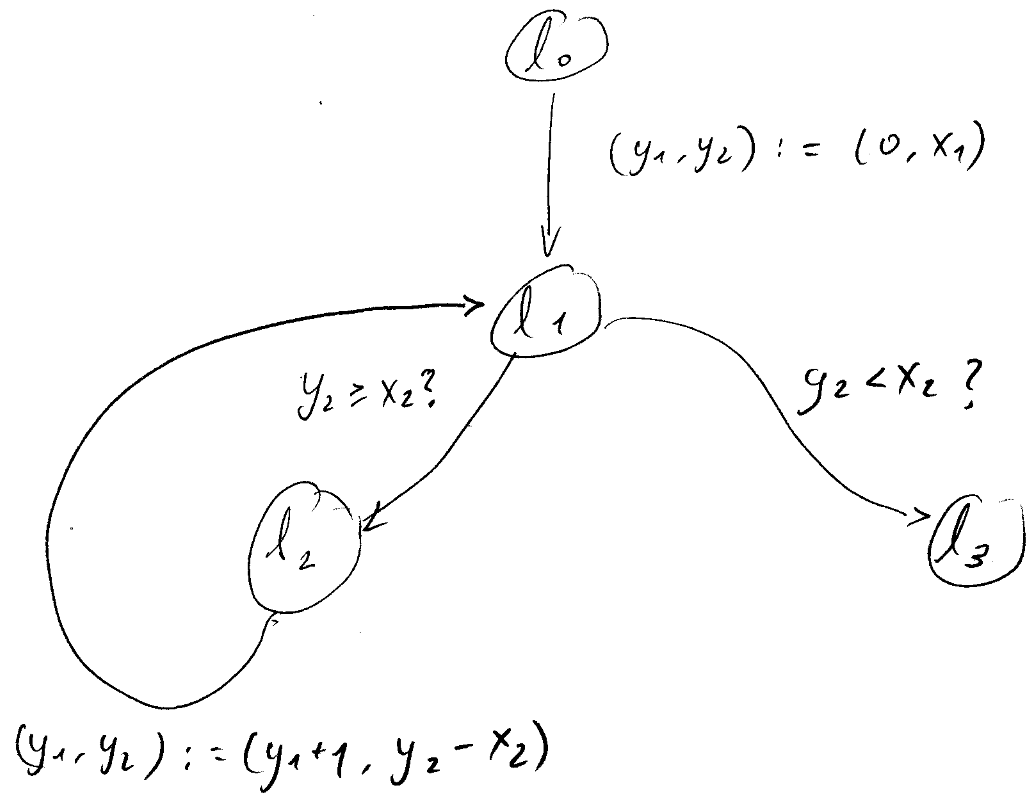
שיעור 2 - הוכחת נכונות חלקית

בשיעור שעבר ראינו את המסגרת להוכחת נכונות חלקית, פיתוח מלא הוכחה בהרצאות, כעת נראה תרגיל לדוגמא:

הוכח כי התוכנית P נכונה ביחס לספציפיקציה

$$(\phi, \psi) = (x_1 \geq 0 \wedge x_2 > 0 \,,\; x_1 = y_1 \cdot x_2 + y_2 \wedge 0 \leq y_2 < x_2)$$

תהיה P תוכנית החלוקה בשלמים משיעור שעבר:



1. נגדיר קבוצת נק' חיתוך:

$$C = \{l_0, l_1, l_3\}$$

2. נגדיר את מסלולי הבסיס:

$\pi_{01} : l_0, l_1$

$\pi_{11} : l_1, l_2, l_1$

$\pi_{13} : l_1, l$

3. הגדרה Summary Guarded Cmds :

לכל מסלול $\overbrace{\pi}^{\text{אימות}}$ נרצה לבנות הוראה שמסכמת את האפקט של הרצת π על וקטור המשתנים V.

