_2$ ו־$|\omega_1| = n = |\omega_2|$, אזי $q(\omega_1) \neq q(\omega_2)$. אחרת, $\omega_1\omega_2$ ו־$\omega_2\omega_1$ גם תתקבלנה.

ראינו למעשה של־L_n יש אוטומט קטן, אבל ל־E_n יש אוטומט גדול. הפעם, נניח שעם המחרוזת ω באורך n מגיעים לקבוצת המצבים S_ω. צריך להראות שאם $\omega_1 \neq \omega_2$ ו־$|\omega_1| = n = |\omega_2|$, אזי $S_{\omega_1} \cap S_{\omega_2} = \emptyset$. ואכן, מ־$S_{\omega_1}$ מגיעים למצב מקבל עם ω_1, ולכן אי אפשר להגיע למצב מקבל מ־S_{ω_2} עם ω_1.

2.2 בעיית הריקנות (Emptyness Problem)

מקבלים כקלט אוטומט $\mathcal{A}$. רוצים לדעת אם $\mathrm{Lang}(\mathcal{A}) = \emptyset$.
אפשר לפתור את הבעיה באמצעות רדוקציה לבעיית ה־Reachability מהמצבים ההתחלתיים למצבים המקבלים. אפשר לפתור את זה עם BFS בזמן לינארי.

אפשר גם לפתור את זה ב־$\mathrm{NSpace}(\log n)$: אם יש n מצבים, אזי כל המחרוזות באורך $\log n$ יכולות להגיע לכל המצבים. אם לא, השפה ריקה. לא יודעים אם אפשר לפתור את הבעיה בצורה דטרמיניסטית – זו בעיה פתוחה

2.3 התנהגות אינסופית של אוטומטים סופיים

עכשיו המסלול שלנו יהיה אינסופי:

$$q_0 a_1 q_2 a_2 \dots q_n a_n \dots$$

כאשר q_i הוא מצב באוטומט ו־a_i היא אות ב־Σ. מהמסלול אפשר לחלץ מחרוזת:

$$a_1 a_2 \dots a_n \dots$$

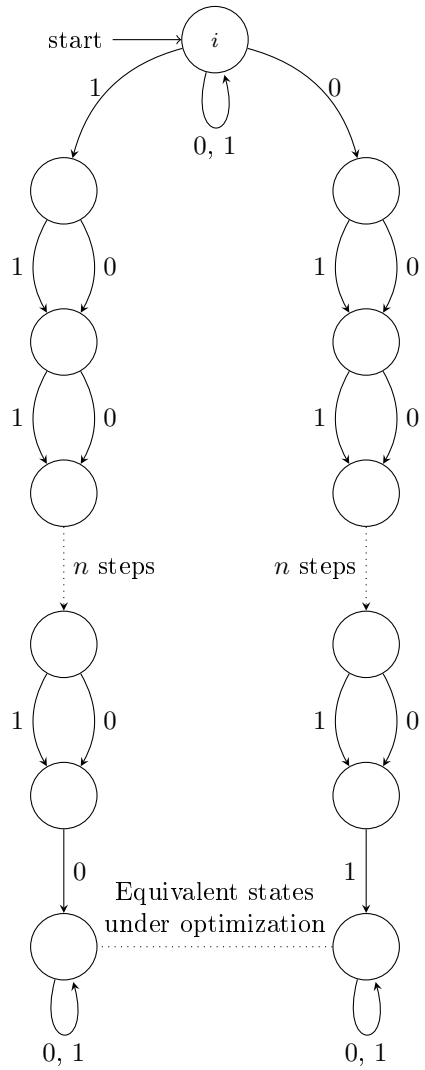
הגדרה 5 (אוטומט של Büchi): מחרוזת מתקבלת (Accepting Run) אם מבקרים במצב מקבל אינסוף פעמים.

הגדרה 6 (אוטומט של Muller): נגדיר עבור הריצה r את $\lim r$ להיות אוסף המצבים שמופיעים אינסוף פעמים ב־r. תנאי הקבלה של Muller מגדיר קבוצות של מצבים, $F_1, \dots, F_k$, כך שהריצה r מקבלת אם $\exists i.\, \lim r = F_i$.

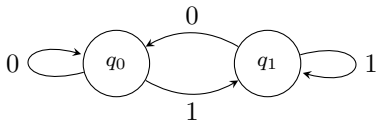
תנאי הקבלה של Büchi מקיים את תכונות הסגירות, אבל אין דטרמיניזציה, כלומר קיימים אוטומטים לא־דטרמיניסטים שאין אוטומטים דטרמיניסטים השקולים להם. Muller מקיים גם הוא את תכונת הסגירות, אבל יש בו דטרמיניזציה. שניהם שקולים למקרה הלא־דטרמיניסטי של Büchi, שניתן לתיאור באמצעות Monadic Logic of Order.
בצורה פורמלית:

הגדרה 7 (אוטומט של Büchi): תנאי הקבלה של Büchi מוגדר על פי התחביר: $F \subseteq Q$, והסמנטיקה: r מתקבלת אם היא מבקרת ב־F אינסוף פעמים.

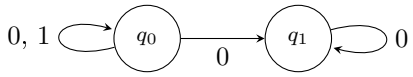
הגדרה 8 (אוטומט של Muller): תחביר: אוסף $F_1, \dots, F_m$ של תת־קבוצות של Q. סמנטיקה: r מתקבלת אם $\exists i.\, (i \in \{1, \dots, m\} \wedge \lim r = F_i)$.



איור 2.1: אוטומט ל-L_n



איור 2.2: אוטומט שמקבל את המחרוזת ω אם יש בה 1 אינסוף פעמים. במקרה של אוטומט Büchi, $F = \{q_1\}$. במקרה של אוטומט Muller, $F_1 = \{q_1\}$, $F_2 = \{q_0, q_1\}$.



איור 2.3: אוטומט לא־דטרמיניסטי שמקבל את המחרוזת ω אם 1 מופיע בה מספר סופי של פעמים. במקרה של אוטומט Büchi, $F = \{q_1\}$. במקרה של אוטומט Muller, $F_1 = \{q_1\}$.

דוגמה 9: איור 2.2 מתאר אוטומט מעל $\{0,1\}$ שמקבל את המחרוזת ω אם יש בה 1 אינסוף פעמים. במקרה של אוטומט Büchi, $F = \{q_1\}$. במקרה של אוטומט Muller, $F_1 = \{q_1\}$, $F_2 = \{q_0, q_1\}$.

דוגמה 10: נבנה אוטומט מעל $\{0,1\}$ שמקבל את ω אם 1 מופיע בה מספר סופי של פעמים. זה קל עבור Muller: האוטומט שבאיור 2.2 הוא טוב, כאשר $F_1 = \{q_0\}$. איור 2.3 מתאר אוטומט Büchi לא־דטרמיניסטי, כאשר $F = \{q_1\}$. אפשר לעשות גם אוטומט Muller לא דטרמיניסטי דומה, שבו $F_1 = \{q_1\}$.

טענה 11: אין אוטומט Büchi דטרמיניסטי שקול לאוטומט שמתואר באיור 2.3.

הוכחה: נניח בשלילה שקיים $\mathcal{A}$ דטרמיניסטי של Büchi שמקבל את השפה (נקרא לה L_0). אזי 0^{n_0} מובילה למצב מקבל. כך גם $0^{n_0}10^{n_1}$ מובילה למצב מקבל. באופן דומה, $0^{n_0}10^{n_1}10^{n_2}$, $0^{n_0}10^{n_1}10^{n_2}10^{n_3}$, וכן הלאה. נגיע למחרוזת $0^{n_0}10^{n_1}1\cdots0^{n_k}1\cdots$. היא מבקרת אינסוף פעמים במצב מקבל, אבל יש בה אינסוף פעמים 1, בסתירה! ■

קל לראות רדוקציה מ־Büchi ל־Muller: בהינתן קבוצת מצבים מקבלת F של Büchi, נבנה קבוצות מקבצים מקבלות של Muller: כל תתי קבוצות המצבים שהחיתוך שלהן עם F לא ריק.
נראה סגירות:

- איחוד: כמו קודם (במקרה שאינו דטרמיניסטי).
- חיתוך: המצבים הם מכפלה קרטזית $Q_1 \times Q_2$. המעברים: $(q_1, q_2) \xrightarrow{a} (q_1', q_2')$ אם $q_1 \xrightarrow{a} q_1'$ וגם $q_2 \xrightarrow{a} q_2'$.

באוטומט Muller, נניח שהמצבים המקבלים ב־$\mathcal{A}_1$ הם $F_1, \ldots, F_n$, וב־$\mathcal{A}_2$ הם $G_1, \ldots, G_m$. אזי המצבים המקבלים בחיתוך הם $S \subseteq Q_1 \times Q_2$, כך ש־$\pi_1(S) = F_i$, $\pi_2(S) = G_j$. נוכיח: נניח ש־r מתקבלת על $\mathcal{A}_1$ ו־$\mathcal{A}_2$. אזי:

$$\begin{aligned} \exists i. \lim_{\mathcal{A}_1} r &= F_i \\ \exists j. \lim_{\mathcal{A}_2} r &= G_j \end{aligned}$$

לכן, r על $\mathcal{A}_1 \wedge \mathcal{A}_2$ מקבלת $\lim_{\mathcal{A}_1 \wedge \mathcal{A}_2} r = S$, ו־$\pi_1(S) = F_i$, $\pi_2(S) = G_j$. נניח כעת ש־S מתקבלת על $\mathcal{A}_1 \wedge \mathcal{A}_2$. אזי לפי ההגדרה זה בסדר.

- הטלה: עושים כמו קודם (בלי לשמור על דטרמיניסטיות).

כדי לדבר על השלמה בלי דטרמיניזציה, נדבר על ביטויים ω־רגולריים. נראה את זה בהמשך

2.4 סוגים נוספים של אוטומטים

סימון נסמן ב־ω את קבוצת המספרים הטבעיים.

הגדרה 12 (אוטומט Büchi מוכלל): תהי $\mathcal{F} \in \mathbf{P}(Q)$. אזי ריצה ρ מתקבלת אם היא מבקרת אינסוף פעמים בכל $F \in \mathcal{F}$.

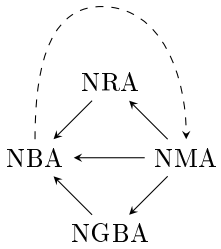
הגדרה 13 (אוטומט של Rabin): תהי קבוצה של זוגות של תתי קבוצות של מצבים: $(F_1, E_1), (F_2, E_2), \ldots, (F_k, E_k)$. אזי הריצה ρ מתקבלת על ידי (F_i, E_i) אם מבקרים אינסוף פעמים ב־F_i ומספר סופי של פעמים ב־E_i. ρ מתקבלת על ידי האוטומט אם היא מקבלת על ידי אחד הזוגות.

