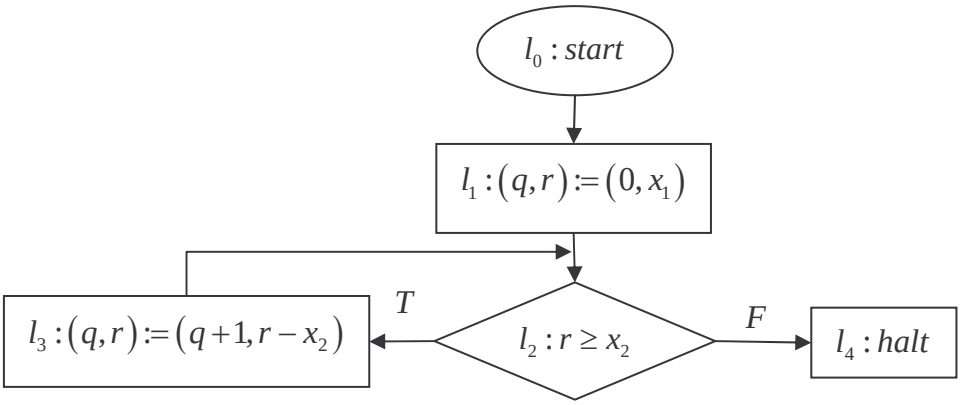
1. שפת מפרט – תחשיב היחסים.
2. שפת תכנות – Flow-chart.
3. כללי הוכחה.

<u>למת ההפרדה:</u>
לכל תוכנית P ומפרט $< q_1, q_2 >$ מתקיים $< q_1 > P < q_2 >$ (נכונות מלאה) אם ורק אם $\models < q_1 > p < true >$ (כל החישובים שמתחילים ב q_1 עוצרים) וגם $\models \{q_1\} P \{q_2\}$ (נכונות חלקית).

דוגמה: תוכנית חלוקה בשלמים

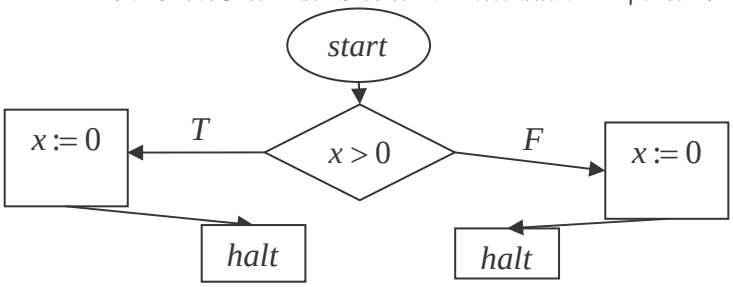


דוגמת הרצה: עבור $x_2 = 3$ $x_1 = 10$

q (מנה)	r (שארית)
0	10
1	7
2	4
3	1

<u>מסלול</u> בחישוב הזרימה: סדרה של צמתים עוקבים בחישוב הזרימה.
<u>מסלול מלא:</u> מסלול שמתחיל ב $start$ ומסתיים ב $halt$.
<u>חישוב של תוכנית:</u> סדרת מצבים שמתאימה למסלול מהצומת ההתחלתי l_0.
<u>חישוב מלא:</u> סדרת מצבים שמתאימה למסלול מלא.

<u>נסתכל רק על מסלולים ללא מעגלים</u>
צריך להראות שכל חישוב מלא (חסר מעגלים) שמספק את $q_1(\bar{x})$ מספק בסופו את $q_2(\bar{x})$.
נתון מסלול: $\tau = l_{i0}, l_{i1}, ..., l_{in}$.
נרצה לחשב:
1. בהינתן מצבו ההתחלתי נרצה לדעת את מצבו הסופי.
2. בהינתן מצבו ההתחלתי נרצה לדעת האם המסלול עביר.



עבור תוכנית זאת מתקיים: $\models < (x < 0), (x = 0) >$

בהינתן מסלול $\tau = l_{i0}, l_{i1}, ..., l_{in}$ נגדיר:

1. טרנספורמציית המצבים (state transformer) $T_\tau(\bar{x})$ על מסלול τ שמתחיל ממצב $\bar{x}$ $T_\tau(\bar{x})$ מתאר את המצב הסופי של התוכנית בעזרת המשתנים של תחילת התוכנית.

2. תנאי הישיגות (reachability condition) $R_\tau(\bar{x})$ - ביטוי שערכו True אם ורק אם τ הוא מסלול עביר עבור המצב ההתחלתי $\bar{x}$.

<u>משפט:</u> בהינתן מסלול סופי $\tau = l_{i0}, l_{i1}, ..., l_{ik}$ שמתחיל ממצב σ_0

א. המסלול עביר (כלומר l_{ik} ישיג מ l_{i0} לאורך המסלול τ) אם ורק אם $\sigma_0 \models R_\tau(\bar{x})$.

