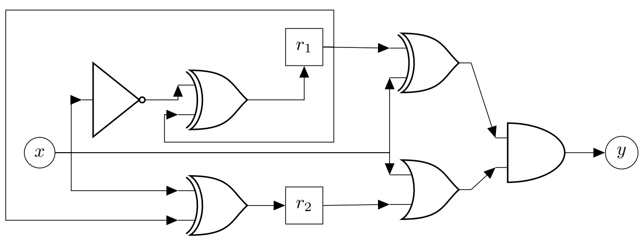
תרגיל בית עיוני מספר 1 בקורס אימות תוכנה בשיטות פורמאליות

6 באפריל 2025

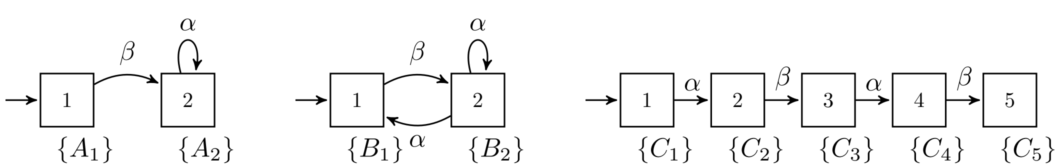
יש לענות על כל השאלות, ולהגיש קובץ PDF.

שאלה 1

א. בנו את מערכת המעברים המתאימה למעגל הלוגי הבא על פי התרגום שלמדנו:



ב. בנו את מערכת המעברים $(TS_A|||_{\{\beta\}}TS_B)|||_{\{\alpha,\beta\}}TS_C$ עבור מערכות המעברים הבאות



TS_A TS_B TS_C

שאלה 2

נתונים שני גרפי תוכנית:

- $PG_1 = (Loc_1, Act_1, Effect_1, \rightarrow_1, Loc_{0,1}, g_{0,1})$ כאשר:
  - $Loc_1 = \{A, B\}$
  - $Act_1 = \{\alpha, \beta\}$
  - $Loc_{0,1} = \{A\}$
  - $g_{0,1} = x == 0$
  - $\rightarrow_1 = \{(A, x == 0, \alpha, B), (B, true, \beta, A)\}$
  - $Effect_1(\alpha, \eta) = \eta[x := 1], \quad Effect_1(\beta, \eta) = \eta[x := 0]$
- $PG_2 = (Loc_2, Act_2, Effect_2, \rightarrow_2, Loc_{0,2}, g_{0,2})$ כאשר:
  - $Loc_2 = \{C, D\}$
  - $Act_2 = \{\gamma, \delta\}$

- $Loc_{0,2} = \{C\}$
- $g_{0,2} = y == 0$
- $\rightarrow_2 = \{(C, y == 0, \gamma, D), (D, true, \delta, C)\}$
- $Effect_2(\gamma, \eta) = \eta[y := 1], \quad Effect_2(\delta, \eta) = \eta[y := 0]$

(א) שרטטו את שני גרפי התוכנית.

(ב) הרכיבו את שני גרפי התוכנית לגרף תוכנית שזור.

(ג) המירו את גרף התוכנית השזור למערכת מעברים מלאה.

(ד) בדקו והסבירו האם במערכת מעברים מתקיימת התכונה: "לעולם לא ייתכן מצב בו $x = 1 \wedge y = 1$".

שאלה 3

בהגדרת התרגום מגרף תוכנית למערכת מעברים החלפנו את כלל הגזירה למעברים בכלל:

$$\frac{l \xrightarrow{g:\alpha} l' \wedge \text{Effect}(\alpha,\eta) \models g}{\langle l,\eta\rangle \xrightarrow{\alpha} \langle l', \text{Effect}(\alpha,\eta)\rangle}$$

את שאר הבנייה השארנו כפי שלמדנו. הסבירו את המשמעות של השינוי. הראו גרף תוכנית שהתרגום שלו משתנה בעקבות השינוי והסבירו למה הגיוני להשתמש בבנייה החדשה עבור הדוגמה שנתתם.

שאלה 4

בהנתן מערכת מעברים $TS = \langle S, \{\alpha, \beta\}, \rightarrow_{org}, I, AP, L\rangle$ נבנה מערכת מעברים $TS' = \langle S, \{\alpha \circ \beta\}, \rightarrow_{new}, I, AP, L\rangle$ לפי כלל הגזירה:

$$\frac{s_1 \xrightarrow{\alpha}_{org} s_2 \wedge s_2 \xrightarrow{\beta}_{org} s_3}{s_1 \xrightarrow{\alpha\circ\beta}_{new} s_3}$$

ונמחק ממנה מצבים ללא מוצא. הוכיחו או הפריכו את הטענות הבאות עבור TS' שלאחר מחיקת המצבים:

א. אם P היא תכונה מהצורה

$$P = \{\sigma \in (2^{AP})^\omega : \forall i \geq 0 \text{ it holds that } \sigma[i] \models \Phi\}$$

באשר Φ היא תכונת מצב כלשהי, אז מתקיים $TS \models P \Rightarrow TS' \models P$.

ב. אם P היא תכונה מהצורה

$$P = \{\sigma \in (2^{AP})^\omega : \forall i \geq 0 \text{ it holds that } \sigma[i] \models \Phi\}$$

באשר Φ היא תכונת מצב כלשהי, אז מתקיים $TS' \models P \Rightarrow TS \models P$.

ג. אם P היא תכונה מהצורה

$$P = \{\sigma \in (2^{AP})^\omega : \exists i \geq 0 \text{ such that } \forall j \geq i \text{ it holds that } \sigma[j] \models \Phi\}$$

באשר Φ היא תכונת מצב כלשהי, אז מתקיים $TS \models P \Rightarrow TS' \models P$.

ד. אם P היא תכונה מהצורה

$$P = \{\sigma \in (2^{AP})^\omega : \exists i \geq 0 \text{ such that } \forall j \geq i \text{ it holds that } \sigma[j] \models \Phi\}$$

באשר Φ היא תכונת מצב כלשהי, אז מתקיים $TS' \models P \Rightarrow TS \models P$.

☺ בהצלחה! ☺