$$\pi: \quad \ell_1 \xrightarrow{c_1 \to [V := f_1(V)]} \ell_2 \rightsquigarrow \cdots \longrightarrow \ell_k \xrightarrow{c_k \to [V := f_k(V)]} \ell_{k+1}$$

$$c_\pi : \; c_1(V) \wedge c_2(f_1(V)) \wedge \cdots \wedge c_k(f_{k-1}(\cdots f_1(V)\cdots))$$

$$f_\pi : \; f_k(f_{k-1}(\cdots f_2(f_1(V))\cdots))$$

ההוראה תהיה מהצורה :

$$G_\pi : c_\pi \to [V := f_\pi(V)]$$

לסיכום :

$$G_{01} : \; (y_1, y_2) := (0, x_1)$$

$$G_{11} : \; y_2 \geq x_2 \to (y_1, y_2) := (y_1 + 1, y_2 - x_2)$$

$$G_{13} : \; y_2 < x_2 \; ?$$

4: הגדרה. assertion (טענה) לכל נק' חיתוך :

$$\phi_0 : \; x_1 \geq 0 \wedge x_2 > 0$$

$$\phi_1 : \; x_1 = y_1 \cdot x_2 + y_2 \wedge 0 \leq y_2$$

$$\phi_3 : \; x_1 = y_1 \cdot x_2 + y_2 \wedge 0 \leq y_2 < x_2$$

(3)

T2

5. לכל מסלול אימות π, שמחבר נק' חיתוך l_i לנק' חיתוך l_j צריך להראות כי מתקיים תנאי האימות:

$$VC_\pi : \underbrace{\varphi_i}_{\text{הטענה שהצמדנו לנק' חיתוך } l_i} \underbrace{(V)}_{\text{מצב המשתנים בכניסה ל-}\pi} \wedge \underbrace{C_\pi}_{\text{תנאי הכניסה למסלול }\pi} \rightarrow \underbrace{\varphi_j}_{\text{הטענה שהצמדנו לנק' חיתוך } l_j} (\underbrace{f_\pi(V)}_{\text{מצב המשתנים ביציאה מ-}\pi\text{.}})$$

$$VC_{01} : \overbrace{x_1 \geq 0 \wedge x_2 > 0}^{\phi_0} \rightarrow x_1 = 0 \cdot x_2 + x_1 \wedge 0 \leq x_1$$

$$\Leftrightarrow x_1 \geq 0 \wedge x_2 > 0 \rightarrow 0 \leq x_1 \Leftrightarrow \underline{\underline{true}}$$

$\Rightarrow$ מתקיימים תנאי האימות למסלול π_{01}

$$VC_{11} : \overbrace{x_1 = y_1 \cdot x_2 + y_2 \wedge 0 \leq y_2}^{\phi_1} \wedge y_2 \geq x_2 \rightarrow$$

$$x_1 = (y_1+1) \cdot x_2 + (y_2 - x_2) \wedge 0 \leq (y_2 - x_2)$$

$$\Leftrightarrow$$

$$x_1 = y_1 \cdot x_2 + y_2 \wedge 0 \leq y_2 \wedge y_2 \geq x_2 \rightarrow$$

$$x_1 = y_1 x_2 + y_2 \wedge 0 \leq (y_2 - x_2)$$

$$\Leftrightarrow \underline{\underline{true}}$$

מכיוון ש: $0 \leq y_2 \wedge y_2 \geq x_2 \rightarrow 0 \leq (y_2 - x_2)$

$\Rightarrow$ מתקיים תנאי האימות למסלול π_{11}.

④
T2

$$VC_{13}: \overbrace{x_1 = y_1 \cdot x_2 + y_2 \wedge 0 \le y_2}^{\varphi_1} \wedge y_2 < x_2 \rightarrow$$

$$x_1 = y_1 \cdot x_2 + y_2 \wedge 0 \le y_2 < x$$

$$\Leftrightarrow \underline{\text{true}}$$

$\Leftarrow$ מתקיים תנאי האימות למסלול π_{13}

קיבלנו כי כל תנאי האימות מתקיימים, עבור כל מסלולי האימות בתכנית P $\Leftarrow$ $N = \{\phi_0, \phi_1, \phi_3\}$ היא רשת טענות אינדוקטיבית (inductive assertion network).

$\Downarrow$

P נכונה חלקית ביחס ל- (φ, ψ).

הדגמת תרגיל בית.