סימונים נגדיר קיצורים לסוגים השונים של האוטומטים:

NBA	Non-deterministic Büchi Automaton
NMA	Non-deterministic Muller Automaton
NRA	Non-deterministic Rabin Automaton
NGBA	Non-deterministic Generalized Büchi Automaton
DBA	Deterministic Büchi Automaton
DMA	Deterministic Muller Automaton
DRA	Deterministic Rabin Automaton

אזי NMA יותר חזק מ־NBA, NRA, NGBA (כלומר יש רדוקציה מ־NMA לכל אחד מהם), וכן יש רדוקציה מכולם ל־NBA. ניתן לראות הסבר גרפי באיור 2.4. ראינו רדוקציה מ־NMA ל־NBA בשיעור הקודם. הרדוקציות מ־NMA ל־NRA, מ־NMA ל־NGBA, מ־NRA ל־NBA ומ־NGBA ל־NBA הן טריוויאליות. אם נראה רדוקציה מ־NBA ל־NMA, נסגור מעגל, ונראה שכל האוטומטים שקולים זה לזה.

נרצה להראות תרגום מ־NBA עם קבוצת קבלה אחת F ל־NMA. נבנה את האוטומט שלנו, אבל במקום F יהיו לנו $F \times F$. משמעות המצב $(p, q) \in F \times F$ היא "אנחנו עכשיו ב־p, מחכים לביקור ב־q". המעברים שלנו יהיו $(p, q) \xrightarrow{a} (p', q)$ אם $p \xrightarrow{a} p'$ וגם



איור 2.4: רדוקציות מסוגים שונים של אוטומטים

$p' \neq q$, ו־$(p, q_i) \xrightarrow{a} (p', q_{i+1})$ אם $p \xrightarrow{a} p'$ וגם $p' = q_i$. כדי שנדע שהסיבוב יסתיים, נוסיף מצבי bravo: $(p, q_0) \xrightarrow{a} \left(q_0^{\text{bravo}}, q_1\right)$ אם $p \xrightarrow{a} q_0$. כמו כן, נוסיף את המעברים $\left(q_0^{\text{bravo}}, q_1\right) \xrightarrow{a} (p, q_1)$ אם $q_0 \xrightarrow{a} p$ וגם $p \neq q_1$.
במקרה הדטרמיניסטי:

$$\text{DBA} \subsetneq \text{DMA} \overset{\text{Hard Construction}}{=} \text{NMA} = \text{DRA}$$

הגדרה 14 (שרשור מחרוזות): תהי L_1 שפה של מחרוזות סופיות, ותהי L_2 שפה (של מחרוזות סופיות או אינסופיות). השרשור של L_1 עם L_2 מסומך על ידי $L_1; L_2$, ומוגדר באופן הבא:

$$L_1; L_2 = \{\omega_1\omega_2 \mid \omega_1 \in L_1 \wedge \omega_2 \in L_2\}$$

למה 15: תהי L_1 שפה של מחרוזות סופיות המתקבלת על ידי אוטומט סופי. תהי L_2 שפה של מחרוזות אינסופיות המתקבלת על ידי NBA. אזי השפה $L_1; L_2$ מתקבלת על ידי NBA.

הוכחה: יהי $\mathcal{A}_1$ אוטומט סופי שמקבל את השפה L_1, ויהי $\mathcal{A}_2$ NBA שמקבל את השפה L_2. אזי מכל מצב מקבל של $\mathcal{A}_1$ נשים מעבר למצב התחלתי של $\mathcal{A}_2$, וכך נקבל NBA חדש שמקבל את $L_1; L_2$. ■

הגדרה 16 (שרשור אינסופי): תהי L שפה. נגדיר את השרשור האינסופי של L (מסומן ב־L^ω) באופן הבא: $s \in L^\omega$ אם ניתן לחלק את s ל־$\cdots s_n \cdots s_1 s_2$, כך ש־$s_i \in L$.

למה 17: תהי L שפה של מחרוזות סופיות המתקבלת על ידי אוטומט סופי. אזי L^ω מתקבלת על ידי NBA.

הוכחה: יהי $\mathcal{A}$ אוטומט סופי שמקבל את L במצבים של F. נבנה NBA שמקבל את L^ω: נוסיף מעבר מכל $q \in F$ ל־$p \in Q$ באות a (כלומר $q \xrightarrow{a} p$) אם $p_0 \xrightarrow{a} q$. נקרא ל־NBA בשם $\mathcal{A}_{\text{new}}$.

צ"ל: $L^\omega \subseteq \text{Language}(\mathcal{A}_{\text{new}})$ ו-$\text{Language}(\mathcal{A}_{\text{new}}) \subseteq L^\omega$.
אם יש מחרוזת ב-L^ω, אזי קל לבנות לה ריצה מתאימה ב-$\mathcal{A}_{\text{new}}$, ולכן $L^\omega \subseteq \text{Language}(\mathcal{A}_{\text{new}})$.
אם יש ריצה שנכנסת ל-F אינסוף פעמים ב-$\mathcal{A}_{\text{new}}$, היא יכולה להסתובב אינסוף פעמים בתוך F, אבל לא לעבור באחד המעברים שהוספנו. לכן, כל הבניה אינה נכונה. בנייה נכונה – תרגיל. ■

2.5 ביטויים ω-רגולריים

הגדרה 18 (שרשור סופי של מחרוזות): תהי L שפה. אזי השרשור הסופי של L עם עצמה i פעמים (המסומן ב-L^i) מוגדר באופן הבא: $s \in L^i$ אם ניתן לחלק את s ל-$s_1 s_2 \cdots s_i$ כך ש-$s_j \in L$ לכל $j \in \{1, \ldots, i\}$.

הגדרה 19 (ביטויים רגולריים): מגדירים ביטויים רגולריים מעל האלפבית Σ בצורה אינדוקטיבית:

- a הוא ביטוי רגולרי עבור $a \in \Sigma$.
- $R_1; R_2$ הוא ביטוי רגולרי עבור הביטויים הרגולריים R_1 ו-R_2.
- $R_1 + R_2$ הוא ביטוי רגולרי עבור הביטויים הרגולריים R_1 ו-R_2 (כאשר המשמעות של $+$ היא איחוד שפות).
- R^+ הוא ביטוי רגולרי עבור הביטוי הרגולרי R (כאשר $R^+ = \bigcup_{i=1}^{\omega} R^i$).

משפט 20: שפה חופשית מ-ϵ מתקבלת על ידי אוטומט סופי אם ורק אם היא ניתנת להגדרה כביטוי רגולרי.

הגדרה 21 (ביטוי ω-רגולרי): מגדירים ביטויים ω-רגולריים מעל האלפבית Σ בצורה אינדוקטיבית:

- R^ω הוא ביטוי ω-רגולרי עבור הביטוי הרגולרי R.
- $R; E$ הוא ביטוי ω-רגולרי עבור הביטוי הרגולרי R והביטוי ה-ω-רגולרי E.
- $E_1 + E_2$ הוא ביטוי ω-רגולרי עבור הביטויים ה-ω-רגולריים E_1 ו-E_2 (כאשר המשמעות של $+$ היא איחוד שפות).

משפט 22: ω-שפה מתקבלת על ידי אוטומט סופי (NBA) אם ורק אם היא ניתנת להגדרה כביטוי ω-רגולרי.

הוכחה: נוכיח שכל ω-שפה שמוגדרת על ידי ביטוי ω-רגולרי מתקבלת על ידי NBA, באמצעות אינדוקציה על המבנה:

1. אם L היא שפה (של מחרוזות סופיות) המתקבלת על ידי האוטומט $\mathcal{A}$, אזי L^ω מתקבלת על ידי NBA, לפי למה 17.
2. אם L_1 היא שפה (של מחרוזות סופיות) המתקבלת על ידי אוטומט סופי, ו-L_2 היא ω-שפה (של מחרוזות אינסופיות) המתקבלת על ידי NBA, אזי מלמה 15, $L_1; L_2$ מתקבלת על ידי NBA.
3. אם L_1 ו-L_2 הן ω-שפות המתקבלות על ידי NBA-ים, אזי $L_1 + L_2$ מתקבלת על ידי NBA (מתכונת הסגירות).

נוכיח שאם L מתקבלת על ידי NBA, אזי היא ω-רגולרית: יש לנו בהתחלה מילים מ-q_0 ל-F, ואז הרבה מילים מ-F ל-F. זה יוצר את הביטוי הרגולרי:

$$\text{Language}\left(q_0, F\right); \text{Language}\left(F, F\right)^{\omega}$$

■

2.6 סגירות של NBA

עבור NBA $\mathcal{A}$, נגדיר יחס שקילות $\sim_{\mathcal{A}}$ על מחרוזות סופיות. נאמר ש-$s \sim_{\mathcal{A}} s'$ אם לכל q_1 ו-q_2:

1. יש ריצה מ-q_1 ל-q_2 על s אם ורק אם יש ריצה כזאת ל-s'.
2. יש ריצה מ-q_1 ל-q_2 על s שעוברת דרך F אם ורק אם יש ריצה כזאת ל-s'.

למה 23: מספר מחלקות השקילות מהצורה $\sim_{\mathcal{A}}$ הוא סופי.

הוכחה: אם יש n מצבים ב-NBA, לכל מחרוזת s נתאים:

1. זוגות (q_1, q_2) כך ש-s עוברת מ-q_1 ל-q_2.
2. זוגות (q_1, q_2) כך ש-s עוברת מ-q_1 ל-q_2 דרך F.

צריך ששתי הקבוצות תהיינה זהות לכל זוג מחרוזות שקולות. יש 2^{n^2} קבוצות כאלה, ולכן יש לכל היותר $2 \cdot 2^{n^2}$ מחלקות שקילות. ■

למה 24: כל מחלקת שקילות מתקבלת על ידי אוטומט מצבים סופי.

הוכחה: נגדיר את המצבים ההתחלתיים על ידי S, ואת המצבים המקבלים לפי S^F (כאשר מחלקת השקילות מוגדרת על ידי $\left(S, S^F\right)$ כאשר $S \subseteq \mathbf{P}\left(Q\right)$ ו-$S^F \subseteq \mathbf{P}\left(Q\right)$). ■

למה 25: $\sim_{\mathcal{A}}$ הוא קונגרואנציה ביחס לשרשור. כלומר, אם $s_1 \sim_{\mathcal{A}} s_1'$ ו-$s_2 \sim_{\mathcal{A}} s_2'$ אזי $s_1 s_2 \sim_{\mathcal{A}} s_1' s_2'$.

