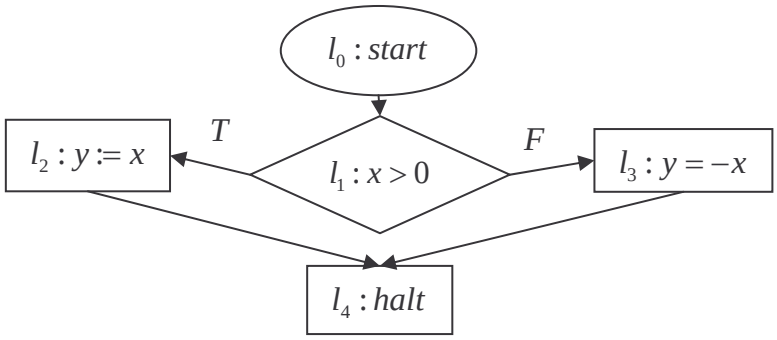


בהינתן מסלול τ בנינו את:

$T_\tau(\bar{x})$ - טרנספורמר

$R_\tau(\bar{x})$ - תנאי המעבר על τ

עבור המסלול השמאלי: $T_\tau(\bar{x}) = T_\tau^0(\bar{x}) = (x,x)$, $R_\tau(\bar{x}) = R_\tau^0(x,y) = x > 0$

עבור המסלול הימני: $T_\tau(\bar{x}) = T_\tau^0(\bar{x}) = (x,-x)$, $R_\tau(\bar{x}) = R_\tau^0(x,y) = x \le 0$

כלל נכונות להוכחת $\{q_1\} P \{q_2\}$:

$$q_1(\bar{x}) \wedge R_\tau(\bar{x}) \to q_2(\bar{x} \leftarrow T_\tau(\bar{x}))$$

(אם תנאי ההתחלה מתקיים והמסלול עביר אז תנאי הסיום מתקיים על הטרנספורמר של משתני ההתחלה)

מפרט התוכנית הנ"ל: $\{True\} P \{y = |x|\}$

נוכיח עבור τ_1 (המסלול השמאלי):

צ"ל: $True \wedge x > 0 \to y = |x| [(x,y) \leftarrow (x,x)]$

זאת אומרת, צריך להוכיח: $x > 0 \to x = |x|$

וזה אכן נכון באופן טריוויאלי.

נוכיח עבור τ_2 (המסלול הימני):

צ"ל: $True \wedge x \le 0 \to y = |x| [(x,y) \leftarrow (x,-x)]$

זאת אומרת, צריך להוכיח: $x \le 0 \to x = -|x|$

וזה אכן נכון באופן טריוויאלי.

כלל ההוכחה של *Floyd* לתוכניות תרשים זרימה <u>עם חוגים</u> (מעגלים מכוונים):

1. נבחר "נקודות חתך" בתוכנית.
   - א. נקודת התחלה l_0 $(start)$.
   - ב. נקודת סיום l_{halt} $(halt)$.
   - ג. לפחות נקודה אחת בכל לולאה (מכוונת).
2. לכל נקודת חתך l, נמצא טענה אינדוקטיבית (invariant שמורה) $I_l(\bar{x})$ כאשר נבחר:

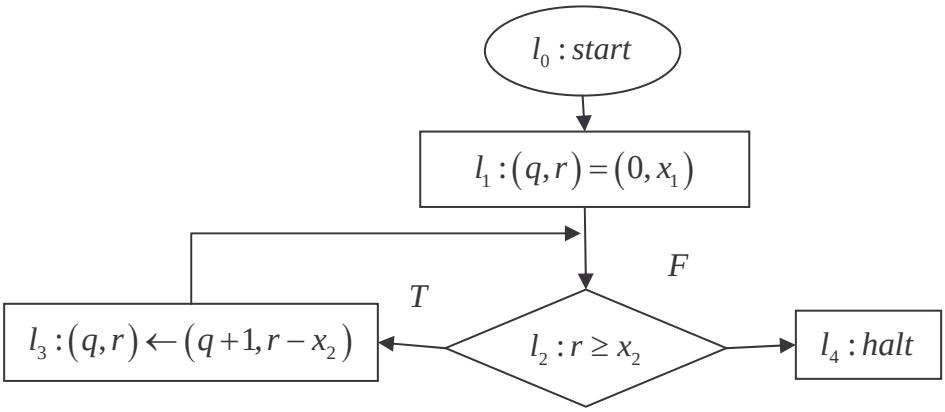
$$I_1(\bar{x}) = q_1(\bar{x}) \qquad\qquad I_{halt}(\bar{x}) = q_2(\bar{x})$$

3. לכל מסלול $\alpha = (l_i, l_j)$ שלא עובר דרך נקודות חתך אחרות נוכיח:

$$I_{li}(\bar{x}) \wedge R_\alpha(\bar{x}) \to I_{lj}[\bar{x} \leftarrow T_\alpha(\bar{x})]$$

(אם מתקיים תנאי ראשון על המשתנים בנקודה הראשונה וגם המסלול עביר אז יתקיים תנאי שני על הטרנספורמר של המסלול על המשתנים).

