ראינו בהרצאה הוכחה של נכונות מלאה $\langle q_1\rangle P\langle q_2\rangle$

ראינו את למת ההפרדה: $\langle q_1\rangle P\langle q_2\rangle \Leftrightarrow \langle q_1\rangle P\langle true\rangle \wedge \{q_1\} P\{q_2\}$ תוכנית היא נכונה באופן מלא על פי $\langle q_1\rangle P\langle q_2\rangle$ אם כל חישוב שמתחיל כשהוא מספק את התנאי q_1 עוצר, ובנוסף אם הוא עוצר (מה שתמיד קורה), אז כשהוא עוצר הוא מספק את q_2.

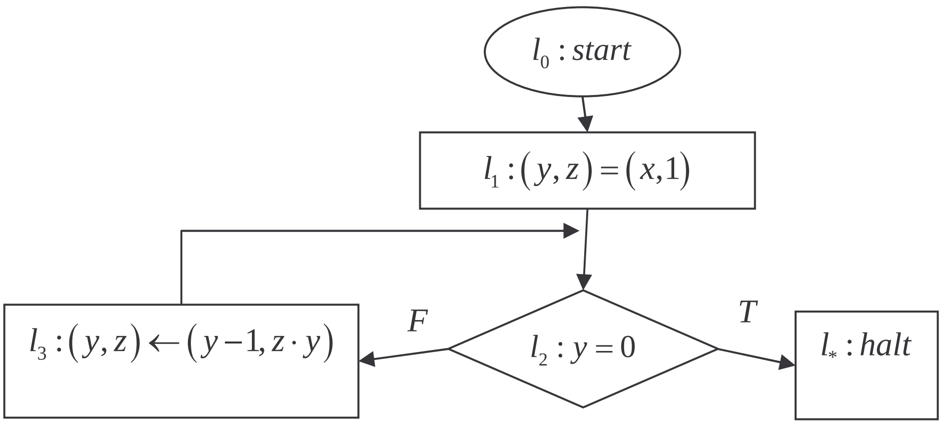
כלל F^* להוכחת עצירה: $\langle q_1(\overline{x})\rangle P\langle True\rangle$

1. בחר קבוצה מבוססת היטב עם סדר חלקי או מלא $(W,<)$. (למשל מספרים טבעיים)
2. בחר קבוצת נקודות חתך C כמו (כמו ב F)
3. לכל נקודת חתך $l\in C$, התאם טענה אינדוקטיבית, $I_l(\overline{x},w)$ כאשר w משתנה שתחומו W.
4. הוכח את תנאי הנכונות הבאים:

א. $\forall\overline{x}\left(q_1(\overline{x})\right)\rightarrow\exists_w I_{Start}(\overline{x},w) \qquad (Init)$

ב. עבור כל מסלול בסיסי $\alpha=(l,l')$ ללא נקודות חתך באמצע:

$$\forall\overline{x}\forall w I_l(\overline{x},w)\wedge R_\alpha(\overline{x},w)\rightarrow\exists \underbrace{w'}_{\in W}\left(w'<w\wedge I_{l'}\left(T_a(\overline{x}),w'\right)\right) \qquad (Dec)$$



תוכנית שמחשבת עצרת. רוצים להוכיח נכונות מלאה.

צריך להראות:

$$\langle x\geq 0\rangle P\langle True\rangle\wedge\underbrace{\{x\geq 0\}P\{z=x!\}}_{*}\Leftrightarrow\langle z\geq 0\rangle P\langle z=x!\rangle$$

* - הוכחנו בתרגול הקודם.

1. **נבחר את הקבוצה** $(\mathbb{N},<)$.
2. **נבחר** $C=\{l_0,l_2,l_*\}$.
3. $I_{l_0}(x,y,z,w)=((w=x+2)\wedge(x\geq 0))$

$I_{l_2}(x,y,z,w)=((w=y+1)\wedge(y\geq 0))$

$I_{l_*}(x,y,z,w)=(w=0)$

$\alpha=l_0,l_1,l_2 \qquad \beta=l_2,l_3,l_2 \qquad \gamma=l_2,l_*$

4. הגדרת המסלולים הבסיסיים וחישוב R ו- T עבורם מופיעים בדף מהתרגול הקודם.