הוכחה: ניעזר באוטומט שמתואר באיור 2.5. ■

למה 26: אם $s_i \sim_{\mathcal{A}} s_i'$ עבור $i \in \mathbb{N}$, אזי $s_1 s_2 \cdots s_n \cdots$ מתקבלת על ידי $\mathcal{A}$ אם ורק אם $s_1' s_2' \cdots s_n' \cdots$ מתקבלת על ידי $\mathcal{A}$.

הוכחה: קל לראות. ■

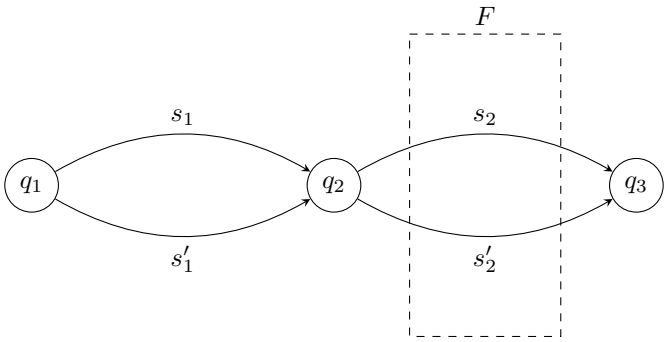
מסקנה 27: אם R_1 ו-R_2 הן מחלקות שקילות של $\sim_{\mathcal{A}}$, אזי $R_1 R_2^{\omega} \subseteq \omega\text{-}Language\left(\mathcal{A}\right)$ או $R_1 R_2^{\omega} \cap \omega\text{-}Language\left(\mathcal{A}\right) = \emptyset$.

למה 28: לכל ω-מחרוזת s, יש מחלקות שקילות R_1 ו-R_2 של $\sim_{\mathcal{A}}$ כך ש-$s \in R_1 R_2^{\omega}$.

הוכחה: שימוש במשפט רמזי. ■

משפט 29: אם ω-מחרוזת מתקבלת על ידי NBA, אזי המשלים שלה מתקבל על ידי NBA.

הוכחה: לפי כל הלמות לעיל, יש קבוצה סופית של זוגות $\left\langle R_1^i, R_2^i \right\rangle$ של מחלקות שקילות של $\sim_{\mathcal{A}}$, כך שהמשלים של $\omega\text{-Language}\left(\mathcal{A}\right)$ הוא $\bigcup_i R_1^i \left(R_2^i\right)^{\omega}$. ■



איור 2.5: אוטומט שמראה כי $\sim_{\mathcal{A}}$ הוא קונגרואנציה ביחס לשרשור

2.7 משפט רמזי

הגדרה 30 (צביעה): תהי C קבוצה סופית (של צבעים). צביעה של $\mathbb{N}$ היא פונקציה col מהזוגות הסדורים $\{\langle i,j\rangle \mid i,j \in \mathbb{N}\}$ ל־C.
תת־קבוצה $H \subseteq \mathbb{N}$ היא הומוגנית ל־col אם יש $c \in C$ כך ש־$col\,(h_1,h_2) = c$ לכל $h_1,h_2 \in H$ כך ש־$h_1 < h_2$.

משפט 31 (רמזי – Ramsey): לכל צביעה col של $\mathbb{N}$ יש קבוצה הומוגנית אינסופית.

נוכיח כעת את למה 28:

הוכחה: תהי s ω־מחרוזת. נגדיר צביעה $col_s\,(i,j)$ יהיה מספר מחלקות השקילות של $\sim_{\mathcal{A}}$ על תת המחרוזת של s במקומות $[i,j)$.
לפי משפט רמזי, קיימת קבוצה הומוגנית אינסופית, $H = \{h_0 < h_1 < \cdots\}$ בצבע R_2.
נגדיר את R_1 להיות מחלקת השקילות של $s\,[0,h_0)$. ■

2.8 סיכום

משפט 32: ω־שפה מתקבלת על ידי NBA אם ורק אם היא ניתנת להגדרה על ידי ביטוי ω־רגולרי אם ורק אם היא ניתנת להגדרה באמצעות MLO[1]. כמו כן, יש תרגומים רקורסיביים בין כל אחת מההצגות.

[1] את זה נראה בפרק הבא.

פרק 3

לוגיקה מונדית

עד עכשיו דיברנו על אוטומטים וביטויים. עכשיו נדבר על לוגיקה. הלוגיקה העיקרית שנעסוק בה נקראת Monadic Logic of Order. נסביר: Monadic – חד־מקומית, Order – סדר.

3.1 לוגיקה מסדר ראשון

ניזכר מהי לוגיקה מסדר ראשון. כל לוגיקה מגדירה תחביר וסמנטיקה.

1. תחביר:
   (א) מילון (פרדיקטים).
   (ב) נוסחאות אטומיות.
   (ג) סימני יחס: למשל $R(x_1, \ldots, x_n)$, כאשר R הוא סימן יחס n־מקומי ו־$x_1, \ldots, x_n$ הם משתנים.
   (ד) סימני פונקציה.
   (ה) בונים נוסחאות חדשות מנוסחאות קיימות באמצעות הקשרים הבולאנים $\wedge$, $\vee$, $\rightarrow$, $\neg$, והכמתים $\forall x$, $\exists x$.
2. סמנטיקה:
   (א) מבנה M.
   (ב) תחום D.

   הסמנטיקה נותנת פירושיםעבור סימני יחס וסימני פונקציה.

הגדרה 33 (השמה): לכל משתנה מתאימים איבר בתחום D. המבנה מסומך ב־M, והסביבה ב־ρ. ההשמה מגדירה את הערך של הנוסחה במבנה ובסביבה.

3.2 לוגיקה מסדר שני

מבחינה תחבירית, יש לנו 2 סוגים של משתנים: התחביר כולל מילון, משתנים מסדר ראשון ומשתנים מסדר שני. נוסחאות אטומיות יראו כמו קודם, או $y(x_1,\ldots,x_k)$, כאשר y היא משתנה מסדר שני k־מקומי. הנוסחאות מכילות כמתים מסדר ראשון וכמתים מסדר שני.

בסמנטיקה, הסביבה מתאימה לכל משתנה מסדר ראשון איבר בתחום, ולכל משתנה מסדר שני היא מתאימה יחס בתחום.

נגדיר לוגיקה מונדית מסדר שני: המשתנים מסדר שני הם רק חד־מקומיים. לכן, נוסחאות אטומיות הן רק מהצורה $R(x_1,\ldots,x_k)$ או $y(x)$. נגדיר לוגיקה מונדית מסדר שני של סדר (Monadic Second-Order Logic of Order): המילון מכיל את יחס הסדר $<$, וכן יחסים חד־מקומיים.

3.3 לוגיקת מחרוזות

נתאים למחרוזת $abaab$ מבנה: יהיו בו 5 איברים: 1, 2, 3, 4 ו־5. המילון: $<$ – יחס סדר, P_a – מקומות המסומנים ב־a ($\{1,3,4\}$), P_b – מקומות המסומנים ב־b ($\{2,5\}$).

למחרוזת $ababcac$ נתאים תחום עם 7 איברים, ומילון עם $<$, P_a, P_b ו־P_c. אפשר גם אחרת: אם נכתוב את a באמצעות $\binom{0}{0}$, b באמצעות $\binom{0}{1}$ ו־c באמצעות $\binom{1}{1}$, נוכל לקודד את המילון בעזרת 2 פרדיקטים בלבד: P_0 שיכיל את $\{1,2,3,4,6\}$, ואת P_1 שיכיל את $\{2,4,5,7\}$.

אפשר גם לעשות את הפעולה ההפוכה: בהינתן מבנה ופרדיקטים, ניתן להתאים להם מחרוזת.

3.4 הצרנות

נכתוב פסוק שנכון על מחרוזת סופית מעל $\{a,b,c\}$ אם האות הראשונה של המחרוזת היא a: "האיבר הכי קטן ב־P_a". איך נעשה את זה? נחלק למשפטים יותר קטנים: "x הכי קטן" יוצרן באופן הבא:

$$\varphi(x) \equiv \forall y.\,(y = x \vee x < y)$$

כעת, נרצה לומר שהאיבר הכי קטן ב־P_a. נעשה את זה כך:

$$\exists x.\,(P_a(x) \wedge \forall y.\,(y = x \vee x < y))$$

ההצרנה היא בלוגיקה מסדר ראשון.

עוד דוגמה: יש מופע של a: $\exists x.P_a(x)$. יש 3 מופעים שונים של a:

$$\exists x.\exists y.\exists z.\,(P_a(x) \wedge P_a(y) \wedge P_a(z) \wedge (x < y < z) \wedge \forall w.P_a(w) \to (w = x \vee w = y \vee w = z))$$

אפשר להצרין את "y הוא העוקב של x":

$$Suc(x,y) \equiv x < y \wedge \neg\exists z.\,(x < z \wedge z < y)$$

ואז נצרין את "יש מופע של ab":

$$\exists x.\exists y.Suc(x,y) \wedge P_a(x) \wedge P_b(y)$$

עוד הצרנה: a מופיע בדיוק במקומות אי־זוגיים. זה שקול לזוג האמירות הבאות:

1. a מופיע במקום הראשון.
2. לכל זוג אותיות, בדיוק אחת מהן היא a.

מכאן, מאוד קל להצרין את הטענה המקורית.
נצרין את הטענה הבאה: "a מופיע בכל המקומות האי־זוגיים". כאן אנחנו זקוקים ללוגיקה מסדר שני. נגדיר את $Odd(y)$ – נוסחה המתארת מקומות אי־זוגיים, כאשר y הוא משתנה מסדר שני. נגדיר את זה כך:

1. האיבר הראשון נמצא ב־y.
2. עבור כל זוג איברים עוקבים, בדיוק אחד מהם ב־y, והשני לא ב־y.

נעשה זאת כך:

$$\begin{aligned} Odd(y) \quad \equiv \quad & (\exists x.\,(y(x) \wedge \forall z.\,(z = x \vee x < z))) \wedge \\ & (\forall u.\forall v.\,(u < v \wedge \neg\exists z.\,(u < z \wedge z < v) \rightarrow (y(u) \leftrightarrow \neq y(v)))) \end{aligned}$$

לכן, ההצרנה של הטענה "a מופיע בכל המקומות האי־זוגיים" תהיה:

$$\forall y.\,(Odd(y) \rightarrow \forall x.\,(y(x) \rightarrow P_a(x)))$$

אפשר גם כך:

$$\exists y.\,(Odd(y) \wedge \forall x.\,(y(x) \rightarrow P_a(x)))$$

נשים לב שאי אפשר להצרין את הטענה הזאת בלוגיקה מסדר ראשון.

