T3-1 13/3/03

שיעור 3

א. בשיעור שעבר נשאלו שאלות בקשר למסלול אימות π :

$$\pi: \quad l_1 \xrightarrow{c_1 \to [V: f_1(V)]} l_2 \dashrightarrow \cdots \to l_k \xrightarrow{c_k \to [V: f_k(V)]} l_{k+1}$$

כאשר:

$$C_\pi: \ c_1(V) \wedge c_2(f_1(V)) \wedge \dots \wedge c_k(f_{k-1}(\dots f_1(V)\dots))$$

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

ה- summary guarded cmd : $G_\pi: C_\pi \to [V: f_\pi(V)]$

הבהרות:

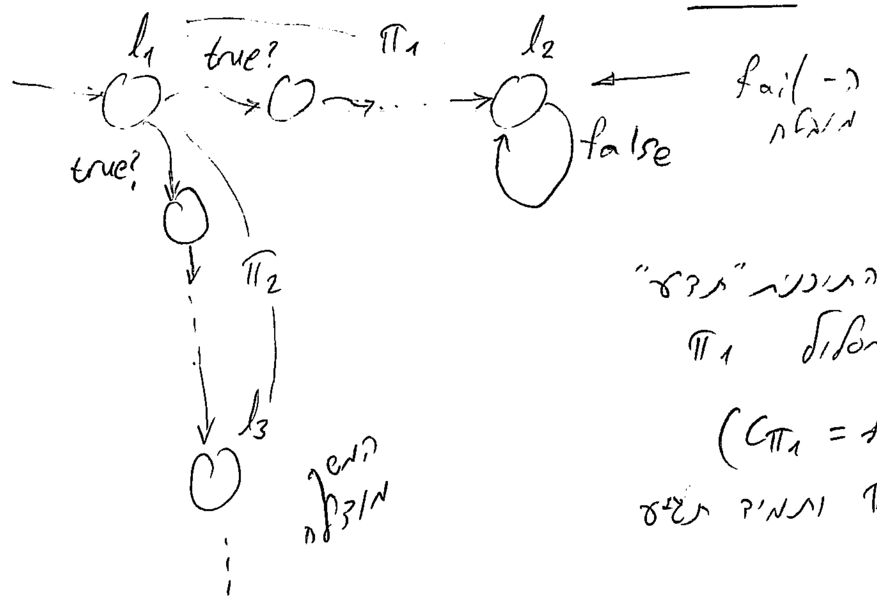
- C_π (תנאי המעבר) - התנאי המבטיח כי אם התוכנית תבחר במסלול π, היא תוכל להריץ אותו במלואו ולהגיע לסופו.
- f_π (טרנספורמציית המסלול) - האפקט הכולל של המסלול π על וקטור המשתנים V.
- גירסת התוכנית "המצומצמת" (reduced) המתקבלת ע"י כל ה- SGC הינה שקולה באופן חלש לתוכנית המקורית.
- מה לא נשמר? מה נשמר?

בתוכניות דטרמיניסטיות - נשמר המיפוי בין הקלט לתוצאות התוכנית - כלומר נשמרת משמעות התוכנית $M(P,d)$.

לא נשמרת קבוצת החישובים $Comp(P,d)$, ובפרט לא חישוב שנכשל. כשלון החישוב יכול "לצוץ" ב- cut-point שהתחלת מסלול הסיומות.

T3-2

בתוכנית אי-דטרמיניסטית - <u>לא נשמר</u> בהכרח המיפוי בין הקלט לתוצאות האפשריות של התוכנית (שכן כאן יכולים להיות יותר מתוצאה אחת עבור קלט). <u>דוגמה</u>:



בגירסה המלאכית התוכנית "תדע" כבר ב-l_1 כי מסלול π_1 חסר תקווה ($C_{\pi_1} = false$) היא תבחר ב-π_2 ותמיד תגיע לסיום מוצלח.