יש להוכיח:

(INIT) $\forall(x,y,z)\Big[\overset{q_1(\overline{x})}{(x\ge 0)} \to \exists w[\overset{I_{l_0}}{(w=x+2)\wedge(x\ge 0)}]\Big]$ ✓

(DEC) α: $\forall(x,y,z,w)\Big[(\overset{I_{l_0}}{(w=x+2)\wedge(x\ge 0)}\wedge \overset{R_\alpha}{\mathit{true}}) \to$
$\exists w'[(w'<w)\wedge(\overset{I_{l2}}{(w'=y+1)\wedge(y\ge 0)})\overset{T_\alpha}{[(x,y,z)\leftarrow(x,x,1)]}]\Big]$

$\equiv \forall(x,y,z,w)\Big[((w=x+2)\wedge(x\ge 0)) \to$
$\exists w'[(w'<w)\wedge((w'=x+1)\wedge(x\ge 0))]\Big]$ ✓

R_β, עדיף לרשום $\neg(y=0)$

β: $\forall(x,y,z,w)\Big[(\overset{I_{l2}}{(w=y+1)\wedge(y\ge 0)}\wedge(y\ne 0)) \to$
$\exists w'[(w'<w)\wedge((w'=y+1)\wedge(y\ge 0))[(x,y,z)\leftarrow(x,y-1,z\cdot y)]]\Big]$

$\equiv \forall(x,y,z,w)\Big[((w=y+1)\wedge(y>0)) \to$
$\exists w'[(w'<w)\wedge((w'=y)\wedge(y-1\ge 0))]\Big]$ ✓

γ: $\forall(x,y,z,w)\Big[((w=y+1)\wedge(y\ge 0)\wedge(y=0)) \to$
$\exists w'[(w'<w)\wedge(w'=0)]\Big]$ ✓

הערות:

1. כשמוכיחים טענות נכונות בתרגילי בית לא מספיק לכתוב ✓ (יש להוסיף נימוק קצר).
2. בחרנו את y+1 להיות הפרמטר כיוון שהוא יורד בכל סיבוב בלולאה.
לא תמיד זה פשוט כל כך. למשל, אם הערך של y היה עולה והיה ידוע שאינו יכול לעבור חסם c אז היינו יכולים לבחור w=c-y שהיה יורד.
3. חשוב לשים לב שבצעד הראשון, מ- l_0 ל- l_2 הערך של y לא יורד, לכן התחלנו עם w=x+2. יש להקפיד על כך שבכל צעד תהיה ירידה.

<u>שאלה:</u>

נתונה תוכנית P בשפת תרשימי הזרימה PLF ונתונות טענות q_1, q_2 מסדר ראשון מעל משתני התוכנית.
נאמר ש $P \models q_1 \rightarrow GLOBALLY q_2$ אם לכל חישוב של P, אם הוא מתחיל ממצב שמספק את q_1 אז כל מצב על מסלול החישוב מספק את q_2.
הציעו כלל נאות ושלם ככל האפשר להוכחת $P \models q_1 \rightarrow GLOBALLY q_2$. נמקו את נאותות ושלמות הכלל.

<u>פתרון:</u>

1. בחר את כל צמתי התוכנית כנקודות חתך.
2. לכל תווית הצמד טענה אינדוקטיבית $I_l(\overline{x})$ כאשר $I_{l_0} = q_1(\overline{x})$ ו $I_{l_*}(\overline{x}) = true$
3. הוכח: $\forall \overline{x}\left[q_1(\overline{x}) \rightarrow q_2(\overline{x})\right]$
4. לכל מסלול בסיסי $\tau = l, l'$ הוכח:

$$\forall \overline{x}\left[I_l \wedge R_{l,l'} \wedge q_2 \rightarrow I_{l'}(\overline{x}) \wedge q_2\left[\overline{x} \leftarrow T_{l,l'}(\overline{x})\right]\right]$$

<u>שאלה:</u>
נרחיב את השפה PLF ע"י כך שנוסיף לה את הפקודה $Case(x)$ כאשר x הוא משתנה כלשהו של התוכנית. לצומת $Case(x)$ יש מספר בנים סופי גדול מאפס. בן אחד יסומן ב $defualt$.
התנאים לא בהכרח זרים ולא בהכרח משלימים.
אם אף אחד מהתנאים לא מתאימים, בוחרים בבן ה $defualt$.
אם כמה תנאים מתאימים - בוחרים באופן אי דטרמיניסטי.
אם רק אחד מהתנאים מתקיימים, עוברים לבן המתאים לו.

$$T_\tau^m(\overline{x}) = T_\tau^{m+1}(\overline{x})$$

$$R_\tau^m(\overline{x}) = R_\tau^{m+1}(\overline{x}) \wedge b_i \qquad b_i$$

(בשביל לעבור להבן ה i צריך שהתנאי עבורו יתקיים, לא חובה שהתנאים עבור שאר הבנים לא יתקיימו)

$$R_\tau^m(\overline{x}) = R_\tau^{m+1}(\overline{x}) \wedge \neg b_1 \wedge \neg b_2 \wedge \neg b_3 \ldots \wedge \neg b_n \qquad default$$