הגדרה 34 (גדירות – Definability): במבנה או במחלקה של מבנה. ראינו פסוק שמגדיר אוסף של מבנים. לכל פסוק מתאימים אוסף של מחרוזות, ואז אומרים שהשפה גדירה על ידי פסוק.

הגדרה 35 (פסוק): נוסחה ללא משתנים חופשיים היא פסוק.

תזכורת בלוגיקה מסדר ראשון לא ניתן לכתוב ביטוי שאומר שהגרף $G = (V, E)$ הוא קשיר.

טענה 36: קשירות של גרף ניתנת לביטוי בלוגיקה מודנית מסדר שני.

הוכחה: נראה פסוק ψ כך ש־ψ נכון ב־G אם ורק אם G קשיר. איך נבטא שאוסף של צמתים Y הוא נגיש מהצומת x? נסמן את הביטוי ב־$Reach(x, Y)$.
בעזרת $Reach$ ניתן לבטא קשירות:

$$\forall x \forall u.\exists Y.\,(Reach(x, Y) \wedge u \in Y)$$

ננסה לנסח את $Reach(x, Y)$: Y היא קבוצה מינימלית שמכילה את x וסגורה תחת שכנות. למה מינימלית? אחרת אפשר היה לקחת את קבוצת כל הצמתים, אבל הם לא בהכרח נגישים מ־x. נגדיר את $Reach(x, Y)$:

$$(x \in Y \wedge (\forall u.\forall v.\,(((u, v) \in E \wedge u \in Y) \rightarrow v \in Y) \wedge (\forall Z.\,(x \in Z \wedge (\forall u.\forall v.\,((u \in Z \wedge (u, v) \in E) \rightarrow v \in Z))))))$$

■

3.5 לוגיקה של מחרוזות

כפי שראינו, נתאים מבנה עבור המחרוזת $abcaab$ מעל $\Sigma = \{a, b, c\}$. נשתמש במילון $<, P_a, P_b, P_c$. התחום שלנו מכיל 6 איברים. המקומות המסומנים ב־P_a הם $\{1, 4, 5\}$. המקומות המסומנים ב־P_b הם $\{2, 6\}$. המקומות המסומנים ב־P_c הם $\{3\}$.

בלוגיקה מסדר שני, התחום שלנו יהיה אותו התחום. המילון יהיה Q_1, Q_2, ונתרגם את a להיות $\binom{0}{0}$, את b להיות $\binom{0}{1}$ ואת c להיות $\binom{1}{0}$. ואז Q_1 יהיה רק המקומות שמכילים את a, ו־Q_2 יהיה המקומות שמכילים את b.

נניח ש־φ פסוק במילון $\{<, P_a, P_b, P_c\}$. אזי φ מגדיר אוסף של מחרוזות. אזי קיים פסוק ψ במילון $\{Q_1, Q_2\}$ שמגדיר בדיוק את אותו האוסף של מחרוזות. קיים גם אלגוריתם שמבצע את ההמרה בין הקידודים: מחליפים את $P_a(x)$ ל־$\neg Q_1(x) \wedge \neg Q_2(x)$, את $P_b(x)$ ל־$Q_2(x)$, ואת $P_c(x)$ ל־$Q_1(x)$. בכיוון השני: $Q_1(x)$ יהפוך ל־$\neg P_a(x) \wedge \neg P_b(x) \wedge \neg P_c(x)$.

כוח הביטוי לא שקול בין שני הקידודים. למשל, הפסוק $\exists y. Q_1(y) \wedge Q_2(y)$ ספיק, אבל לא מעל $\Sigma = \{a, b, c\}$. לכן, צריך לחדד את הטענה שלנו.

3.6 עוד מבנים

נגדיר כמה מבנים חדשים:

הגדרה 37 (שרשרת): שרשרת ($Chain$) מוגדרת על ידי $\mathcal{C} = (\mathcal{A}, <, P_1, \ldots, P_m)$, כאשר $<$ הוא יחס סדר לינארי ו־P_i הם פרדיקטים מונדיים (חד־מקומיים).

הגדרה 38 (עץ בינארי מלא): עץ בינארי מלא ($Full\ Binary\ Tree$) מסומן ב־T_2, ומוגדר על ידי החתימה $\{<, Right, Left\}$, כאשר $Right$ ו־$Left$ הם פרדיקטים מונדיים.

נשתמש גם במבנים הבאים כדי לוודא פסוקים:

1. ω־מחרוזת.
2. שרשראות.
3. T_2.

תזכורת בקורס לוגיקה למדנו שאי אפשר לבטא בלוגיקה מסדר ראשון שסדר לינארי הוא סופי. נצרין את הטענה הזאת בלוגיקה מסדר שני.

נצרין תחילה את הטענה עבור ω־מחרוזות: לכל איבר יש איבר a יותר גדול ממנו:

$$\forall u. \exists v. (u < v \wedge P_a(v))$$

נצרין כעת את הטענה עבור שרשראות. הנוסחה שלהלן לא בהכרח עובדת, כי למשל אם נגדיר ש־$P_a = [m, n]$, אזי יש אינסוף איברים ש־P_a מופיע בהם (למשל על הממשיים), אבל יש לקבוצה הזאת מקסימום. הטריק יהיה כדלקמן: או שיש לנו תת־סדרה עולה ממש של P_a, או שיש לנו תת־סדרה יורדת ממש. כלומר, יש Y, תת־קבוצה של P_a, שהיא לא חסומה מלמעלה, או לא חסומה מלמטה. נצרין:

$$\exists Y. \left(\underbrace{Y \subseteq P_a}_{\star} \wedge [(\forall u. (Y(u) \to \exists v. (v < u \wedge Y(v)))) \vee (\forall u. (Y(u) \to \exists v. (u < v \wedge Y(v))))] \right)$$

כמובן שאת $\star$ קל להצרין בצורה פורמלית.

נצרין כעת את הטענה ל־T_2: נשתמש במשפט הבא: "P_a אינסופית אם ורק אם יש מסלול שמכיל אינסוף צמתים של P_a". המסלול מגדיר לנו יחס סדר, והוא צריך להיות אינסופי. אפשר עכשיו לדרוש כמו במקרה הקודם.

כשמדברים על ω־מחרוזות, לפעמים מסתכלים על S1S: Second order logic of One-Successor, כאשר ההגדרה הפורמלית היא:

$$\begin{aligned} \text{S1S} &= \text{MLO}\,(Succ) \\ \text{MLO} &= \text{MSO}\,(<) \end{aligned}$$

אפשר לבטא את $Succ\,(x,y)$ באמצעות הנוסחה:

$$x < y \wedge \forall z.\,((x \neq z \wedge y \neq z) \rightarrow (z < x \vee y < z))$$

איך נבטא את $<$ באמצעות $Succ$? כל קבוצה Y שמכילה את x וסגורה תחת $Succ$, גם מכילה את y.

כשמדברים על עצים, אפשר לדבר על S2S: Second order logic of Two-Successors.

3.7 שקילות בין MLO לאוטומט Büchi

משפט 39: לכל אוטומט $Büchi$ $\mathcal{A}$ יש נוסחת MLO $\varphi_{\mathcal{A}}$ כך שלכל ω־מחרוזת s, מתקיים $s \models \varphi_{\mathcal{A}}$ אם ורק אם $\mathcal{A}$ מקבל את s.

הוכחה: נסתכל על האלפבית הבא: $\Sigma \times Q$. אזי נסמן: $Q = \{q_0, \ldots, q_n\}$, $\Sigma = \{a_1, \ldots, a_n\}$. נגדיר את הפרדיקטים $X_{q_0}, \ldots, X_{q_n}$ ו־$P_{a_1}, \ldots, P_{a_m}$.

נצטרך להגדיר נוסחה $Run_{\mathcal{A}}$ שתספק את:

1. כל איבר שייך בדיוק ל־X_{q_i} בודד.
2. האיבר המינימלי נמצא ב־X_{q_0}.
3. המעברים הם לפי טבלת המעברים של $\mathcal{A}$. למשל, אם u נמצאים במצב q_i ורואים את a_j, נצריך ונקבל:

$$\forall u.\,\left(X_{q_i}\,(u) \wedge P_{a_j}\,(u)\right) \rightarrow (\exists v.Succ\,(u,v) \wedge X_{q_\ell}\,(v))$$

את זה עושים לכל q_i ולכל a_j, כאשר המעבר הוא $q_i \xrightarrow{a_j} q_\ell$.

4. נמצאים במצב של F אינסוף פעמים.

סיבוכיות התרגום היא לינארית. ■

משפט 40: לכל נוסחת MLO $\varphi\,(X_1, \ldots, X_n)$ יש אוטומט $Büchi$ $\mathcal{A}_\varphi$ מעל האלפבית $\mathbb{B}^n$, כך שלכל $(P_1, \ldots, P_n) \in (\mathbb{B}^\omega)^n$ מתקיים $\left(\mathbb{N}, <, \overline{P}\right) \models \varphi\left(\overline{X}\right)$ אם ורק אם $\mathcal{A}_\varphi$ מקבלת את ה־ω־מחרוזת $(P_1, \ldots, P_n)$.

הוכחה: נבנה לפי אינדוקציה מבנית על מבנה הנוסחה.
סיבוכיות התרגום היא פונקציה שאינה אלמנטרית. ■

הגדרה 41 (פונקציה אלמנטרית): נגדיר את הפונקציה $Tower(i,x)$: הפעלה i פעמים של הפונקציה המעריכית, כאשר:

$$Tower(i,x)=\begin{cases}2^x & i=1\\ 2^{Tower(i-1,x)} & \text{otherwise}\end{cases}$$

נאמר על פונקציה f שהיא אלמנטרית אם קיים k כך שבאופן אסימפטוטי: $f(x) < Tower(x,k)$.

משפט 42: אין תרגום בסיבוכיות אלמנטרית מנוסחת MLO לאוטומט $Büchi$ מעל ω־מחרוזות.