ב. בשיעור שעבר הדגמנו את השיטה של הוכחת נכונות חלקית באמצעות <u>שיטת הטענות האינדוקטיביות</u> (inductive assertions)

חתכנו את כל המעגלים ע"י נק' חיתוך, ובין כל שתי נק' חיתוך הגדרנו מסלול אטומי. לכל נק' חיתוך הצמדנו פרדיקט ולכל מסלול אטומי π:

$$\underset{P_i(V)}{l_i} \longrightarrow \underset{P_j(f_\pi(V))}{l_j}$$

דרשנו כי:

$$P_i(V) \rightarrow P_j(f_\pi(V)) \quad (*)$$

כלומר קיום הפרדיקט בכניסה גורר לוגית קיום הפרדיקט שביציאה מהמסלול. הדבר דומה לצעד אינדוקציה - נכונות עבור n גוררת נכונות עבור $n+1$, מכיוון שהתחלנו

התוכנית הצמדנו את φ ולסוף התוכנית הצמדנו את ψ קיבלנו את נכונות התוכנית ע"י הגרירה הלוגית שמתקבלת במעבר בין נק' החיתוך, החל מ-l_0 ועד l_t.

כעת נוכיח את נכונות השיטה (דף 23 בהרצאות).

<u>הגדרה</u>

קבוצת טענות (= רשת טענות) $N=\{\varphi_0,\dots\varphi_t\}$ עבור תוכנית P קרויה <u>אינדוקטיבית</u> אם כל תנאי האימות VC_π מתקיימים לגבי כל מסלולי האימות של P.

<u>הגדרה:</u>

רשת N קרויה אינווריאנטית ("שמורה"?) אם לכל מצב $<l_i, d>$ בחישוב-φ_0, כאשר $l_i \in C$, $d \models \varphi_i$.

כלומר, בכל "ביקור" של חישוב-φ_0 בנק' חיתוך l_i, מצב המשתנים שמספק <u>את הטענה φ_i</u> שמוצמדת ל-l_i.

<u>טענה 1:</u> כל רשת אינדוקטיבית היא אינווריאנטית.

<u>הוכחה:</u>

תהי $N=\{\varphi_0,\dots,\varphi_t\}$ רשת אינדוקטיבית ויהי σ

$$\sigma:\ <l_{i_0}, d_0> \xrightarrow{\pi_0} <l_{i_1}, d_1> \xrightarrow{\pi_1} \cdots \xrightarrow{\pi_{k-1}} <l_{i_k}, d_k> \xrightarrow{\pi_k} \cdots$$

חישוב-φ_0 כאשר סדרת נק' החיתוך בהם עוברים במהלך σ הן: $l_{i_0}, l_{i_1}, l_{i_2},\dots$; $\pi_0,\pi_1,\dots$ מסלולי האימות המחברים.

נוכיח באינדוקציה שלכל $j>0$ כי $d_j \models \varphi_{i_j}$.

<u>בסיס:</u> עבור $j=0$, $l_0 = l_{i_0}$ ומכיוון ש-σ היא מישב-φ_0 הרי ש- $d_0 \models \varphi_0$.

<u>צעד:</u> נניח כי $d_j \models \varphi_{i_j}$, ונראה כי: $d_{j+1} \models \varphi_{i_{j+1}}$.

מכיוון ש-σ עבר מ-l_{i_j} ל-$l_{i_{j+1}}$ דרך מסלול אטומי π_j, אז $d_j \models c_{\pi_j}$ וגם $d_{j+1} = f_{\pi_j}(d_j)$. כמו כן מתקיים <u>תנאי האימות:</u>

$$VC_{\pi_j} : \varphi_{i_j}(d_j) \wedge c_{\pi_j}(d_j) \to \varphi_{i_{j+1}}(f_{\pi_j}(d_j))$$

ומכיוון שמתקיימים $\varphi_{i_j}(d_j)$ וגם $c_{\pi_j}(d_j)$ הרי שמתקיים $\varphi_{i_{j+1}}(f_{\pi_j}(d_j))$ שזה בעצם $\varphi_{i_{j+1}}(d_{j+1})$. קיבלנו: $d_{j+1} \models \varphi_{i_{j+1}}$.

■

<u>מסקנה 2:</u>

אם $N=\{\varphi_0,\dots,\varphi_t\}$ רשת אינדוקטיבית אז התכנית P נכונה חלקית ביחס למפרט (φ_0,φ_t).

<u>הגדרה:</u>

רשת $N=\{\varphi_0,\dots,\varphi_t\}$ סוגרת מפרט (p,q) אם מתקיימים
$\varphi_t \to q$, $p \to \varphi_0$

<u>מסקנה 3:</u>

אם N רשת אינדוקטיבית שסוגרת את המפרט (p,q) אז התכנית P נכונה חלקית ביחס למפרט (p,q).

כלומר, ניתן לבחור <u>טענה חלשה מ-p עבור φ_0</u> (ו/או) <u>טענה חזקה מ-q עבור φ_t</u>.