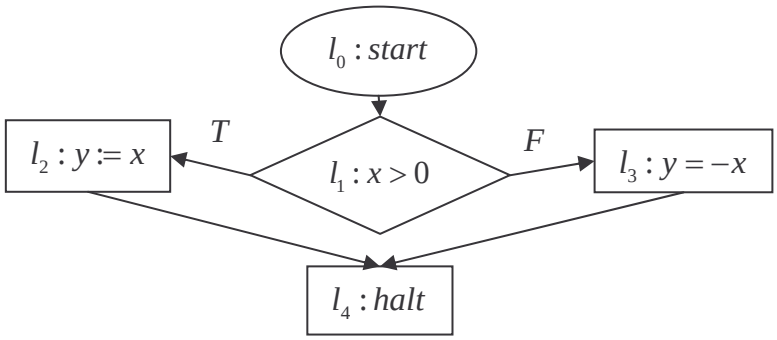
ב. אם המסלול מסתיים ב l_{ik} במצב σ_k אזי מתקיים ש $\sigma_k = \sigma_0[\bar{x} \leftarrow T_\tau(\bar{x})]$

לדוגמה: אם $T_\tau(x,y) = (x+y, y)$ וגם $\sigma_0(x,y) = (2,4)$

אז $\sigma_k(x,y) = (6,4)$

נחשב את $T_\tau(\bar{x})$ ואת $R_\tau(\bar{x})$ ע"י חישוב "אחורנית":

בהינתן מסלול $\tau = l_{i0}, l_{i1}, ..., l_{ik}$ נתחיל עם $T_\tau^k(\bar{x})$ ונסיים עם $T_\tau^0(\bar{x})$. $T_\tau(\bar{x}) = T_\tau^0(\bar{x})$



מסלול ימני $\tau = l_0, l_1, l_3, l_4$	מסלול שמאלי $\tau = l_0, l_1, l_2, l_4$
$l_0 : start$ $T_\tau^0(\bar{x}) = (x, -x)$	$l_0 : start$ $T_\tau^0(\bar{x}) = (x, x)$
$l_1 : x > 0$ $T_\tau^1(\bar{x}) = (x, -x)$	$l_1 : x > 0$ $T_\tau^1(\bar{x}) = (x, x)$
$l_3 : y := -x$ $T_\tau^2(\bar{x}) = (x, -x)$	$l_2 : y := x$ $T_\tau^2(\bar{x}) = (x, x)$
$l_4 : halt$ $T_\tau^3(\bar{x}) = (x, y)$	$l_4 : halt$ $T_\tau^3(\bar{x}) = (x, y)$
$T_\tau(\bar{x}) = T_\tau^0(\bar{x}) = (x, -x)$	$T_\tau(\bar{x}) = T_\tau^0(\bar{x}) = (x, x)$
$l_0 : start$ $R_\tau^0(x,y) = x \le 0$	$l_0 : start$ $R_\tau^0(x,y) = x > 0$
$l_1 : x > 0$ $R_\tau^1(x,y) = x \le 0$	$l_1 : x > 0$ $R_\tau^1(x,y) = x > 0$
$l_3 : y := -x$ $R_\tau^2(x,y) = True[y \leftarrow -x] = True$	$l_2 : y := x$ $R_\tau^2(x,y) = True[y \leftarrow x] = True$
$l_4 : halt$ $R_\tau^3(x,y) = True$	$l_4 : halt$ $R_\tau^3(x,y) = True$
$R_\tau(\bar{x}) = R_\tau^0(x,y) = x \le 0$	$R_\tau(\bar{x}) = R_\tau^0(x,y) = x > 0$

הגדרה אינדוקטיבית של $T_\tau(\bar{x})$ ושל $R_\tau(\bar{x})$

בסיס ההגדרה: $T_\tau^k(\bar{x}) = (\bar{x})$, $R_\tau^k(\bar{x}) = True$

צעד האינדוקציה: בהינתן T_τ^{k+1}, R_τ^{k+1}

א. הצבה: $\bar{x} := \bar{e}$:

$$R_\tau^k(\bar{x}) = R_\tau^{k+1}[\bar{x} \leftarrow \bar{e}]$$
$$T_\tau^k(\bar{x}) = T_\tau^{k+1}[\bar{x} \leftarrow \bar{e}]$$

ב. תנאי : $b(\bar{x})$: אם זה הצד החיובי של התנאי:

$$R_\tau^k(\bar{x}) = R_\tau^{k+1}(\bar{x}) \wedge b(\bar{x})$$
$$T_\tau^k(\bar{x}) = T_\tau^{k+1}(\bar{x})$$

אם זה הצד השלילי של התנאי:

$$R_\tau^k(\bar{x}) = R_\tau^{k+1}(\bar{x}) \wedge \neg b(\bar{x})$$
$$T_\tau^k(\bar{x}) = T_\tau^{k+1}(\bar{x})$$

כלל להוכחת נכונות עבור תוכניות ללא מעגלים:

תוכנית ללא מעגלים P ביחס למפרט $< q_1, q_2 >$ (כלומר $< q_1 > P < q_2 >$) נכונה אם ורק אם לכל מסלול מלא τ של P מתקיים: $q_1(\bar{x}) \wedge R_\tau(\bar{x}) \rightarrow q_2(T_\tau(\bar{x}))$

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