3.8 גרסת סדר־ראשון של MSO

הגדרה 43 (גרסת סדר־ראשון של MSO): נגדיר את גרסת הסדר הראשון של MSO (*First-Order version of MSO*): תהי לוגיקה מונדית מסדר שני מעל החתימה Δ. יהי $\mathcal{A}$ מבנה של Δ.
מבנה קבוצת החזרה של $\mathcal{A}$ – $\mathbf{P}(\mathcal{A})$ הוא מבנה עבור $\Delta\cup\{\subseteq\}$. האיברים של $\mathbf{P}(\mathcal{A})$ הם תתי־הקבוצות של $\mathcal{A}$. הפירוש של סימני היחס:

1. $\subseteq$: יחס הכלה של קבוצות.
2. $R^{\mathbf{P}(\mathcal{A})}(A_1,A_2)$ אם $A_i=\{a_i\}$ ו־$R^{\mathcal{A}}(a_1,a_2)$.

באופן דומה, מגדירים גם סימני יחס n־מקומיים.

משפט 44: השפה המונדית מסדר שני מעל $\mathcal{A}$ שקולה לגרסת הסדר־הראשון שלה מעל $\mathbf{P}(\mathcal{A})$.

3.9 הקשר לביטויים רגולריים

נבצעתרגום מביטויים רגולריים (של מחרוזות) ל־MLO. עבור כל ביטוי E נרצה לבנות פסוק φ_E שמקבל בדיוק את אותן המחרוזות (כלומר שניהם מגדירים את אותה השפה).
בשביל הנוחות, נבנה את $\varphi_E(t_0,t_1)$, כך שעבור כל מחרוזת s, נפרש את t_0,t_1 כ־$i<j$ ב־s. נרצה ש־$s[i,j]$ יהיה ב־E אם ורק אם $s_{i,j}\models\varphi_E(t_0,t_1)$.
נראה באינדוקציה:

בסיס צריך להראות שאם $t_0=t_1$, אזי P_a.

מעברים עבור E_1+E_2, עם האופרטור $\vee$. עבור $E_1;E_2$ – גם קל. עבור E^+: קיימת קבוצה Y (של נקודות חלוקה), כך שעבור כל זוג איברים עוקבים ב־Y, המחרוזת בין האיברים האלה נמצאת ב־E.

3.10 פער לא־אלמנטרי בתמציתיות בין MLE לאוטומטים

הגדרה 45 (מונה - Counter): לכל n, נגדיר קבוצה של מחרוזות שלהן נקרא מוניס ברמה n. המונים ברמה n הם מחרוזות מעל האלפבית $\{0_1, 1_1, 0_2, 1_2, \ldots, 0_n, 1_n\}$, והם יכולים "למנות" עד $Tower(n,1)-1$.

המונים ברמה 1 הם 0_1 ו־1_1, והערכים שלהם הם 0 ו־1, בהתאמה. המונים ברמה 2 הם ארבע מחרוזות מהצורה $1_1 a 0_1 b$ כאשר $a, b \in \{0_2, 1_2\}$. הערכים הם:

$$Val(1_1 a 0_1 b) = 2 \cdot a + b$$

מונים ברמה $n+1$ הם מהצורה $s_1 a_1 s_2 a_2 \ldots s_k a_k$, כאשר $s_1, \ldots, s_k$ היא רשימה של כל המונים ברמה n בסדר יורד, ו־$a_i \in \{0_{n+1}, 1_{n+1}\}$. הערך של מונה ברמה $n+1$ מוגדר בצואה הבאה:

$$Val(s_1 a_1 s_2 a_2 \ldots s_k a_k) = 2^{k-1} \cdot a_1 + 2^{k-2} \cdot a_2 + \ldots 2^0 \cdot a_k$$

למה 46: יש נוסחה $Count_n(t_1, t_2)$ כך שלכל מחרוזת u ו־$i, j \in \mathbb{N}$, $i \leq j$, $u \models$ $Count_n(i,j)$ אם ורק אם תת־המחרוזת של u במקומות $[i,j]$ היא מונה ברמה n.
כמו כן, הגודל של $Count_n$ הוא אקספוננציאלי ב־n.

הוכחה: נניח ש־$v = u[t_1, t_2]$. אזי הנוסחה $Count_n(t_1, t_2)$ אומרת את הדברים הבאים:

1. v מתחילה במונה המקסימלי ברמה n.

   לשם כך, נגדיר את $Max_n(t,t')$: המונה המקסימלי ברמה n. הוא מוגדר על ידי $Count_n(t,t')$, ואין מופע של 0_n.

2. v מסתיימת באות ב־$\{0_{n+1}, 1_{n+1}\}$, ולפניה יש מונה מינימלי ברמה n.

   לשם כך, נגדיר את $Min_n(t,t')$: המונה המינימלי ברמה n. הוא מוגדר על ידי $Count_n(t,t')$, ואין מופע של 1_n.

3. אם ב־t יש אות ב־$\{0_{n+1}, 1_{n+1}\}$, אזי מייד לפני t יש מונה v ברמה n, ומייד אחרי t יש מונה v' ברמה n, והערך של v הוא הערך של $v'+1$.

   לשם כך, נגדיר את $Next_n(t,t',h,h')$: הערך של המונה ברמה n ב־$[t,t']$ הוא העוקב של הערך של המונה ברמה n ב־$[h,h']$.

כמו כן, נגדיר גם את הנוסחה הבאה: $Same_n(t,t',h,h')$: הערך של המונה ברמה n על $[t,t']$ הוא אותו הערך כמו של המונה ברמה n על $[h,h']$.
יהי ℓ_n האורך המקסימלי של $Count_n$, Max_n, Min_n, $Next_n$, $Same_n$. קל לראות ש־$\ell_n < 10 \cdot \ell_{n-1}$. לכן, $\ell_n < 10^n \cdot \ell_0$. ■

מסקנה 47: יש פער לא אלמנטרי בתמציתיות בין MLO לאוטומטים.

הגדרה 48 (ביטוי רגולרי מורחב (Extenden Regular Expression)): מגדירים ביטוי רגולרי מורחב (*Extended Regular Expression*), או בקיצור ERE, כביטוי רגולרי, התומך בנוסף בפעולת ההשלמה: $\neg ERE$.

לביטויים רגולריים מורחבים יש את אותו כוח הביטוי כמו לביטויים רגולריים רגילים.

הגדרה 49 (ביטוי רגולרי מורחב ללא כוכב (Extended Star Free Regular Expression)): מגדירים ביטוי רגולרי מורחב ללא כוכב (*Extended Star Free Regular Expression*), או בקיצר SF, כביטוי רגולרי מורחב, אך ללא פעולת הכוכב (*). כלומר:

$$SF = a \mid SF; SF \mid SF + SF \mid \neg SF$$

משפט 50: יש פער לא־אלמנטרי בתמציתיות בין ביטויים רגולריים מורחבים ללא כוכב לבין אוטומטים.

3.11 סיכום

לכל אוטומט $\mathcal{A}$ בנינו נוסחה שמגדירה את אותה ω־שפה.

נניח ש־φ ספיקה על ω־מחרוזת. אזי היא ספיקה גם על מחרוזת פריודית מהצורה uv^ω. נוכיח את זה בעזרת העובדה ש־φ שקולה לאוטומט, והאוטומט מקבל מחרוזת מחזורית.

פרק 4

לוגיקת זמן (Temporal Logic)

4.1 הגדרה ללוגיקת זמן בסיסית

נגדיר לוגיקת זמן בסיסית:

- התחביר:
  - המשתנים: $p_1, p_2, \ldots$.
  - הקשרים (Modalities):
    - $\Diamond$ – Eventually, כלומר בסופו של דבר. לפעמים מסומן גם ב־**F**.
    - $\Box$ – Always, כלומר תמיד. לפעמים מסומך גם ב־**G**.
  - הנוסחאות הן מהצורות הבאות:
    - p_i.
    - $\neg F$.
    - $F_1 \wedge F_2$.
    - $F_1 \vee F_2$.
    - $F_1 \rightarrow F_2$.
    - $\Diamond F$.
    - $\Box F$.
- הסמנטיקה:
  - המבנה $M = (T, <, I)$, כאשר T הוא זמן, $<$ הוא יחס סדר (על הזמן), $I : At \rightarrow \mathbf{P}(t)$ הוא הפירוש של האטומים בזמן.
  - הספיקות:
    - $M, t \models p$ אם ורק אם $t \in I(p)$.
    - $M, t \models \neg F$ אם ורק אם $M, t \not\models F$.
    - $M, t \models F_1 \wedge F_2$ אם ורק אם $M, t \models F_1$ וגם $M, t \models F_2$.
    - $M, t \models F_1 \vee F_2$ אם ורק אם $M, t \models F_1$ או $M, t \models F_2$.

* $M,t \models F_1 \to F_2$ גורר ש־$M,t \models F_1$ אם ורק אם $M,t \models F_2$.
* $M,t \models \Diamond F$ אם ורק אם קיים $t' > t$ ב־M כך ש־$M,t' \models F$.
* $M,t \models \Box F$ אם ורק אם לכל $t' > t$ ב־M מתקיים $M,t' \models F$.

הלוגיקה הזאת מסומנת ב־$\mathcal{TL}(\Diamond,\Box)$.

4.2 לוגיקות זמן שקולות

נגדיר בצורה במנטית את הקשר $\Box_{ns}$: $M,t \models \Box_{ns} F$ אם ורק אם לכל $t' \geq t$ מתקיים $M,t' \models F$. נסמן את הלוגיקה הזאת ב־$\mathcal{TL}(\Diamond,\Box,\Box_{ns})$.

שאלה האם $\mathcal{TL}(\Diamond,\Box) = \mathcal{TL}(\Diamond,\Box,\Box_{ns})$?

תשובה כן, כי $\Box_{ns} F$ יהפוך ל־$F \wedge \Box F$.

שאלה האם $\mathcal{TL}(\Diamond,\Box) = \mathcal{TL}(\Diamond,\Box_{ns})$?

תשובה אין לנו דרך לבטא אם $\Box_{ns} F$ באמצעות $\Box$ ו־$\Diamond$ בלבד, ולכן התשובה היא לא.

שאלה האם $\mathcal{TL}(\Diamond) = \mathcal{TL}(\Diamond,\Box,\Box_{ns})$?

תשובה כן, כי $\Box F$ שקול ל־$\neg \Diamond \neg F$, וראינו כבר שאפשר לבטא את $\Box_{ns} F$ באמצעות $\Diamond$ ו־$\Box$.