דוגמה:



ננסה להוכיח שבסוף התוכנית $x_1 = qx_2 + r \wedge r < x_2$

$$\{x_1 = X_1 \wedge x_2 = X_2 \wedge x_1 \geq 0 \wedge x_2 > 0\} P \{X_1 = qX_2 + r \wedge 0 \leq r < X_2 \wedge x_1 = X_1 \wedge x_2 = X_2\}$$

$$I_1 = q_1(\bar{x})$$
$$I_4 = q_2(\bar{x})$$
$$I_2 = (x_1 = qx_2 + r) \wedge r \geq 0 \wedge x_1 = X_1 \wedge x_2 = X_2$$

מסלול מ l_2 לעצמו:

$$\overbrace{(x_1 = x_2 q + r \wedge r \geq 0 \wedge x_1 = X_1 \wedge x_2 = X_2)}^{I_2(\bar{x})} \wedge \overbrace{(r \geq x_2)}^{R_\alpha} \rightarrow$$
$$\underbrace{I_2[\bar{x} \leftarrow (x_1, X_1, x_2, X_2, q, r \leftarrow x_1, X_1, x_2, X_2, q+1, r-x_2)]}_{I_2[\bar{x} \leftarrow T_\alpha(\bar{x})]}$$

$$x_1 = qx_2 + r \wedge x_1 = X_1 \wedge x_2 = X_2 \wedge r \geq 0 \wedge r \geq x_2$$
$$\rightarrow x_1 = \underbrace{(q+1)x_2 + r - x_2}_{=qx_2+r} \wedge \underbrace{x_1 = X_1}_{*} \wedge \underbrace{x_2 = X_2}_{*} \wedge \underbrace{r - x_2}_{*} \geq 0$$

* = נכון באופן טריוויאלי.

מסלול מ l_0 ל l_2

$$\overbrace{x_1 = X_1 \wedge x_2 = X_2 \wedge x_1 \geq 0 \wedge x_2 > 0}^{I_0(\bar{x})} \wedge \overbrace{True}^{R_\alpha(\bar{x})} \rightarrow I_2[\bar{x} \leftarrow (x_1, X_1, x_2, X_2, q, r \leftarrow x_1, X_1, x_2, X_2, 0, x_1)]$$

לפתור בבית...

<u>הוכחת נאותות</u> $(soundness)$: F – מערכת הוכחה של פלויד.

$\models \{q_1\} P \{q_2\}$ אז $\vdash_F \{q_1\} P \{q_2\}$

(אם ניתן להוכיח את הטענה במערכת ההוכחה, אז הטענה נכונה).

למה: אם $\vdash_F \{q_1\}P\{q_2\}$ אזי לכל חישוב π של P, שמתחיל ממצב σ_0 שמקיים: $\sigma_0 \models q_1(\bar{x})$, אם החישוב מגיע לנקודת חתך l' במצב σ' אזי $\sigma' \models I_{l'}(\bar{x})$

(זאת אומרת שאם ניתן במערכת ההוכחה להוכיח את $\{q_1\}P\{q_2\}$ אז כל חישוב שמתחיל ממצב σ_0 ומספק את תנאי ההתחלה, אם הוא מגיע לנקודת החתך במצב כלשהו, אז המצב החדש מספק את התנאי של נקודת החתך).

הוכחה באינדוקציה על מספר נקודות החתך ב π:

<u>בסיס</u>: $l' = l_0$, $\sigma_0 \models q_1(\bar{x})$ ולכן $\sigma' = \sigma_0$ ולכן $\sigma' \models q_1(\bar{x})$

$I_{l'}(\bar{x}) = q_1(\bar{x})$, מכאן ש $\sigma' \models I_{l'}(\bar{x})$.

<u>צעד</u>: $l_0 \to\to\to \ldots \to l_n \to l_{n+1}$

נתון: $I_n(\bar{x}) \wedge R_{n,n+1}(\bar{x}) \to I_{n+1}(\bar{x} \leftarrow T_{n,n+1}(\bar{x}))$ (מפלויד)

ע"פ הנחת האינדוקציה $\sigma_n \models I_n(\bar{x})$ וגם $\sigma_n \models R_{n,n+1}(\bar{x})$

(המצב מספק את I_n והמסלול ל l_{n+1} עביר)

לכן נסיק ש $\sigma_n \models I_{n+1}[\bar{x} \leftarrow T_{n,n+1}(\bar{x})]$. (משוואה מספר 1)

מה שאנחנו צריכים להוכיח זה: $\sigma_{n+1} \models I_{n+1}$.

אנחנו יודעים ש $\sigma_{n+1} = \sigma_n[\bar{x} \leftarrow T_{n,n+1}(\bar{x})]$. (משוואה מספר 2)

נסתמך על המשפט מתחשיב היחסים: $S[\bar{x} \leftarrow e] \models \varphi \leftrightarrow S \models \varphi[\bar{x} \leftarrow e]$

כאשר e הוא ביטוי כלשהו ו S מצב.

$\sigma_n[\bar{x} \leftarrow T_{n,n+1}(\bar{x})] \models I_{n+1}(\bar{x})$ (ע"פ המשפט ומשוואה מספר 1)

ולכן ע"פ משוואה מספר 2: $\sigma_{n+1} \models I_{n+1}$.

מש"ל!!!

בהינתן הלמה נוכיח נאותות:

π מסתיים במצב הסופי $(halt)$ שנסמנו ב σ_k.

מכיוון שבחרנו $I_{halt} = q_2(\bar{x})$ אזי לפי הלמה מתקיים $\sigma_k \models q_2(\bar{x})$