4.3 עוד לוגיקות זמן

נגדיר קשר חדש: $\bigcirc$ (Next). אם מדברים על זמן דיסקרטי, אזי $M,t \models \bigcirc F$ אם ורק אם יש רגע עוקב ל־t (נקרא לו t') כך ש־$M,t' \models F$. לפעמים מסמנים את $\bigcirc\varphi$ גם ב־$\mathbf{X}\varphi$.
נשים לב: $\Box F$ שקול ל־$F \wedge \bigcirc\Box_{ns} F$.
חסר לנו קשר שאומר "עד ש" (Until). לכן, נגדיר אותו באופן הבא: $M,t_0 \models F\,\mathbf{Until}\,G$ אם ורק אם קיים $t_1 > t_0$ כך ש־$M,t_1 \models G$ וגם לכל $t \in (t_0,t_1)$ מתקיים $M,t \models F$.
אי אפשר לבטא את **Until** בעזרת $\bigcirc$, $\Box$, $\Diamond$, אבל ההיפך לא נכון:

$$\begin{aligned} \Diamond\varphi &\equiv true\,\mathbf{Until}\,\varphi \\ \bigcirc\varphi &\equiv false\,\mathbf{Until}\,\varphi \\ \Box\varphi &\equiv \neg(\Diamond\neg\varphi) \end{aligned}$$

עד עכשיו הסתכלנו על לוגיקת זמן עתידית. אפשר גם להגדיר לוגיקת זמן עבר, באמצעות הקשרים **Since**, $\overleftarrow{\Box}$, $\overleftarrow{\Diamond}$ ו־$\overleftarrow{\bigcirc}$.
אפשר להגדיר גם $\mathbf{Until}^{ns}$ שמדבר על אינטרוול סגור. מגדירים זאת כך:

$$\varphi\,\mathbf{Until}^{ns}\,\psi \equiv \varphi \wedge (\varphi\,\mathbf{Until}\,\psi)$$

4.4 דוגמאות להצרנות

נניח שאנחנו מתכננים מפרט למעלית. נרצה שהמעלית שלנו תקיים את התכונות הבאות:

1. דלת בקומה כלשהי לא נפתחת אם תא המעלית לא נמצא באותה הקומה.
2. אורות החיווי משקפות את המצב של הבקשות הנוכחיות.

נניח שבבניין יש 10 קומות. לכן, לכל $i \in \{1,2,3,4,5,6,7,8,9,10\}$, הפרדיקטים שלנו יהיו:

- $OpenDoor_i$: הדלת של קומה i פתוחה.
- At_i: המעלית נמצאת בקומה i.
- $Call_i$: המעלית נקראה מקומה i.
- $CallLight_i$: נורית החיווי בקומה i דלוקה.

נצרין את 1:

$$AL\left(OpenDoor_i \rightarrow At_i\right)$$

כאשר $AL\left(F\right) = \overleftarrow{\Box} F \wedge F \wedge \Box F$ (Always).
נצרין את 2: נוסיף את הפרדיקט $Service_i$, שמוגדר על ידי:

$$Service_i \equiv At_i \wedge OpenDoor_i$$

אזי ההצרנה של 2 תהיה:

$$AL\left(\left(Call_i \rightarrow CallLight_i\right) \textbf{ Until } Service_i\right)$$

נראה עוד דוגמה: P_1 נכון תמיד החל מנקודה כלשהי בעתיד (Infinitely Often). מעל $\mathbb{N}$: $\Box \diamond P_1$. מעל $\mathbb{R}$: יכול להיות ש־P_1 לא חסום, ואז $\Box \diamond P_1$ מתקיים. מצד שני, יכול להיות שיש t בעתיד כך ש:

$$t = \sup\left\{t' \mid t' < t \wedge P_1\left(t'\right)\right\}$$

או:

$$t = \inf\left\{t' \mid t' > t \wedge P_1\left(t'\right)\right\}$$

נגדיר את ה־Modelities הבאים:

- $\mathbf{K}^-\left(P_1\right)$: נכון ב־$t$ אם $t = \sup\left\{t' \mid t' < t \wedge P_1\left(t\right)\right\}$. אפשר לומר:

$$\mathbf{K}^-\left(P_1\right) \equiv \neg\left(\neg P \textbf{ Since } true\right)$$

- $\mathbf{K}^+\left(P_1\right)$: באופן דומה.

אזי את "P_1 נכון תמיד החל מנקודה כלשהי בעתיד (Infinitely Often)" נתרגם בצורה הבאה:

$$(\Box \diamond P_1) \vee \left(\diamond \mathbf{K}^- (P_1)\right) \vee \left(\diamond \mathbf{K}^+ (P_1)\right)$$

מעל $\mathbb{Q}$ לא נוכל להצרין את הטענה, מכיוון שהיא לא ניתנת להצרנה בלוגיקה מסדר ראשון.

4.5 משפט Kamp

4.5.1 משפט Kamp

4.5.1.1 מ־$\mathcal{TL}$ ל־$\mathcal{FOMLO}$

כל ה־Modalities שראינו יכולים להיתרגם בקלות ללוגיקה מונדית מסדר ראשון עם סדר ($\mathcal{FOMLO}$). למשל, עבור הנוסחה $P\,\mathbf{Until}\,Q$:

$$\varphi_{\mathbf{Until}}(x_0, P, Q) \equiv \exists x'.\,(x' > x_0 \wedge Q(x') \wedge (\forall x_1.\,((x_0 < x_1 \wedge x_1 < x') \to P(x_1))))$$

משפט 51 (מ־$\mathcal{TL}(\mathbf{Until}, \mathbf{Since})$ ל־$\mathcal{FOMLO}$): לכל נוסחה $A \in \mathcal{TL}(\mathbf{Until}, \mathbf{Since})$ יש נוסחה $\varphi_A(x_0) \in \mathcal{FOMLO}$ כך שלכל M ו־t:

$$M, t \models A \iff M, t \models \varphi_A(x_0)$$

הוכחה: באמצעות אינדוקציה מבנית פשוטה. ■

4.5.1.2 משפט Kamp

הגדרה 52 (שרשרת): סדר לינארי עם פרדיקטים מונדים נקרא שרשרת (*Chain*).

משפט 53: לכל נוסחה $\varphi(x_0) \in \mathcal{FOMLO}$ עם איבר חופשי אחד יש נוסחה $A \in \mathcal{TL}(\mathbf{Until}, \mathbf{Since})$ ששקולה ל־φ מעל שרשראות של $(\mathbb{N}, <)$.

הגדרה 54 (שלמות Dedekind): סדר לינארי $(T, <)$ ייקרא *Dedekind*־שלם (*Dedekind-Complete*) אם לכל תת־קבוצה לא ריקה $S \subseteq T$:

1. אם ל־S יש חסם תחתון ב־T, אז יש לה חסם תחתון צמוד ב־T, כלומר $\inf(S) \in T$.
2. אם ל־S יש חסם עליון ב־T, אז יש לה חסם עליון צמוד ב־T, כלומר $\sup(S) \in T$.

דוגמה 55: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ הם Dedekind־שלמות. $\mathbb{Q}$ היא לא Dedekind־שלמה.

משפט 56: לכל נוסחה $\varphi(x_0) \in \mathcal{FOMLO}$ עם משתנה חופשי יחיד יש נוסחה $A \in \mathcal{TL}(\mathbf{Until}, \mathbf{Since})$ ששקולה ל־φ מעל שרשרת שהיא *Dedekind*־שלמה.

4.5.2 הוכחת משפט Kamp

4.5.2.1 על ההוכחה

משפט מכונן זה הוא יריית הפתיחה למחקר של תחום שלמות הביטוי, והוא עדיין אחת התוצאות הכי מעניינות והייחודיות בלוגיקה טמפורלית. קיימות מעט מאוד, אם בכלל, תוצאות מודאליות דומות. נמצאו כמה הוכחות חלופיות של המשפט, ותוצאות חזקות יותר, אך אף אחת מהן אינה טריוויאלית (לפחות לרוב האנשים).
המשפט של Kamp הוכח:

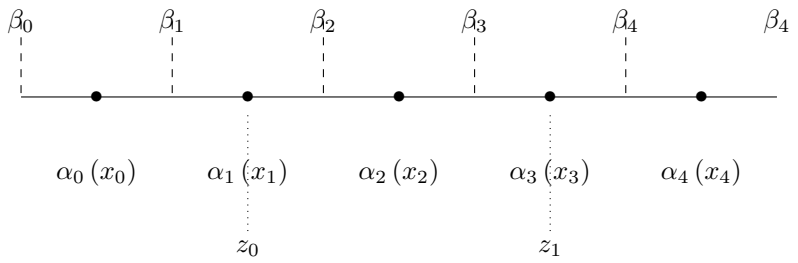
1. בתזה של Kamp (1968). ההוכחה כוללת יותר מ־100 עמודים.
2. מתווה של ההוכחה פורסם על ידי Gabbay, Pnueli, Stavi ו־Shelah (1980) עבור $\mathbb{N}$, ונאמר שההוכחה יכולה להתרחב גם לכל מרחב שהוא Dedekind־שלם.
3. על ידי Gabbay (1981) על ידי טענת ההפרדה ל־$\mathbb{N}$. ההוכחה הורחבה לכל מרחב Dedekind־שלם מאוחר יותר.
4. על ידי Hodkinson (1995) על ידי טענות משחקים, וההוכחה הופשטה ב־1999 (ההפשטה לא פורסמה).

הגדרה 57 (תכונת ההפרדה): אם כל נוסחה שקולה לקומבינציה בולאנית של הזמנים עתיד, עבר והווה, הלוגיקה מקיימת את תכונת ההפרדה.

4.5.2.2 נוסחאות $\forall\vec{\exists}$

הגדרה 58 (נוסחאות $\forall\vec{\exists}$): תהי Σ קבוצה של פרדיקטים מונדיים. נוסחת $\forall\vec{\exists}$ מעל Σ היא נוסחה מהצורה:

$$\begin{aligned}\psi(z_0,\ldots,z_m) \quad = \quad & \exists x_n \ldots \exists x_1 \exists x_0. \\ & \underbrace{\left(\bigwedge_{k=0}^{m} z_k = x_{i_k}\right) \wedge (x_n > x_{n-1} > \cdots > x_1 > x_0)}_{\text{Ordering}} \\ \wedge \quad & \underbrace{\bigwedge_{j=0}^{n} \alpha_j(x_j)}_{\text{Each } \alpha_j \text{ holds at } x_j} \\ \wedge \quad & \underbrace{\bigwedge_{j=1}^{n} \left[(\forall y)^{>x_j}_{>x_{j-1}} \beta_j(y)\right]}_{\text{Each } \beta_j \text{holds along } (x_{j-1},x_j)} \\ \wedge \quad & \underbrace{(\forall y)_{>x_n} \beta_{n+1}(y)}_{\beta_{n+1} \text{ holds everywhere after } x_n} \\ \wedge \quad & \underbrace{(\forall y)^{<x_0} \beta_0(y)}_{\beta_0 \text{ holds everywhere before } x_0}\end{aligned}$$



איור 4.1: דוגמה לנוסחת $\forall\overrightarrow{\exists}$

כאשר $\{\alpha_j\}_{i=0}^{n}$ ו־$\{\beta_j\}_{j=0}^{n+1}$ הן נוסחאות ללא כמתים מעל Σ, וכן:

$$\begin{aligned}(\forall y)_{>c_1}^{<c_0}\varphi &\equiv \forall y.\left((c_0 < y \wedge y < c_1) \rightarrow \varphi\right)\\ x_n > \cdots > x_1 > x_0 &\equiv \bigwedge_{j=0}^{n-1} x_j < x_{j+1}\end{aligned}$$

ניתן לראות דוגמה לנוסחת $\forall\overrightarrow{\exists}$ באיור 4.1.
התכונות של נוסחאות $\forall\overrightarrow{\exists}$:

1. קוניונקציה (באמצעות $\vee$) של נוסחאות $\forall\overrightarrow{\exists}$ שקול לדיסיונקציה (באמצעות $\wedge$) של (כמה) נוסחאות $\forall\overrightarrow{\exists}$.
2. כל נוסחת $\forall\overrightarrow{\exists}$ שקולה לקוניונקציה של נוסחאות $\forall\overrightarrow{\exists}$ עם לכל יותר שני משתנים חופשיים.
3. לכל נוסחת $\forall\overrightarrow{\exists}$ φ, הנוסחה $\exists x.\varphi$ שקולה לנוסחת $\forall\overrightarrow{\exists}$.

הגדרה 59 (נוסחאות $\forall\overrightarrow{\exists}\vee$): נוסחה היא נוסחת $\forall\overrightarrow{\exists}\vee$ אם היא שקולה לקוניונקציה של נוסחאות $\forall\overrightarrow{\exists}$.

למה 60 (תכונות הסגירות): הקבוצה של נוסחאות $\forall\overrightarrow{\exists}\vee$ סגורה תחת הפעלות של $\vee$, $\wedge$ ו־$\exists$.

הוכחה: באמצעות שימוש בתכונות 1 ו־3, ובחלוקה של $\exists$ עם $\vee$. ■

קבוצת נוסאחות ה־$\forall\overrightarrow{\exists}\vee$ לא סגורה תחת שלילה ($\neg$). אולם השלילה של נוסחת $\forall\overrightarrow{\exists}\vee$ שקולה לנוסחת $\forall\overrightarrow{\exists}\vee$ בהרחבה של שרשראות על ידי כל הפרדיקטים הניתנים להגדרה ב־$\mathcal{TL}(\mathbf{Until},\mathbf{Since})$.

4.5.2.3 מנוסחאות $\forall\overrightarrow{\exists}\vee$ לנוסחאות $\mathcal{TL}(\mathbf{Until},\mathbf{Since})$

טענה 61: כל נוסחת $\forall\overrightarrow{\exists}\vee$ עם איבר חופשי אחד שקולה לנוסחה ב־$\mathcal{TL}(\mathbf{Until},\mathbf{Since})$.

הוכחה: φ שקולה ל־ψ כאשר:

$$\begin{aligned}\varphi &\equiv \exists x_n\ldots\exists x_1\exists x_0.z_0=0_k\wedge(x_n>x_{n-1}>\cdots>x_1>x_0)\wedge\bigwedge_{j=0}^{n}\alpha_j(x_j)\\ &\quad\wedge\bigwedge_{j=1}^{n}\left[\left((\forall y)^{\leq x_j}_{>x_{j-1}}\beta_j(y)\right)\wedge\left((\forall y)^{<x-0}\beta_0(y)\right)\wedge\left((\forall y)_{>x_n}\beta_n(y)\right)\right]\\ \psi &= (A_k\wedge(B_{k+1}\mathbf{Until}(A_{k+1}\wedge(B_{k+2}\mathbf{Until}\cdots(A_{n-1}\wedge(B_n\mathbf{Until}(A_n\wedge\Box B_{n+1})))\cdots))))\\ &\quad\vee\left(A_k\wedge\left(B_{k-1}\mathbf{Since}\left(A_{k-1}\wedge\left(B_{k-2}\mathbf{Since}\cdots\left(A_1\wedge\left(B_1\mathbf{Since}\left(A_0\wedge\overleftarrow{\Box}B_0\right)\right)\right)\cdots\right)\right)\right)\right)\end{aligned}$$

■

4.5.2.4 הרחבה קנונית

הגדרה 62 (הרחבה קנונית): נניח ש־M הוא Σ־שרשרת, ו־$\mathcal{L}$ לוגיקה טמפורלית. נגדיר:

$$\mathcal{L}[\Sigma]=\{A\mid A\text{ is an }\mathcal{L}\text{-formula over }\Sigma\}$$

ההרחבה הקנונית לפי $\mathcal{L}$ של M היא הרחבה של M להיות $\mathcal{L}[\Sigma]$־שרשרת, כאשר $A\in\mathcal{L}[\Sigma]$ מפורש כ־$\{a\in M\mid M,a\models A\}$.

נאמר שנוחסאות מסדר ראשון בחתימה $\mathcal{L}[\Sigma]\cup\{<\}$ שקולות מעל M (או מעל מחלקה $\mathcal{C}$ של Σ־שרשראות) אם הן שקולות בהרחבה הקנונית של M (או בהרחבה הקנונית של כל $M\in\mathcal{C}$).

4.5.2.5 שקילות בהרחבה הקנונית

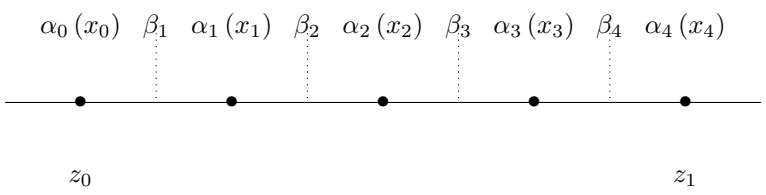
נוסחאות $\forall\overrightarrow{\exists}$ ו־$\forall\overrightarrow{\exists}\vee$ מוגדרות כום קודם, אבל עכשיו הן משמשות כאטומים בפרדיקטים הניתנים להגדרה ב־$\mathcal{L}$. כל מה שתקף קודם, תקף גם עכשיו, עבור הכתיב החדש של נוסחאות $\forall\overrightarrow{\exists}\vee$. בפרט, מעל הרחבה קנונית של $\mathcal{TL}(\mathbf{Until},\mathbf{Since})$:

1. כל נוסחאת $\forall\overrightarrow{\exists}\vee$ עם משתנה חופשי אחד שקולה לנוסחה ב־$\mathcal{TL}(\mathbf{Until},\mathbf{Since})$.
2. קבוצת נוסחאות $\forall\overrightarrow{\exists}\vee$ סגורה תחת קוניונקציה, דיסיונקציה וכימות קיום.

כמו כן, הקבוצה של נוסחאות $\forall\overrightarrow{\exists}\vee$ עכשיו סגורה גם תחת שלילה.

4.5.2.6 הוכחת משפט Kamp

הצעה 63 (סגירות תחת שלילה): השלילה של נוסחאות $\forall\overrightarrow{\exists}$ עם לכל היותר שני משתנים חופשיים שקולה מעל שרשראות *Dedekind*־שלמות לדיסיונקציה של נוסחאות $\forall\overrightarrow{\exists}\vee$.



איור 4.2: $[\alpha_0, \beta_1, \alpha_1, \beta_2, \ldots, \beta_n, \alpha_n](z_0, z_1)$

הוכחה: השלילה של:

$$\exists x_0 \ldots \exists x_n. \left(z = x_0 \wedge (x_0 < x_1 < \cdots x_n) \wedge x_n = z_1 \wedge \left(\bigwedge_{i=0}^{n} \alpha_i(x_1) \right) \wedge \left(\bigwedge_{i=0}^{n-1} (\forall y)_{>x_i}^{<x_{i+1}} \beta_{i+1}(y) \right) \right)$$

שקולה לדיסיונקציה של נוסחאות $\forall\overrightarrow{\exists}$. נוכיח את זה בשלבים.
נסמן ב־$[\alpha_0, \beta_1, \alpha_1, \beta_2, \ldots, \beta_n, \alpha_n](z_0, z_1)$ את הנוסחה לעיל. ניתן לראות דוגמה לכך באיור 4.2.

טענה 64: השלילה של $\exists x_1 \ldots \exists x_n (z_0 < x_1 < \cdots < x_n < z_1) \wedge \bigwedge_{i=1}^{n} P_i(x_i)$ שקולה לנוסחה $O_n[P_1, \ldots, P_n](z_0, z_1)$ שהיא נוסחת $\forall\overrightarrow{\exists}\vee$.

הוכחה: באינדוקציה על n.
בסיס: $n = 1$. אזי הנוסחה שלנו היא $\exists x_1. z_0 < x_1 < z_1 \wedge P_1(x_1)$. ברור שנוסחה זו היא נוסחת $\forall\overrightarrow{\exists}$, ולכן גם נוסחת $\forall\overrightarrow{\exists}\vee$.
מעבר: נניח n. נוכיח $n+1$. יש לנו שני מקרים:

מקרה 1 P_1 לא נכונה על (z_0, z_1).

מקרה 2 P_1 נכונה בנקודה ב־(z_0, z_1). יהיה $z = \inf\{t \in (z_0, z_1) \mid P_1(t)\}$. אם $z = z_0$, אזי $\mathbf{K}^+(P_1)(z_0)$. אחרת, $z \in (z_0, z_1)$. בתת־מקרה זה, z ניתן להגדרה על ידי נוסחת $\forall\overrightarrow{\exists}$:

$$z_0 < z < z_1 \wedge \left((\forall y)_{>z_0}^{<z} \neg P_1(y) \right) \wedge P_1(z) \wedge \mathbf{K}^+(P_1)(z)$$

לכן, $(\forall y)_{>z_0}^{<z_1} \neg P_1(y)$ היא דיסיונקציה של $O_{n+1}[P_1, \ldots, P_{n+1}](z_0, z_1)$ (עבור $z_0 \leq z_1$) של:

1. $\mathbf{K}^+(P_1)(z_0) \wedge O_n[P_2, \ldots, P_{n+1}](z_0, z_1)$.
2. $\exists z. \left(z_0 < z < z_1 \wedge \left((\forall y)_{>z_0}^{<z} \neg P_1(y) \right) \wedge (P_1(z) \vee \mathbf{K}^+(P_1)(z)) \wedge O_n[P_2, \ldots, P_{n+1}](z, z_1) \right)$.

זה שקול לנוסחת $\forall\overrightarrow{\exists}\vee$. ■

מסקנה 65: הנוסחה

$$\neg\left(\exists z\right)_{>z_0}^{<z_1}\left[\alpha_0,\beta_1,\alpha_1,\beta_1,\ldots,\beta_n,\alpha_n\right]\left(z_0,z\right)$$

שקולה לנוסחת $\forall\overrightarrow{\exists}\vee$, כאשר:

$$\left(\exists z\right)_{>x}^{<y}\varphi\equiv\exists z.\left(x<z<y\wedge\varphi\right)$$

הוכחה: נגדיר את F_n להיות α_n ו־F_{i-1} להיות $\alpha_{i-1}\wedge\beta_i\mathbf{Until}F_i$. אזי:

$$\left(\exists z\right)_{>z_0}^{<z_1}\left[\alpha_0,\beta_1,\alpha_1,\beta_2,\ldots,\beta_n,\alpha_n\right]\left(z_0,z\right)$$

אם ורק אם

$$F_0\left(z_0\right)\wedge\exists x_1\ldots\exists x_n\left(z_0<x_1<\cdots<x_n<z_1\wedge\bigwedge_{i=1}^{n}F_i\left(x_i\right)\right)$$

לכן, $\left(z_0,z\right)\left[\alpha_0,\beta_1,\alpha_1,\beta_2,\ldots,\beta_n,\alpha_n\right]\left(\exists z\right)_{>z_0}^{<z_1}\neg$ שקולה ל־$\neg F_0\left(z_0\right)\vee O_n\left[F_1,\ldots,F_n\right]\left(z_0,z_1\right)$, ששקולה לנוסחת $\forall\overrightarrow{\exists}\vee$. ■

נוכיח כעת ש־$\neg\left[\alpha_0,\beta_1,\alpha_1,\beta_2,\ldots,\beta_n,\alpha_n\right]\left(z_0,z_1\right)$ שקולה מעל שרשראות Dedekind־שלמות לנוסחת $\forall\overrightarrow{\exists}\vee$.

נחלק את ההוכחה ל־3 מקרים:

1. $\neg\left(\beta_1\mathbf{Until}\alpha_1\right)\left(z_0\right)$ או $\neg\alpha_0\left(z_0\right)$.

מקרה זה כבר מתאר נוסחת $\forall\overrightarrow{\exists}\vee$ (בהרחבה קנונית). לכן, במקרה זה, $\neg\left[\alpha_0,\beta_1,\alpha_1,\beta_2,\ldots,\beta_n,\alpha_n\right]\left(z_0,z_1\right)$ שקולה ל־$true$.

2. $\alpha_0\left(z_0\right)$ וגם β_1 נכונה ב־$\left(z_0,z_1\right)$.

המקרה הזה מתואר על ידי נוסחת $\forall\overrightarrow{\exists}\vee$:

$$\alpha_0\left(z_0\right)\wedge\left(\left(\forall z\right)_{>z_0}^{<z_1}\beta_1\left(z\right)\right)$$

במקרה הזה, הנוסחה $\neg\left[\alpha_0,\beta_1,\alpha_1,\beta_2,\ldots,\beta_n,\alpha_n\right]\left(z_0,z_1\right)$ שקולה ל"אין $z\in\left(z_0,z_1\right)$ כך ש־$\left[\alpha_1,\beta_2,\ldots,\beta_n,\alpha_n\right]\left(z,z_1\right)$". ממסקנה 65, הנוסחה ניתנת לביטוי כנוסחת $\forall\overrightarrow{\exists}\vee$.

3. $\alpha_0\left(z_0\right)\wedge\left(\beta_1\mathbf{Until}\alpha_1\right)\left(z_0\right)$ וגם יש $x\in\left(z_0,z_1\right)$ שמתקיים $\neg\beta_1\left(x\right)$.

בבירור, ניתן לכתוב את המקרה כנוסחת $\forall\overrightarrow{\exists}\vee$.

נוכיח את מקרה זה באמצעות אינדוקציה על n. נגדיר את הנוסחאות הבאות:

(א) $A_i^-\left(z_0,z\right)\equiv\left[\alpha_0,\beta_1,\ldots,\beta_i,\alpha_i\right]\left(z_0,z\right)$ עבור $i\in\{1,\ldots,n\}$.

(ב) $A_i^+\left(z,z_1\right)\equiv\left[\alpha_i,\beta_{i+1},\ldots,\beta_{n+1},\alpha_{n+1}\right]\left(z,z_1\right)$ עבור $i\in\{1,\ldots,n\}$.

(ג) $A_i(z_0,z,z_1) \equiv A_i^-(z_0,z) \wedge A_i^+(z,z_1)$ עבור $i \in \{1,\ldots,n\}$.

(ד) $B_i^-(z_0,z) \equiv [\alpha_0,\beta_1,\ldots,\beta_{i-1},\alpha_{i-1},\beta_i,\beta_i](z_0,z)$ עבור $i \in \{1,\ldots,n+1\}$.

(ה) $B_i^+(z,z_1) \equiv [\beta_i,\beta_i,\alpha_i,\beta_{i+1},\ldots,\beta_{n+1},\alpha_{n+1}](z,z_1)$ עבור $i \in \{1,\ldots,n+1\}$.

(ו) $B_i(z_0,z,z_1) \equiv B_i^-(z_0,z) \wedge B_i^+(z,z_1)$ עבור $i \in \{1,\ldots,n+1\}$.

$$B_2(z_0,z,z_1) \equiv [\alpha_0,\beta_1,\alpha_1,\beta_2,\beta_2](z_0,z) \wedge [\beta_2,\beta_2,\alpha_2,\beta_3,\ldots,\beta_{n+1},\alpha_{n+1}](z,z_1)$$

אם (z_0,z_1) היא קבוצה לא ריקה, נקבל:

$$[\alpha_0,\beta_1,\alpha_1,\beta_2,\ldots,\beta_{n+1},\alpha_{n+1}](z_0,z_1) \equiv (\forall z)_{>z_0}^{<z_1}\left(\left(\bigvee_{i=1}^{n} A_i\right) \wedge \left(\bigvee_{i=1}^{n+1} B_i\right)\right)$$

לכן, לכל φ

$$\left((\exists z)_{>z_0}^{<z_1}\varphi(z)\right) \wedge \neg[\alpha_0,\beta_1,\alpha_1,\beta_2,\ldots,\beta_{n+1},\alpha_{n+1}](z_0,z_1)$$

שקול ל:

$$(\exists z)_{>z_0}^{<z_1}\left(\varphi(z) \wedge \bigwedge_{i=1}^{n}\neg A_i \wedge \bigwedge_{i=1}^{n+1}\neg B_i\right)$$

בפרט,

$$\left((\exists z)_{>z_0}^{<z_1}\inf_{\neg\beta_1}(z)\right) \wedge \neg[\alpha_0,\beta_1,\alpha_1,\beta_2,\ldots,\beta_{n+1},\alpha_{n+1}](z_0,z_1)$$

שקול ל:

$$(\exists z)_{>z_0}^{<z_1}\left(\inf_{\neg\beta_1}(z) \wedge \bigwedge_{i=1}^{n}\neg A_i \wedge \bigwedge_{i=1}^{n+1}\neg B_i\right)$$

לכל אחד מהמקרים:

1. בנינו נוסחת $\vec{\exists}\forall\vee$, שנקרא לה $Cond_i$, שמתארת את המקרה.
2. הראנו שאם $Cond_i$ נכונה, אז $\neg[\alpha_0,\beta_1,\alpha_1,\beta_2,\ldots,\beta_n,\alpha_n](z_0,z_1)$ שקולה לנוסחה $Form_i$ שהיא נוסחת $\vec{\exists}\forall\vee$.

לכן, $\neg[\alpha_0,\beta_1,\alpha_1,\beta_2,\ldots,\beta_n,\alpha_n](z_0,z_1)$ שקולה ל־$\bigvee_i[Cond_i \wedge Form_i]$, שהיא נוסחת $\vec{\exists}\forall\vee$. ■

הצעה 66: כל נוסחה מסדר ראשון שקולה מעל שרשרת *Dedekind* שלמה לדיסיונקציה של נוסחאות $\vec{\exists}\forall\vee$.

משפט 67 (Kamp): לכל נוסחה $\varphi(x) \in \mathcal{FOMLO}$ עם משתנה חופשי אחד יש נוסחה ב־$\mathcal{TL}(\mathbf{Until}, \mathbf{Since})$ ששקולה ל־φ מעל שרשראות *Dedekind*־שלמות.

הוכחה: $\varphi(x)$ שקולה מעל שרשראות Dedekind־שלמות לדיסיונקציה של נוסחאות $\forall \vec{\exists} \wedge$. נקרא להן $\{\varphi_i(x)\}$.
$\varphi_i(x)$ שקולה לנוסחה ב־$\mathcal{TL}(\mathbf{Until}, \mathbf{Since})$. לכן, $\varphi(x)$ שקולה מעל שרשראות Dedekind־שלמות לנוסחה ב־$\mathcal{TL}(\mathbf{Until}, \mathbf{Since})$. ■

4.6 משפט Stavi

ראינו ש־$\mathcal{TL}(\mathbf{Until}, \mathbf{Since})$ יותר חלשה מ־$\mathcal{FOMLO}$ מעל $\mathbb{Q}$.
נגדיר קשר חדש: ה־**Until** של Stavi: $P\,\mathbf{Until}^s\,Q$ מתקיים ב־t_0 אם יש מרווח $g > t_0$ כך ש:

1. P מתקיים על (t_0, g).
2. $\neg P$ מתקיים במרחק שרירותי מ־g.
3. Q מתקיים כמה זמן אחרי g.

באופן דומה, מגדירים את ה־**Since** של Stavi (**Since**^{s}).

משפט 68 (Stavi): ל־$\mathcal{TL}(\mathbf{Until}, \mathbf{Since}, \mathbf{Until}^s, \mathbf{Since}^s)$ יש כוח ביטוי שקול ל־$\mathcal{FOMLO}$ מעל כל סדר לינארי.

פורסמו שתי הוכחות למשפט Stavi. שתיהן קשות באופן קיצוני. ההוכחה שלנו למשפט Kamp ניתנת לשינוי בקלות כדי להוכיח את משפט Stavi.