כלל F להוכחת נכונות חלקית (FLOYD)
1. מוצאים נקודות חתך, לפחות אחת בכל לולאה.
2. מתאימים אינווריאנטה I_l לכל נקודת חתך.
3. עבור כל מסלול α בין שתי נקודות חתך "רציפות" מוכיחים:
$$I_l(\bar{x}) \wedge R_\alpha(\bar{x}) \to I_{l'}(\bar{x} \leftarrow T_\alpha(\bar{x}))$$

הוכחנו נאותות של F, כלומר, שאם $\vdash_F \{q_1\} P \{q_2\}$ אז $\models \{q_1\} P \{q_2\}$

שלמות של F:
צ"ל שאם $\models \{q_1\} P \{q_2\}$ אז $\vdash_F \{q_1\} P \{q_2\}$
כלומר קיימות נקודות חתך ואינווריאנטות בעזרתן ניתן להוכיח נכונות.

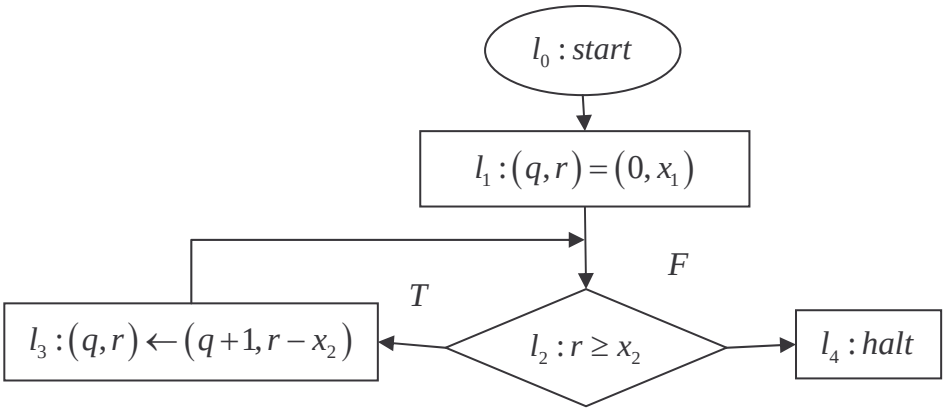
כלל F^* להוכחת עצירה:
קבוצה מבוססת היטב: $well-founded-set$:
קבוצה עם יחס סדר (יתכן סדר חלקי) $(W,>)$ הינה מבוססת היטב אם לא קיימת ב W סדרה יורדת אינסופית. כלומר לא קיימת סדרה $w_0 > w_1 > w_2 \ldots$ כך ש $\forall i : w_i \in W$.

דוגמאות:
1. המספרים הטבעיים עם היחס "גדול מ..." ('>') - קבוצה מבוססת היטב.
2. המספרים הממשיים החיוביים עם היחס "גדול מ..." - לא קבוצה מבוססת היטב - תמיד אפשר למצוא מספר חיובי קטן יותר.
3. מחרוזת עם היחס "רישא ממש" - סדרה מבוססת היטב - אם אורך המילה הראשונה הוא n אז בסדרה יש לכל היותר $n+1$ מילים.
4. נתונה קבוצה סופית A. קבוצת החזקה $P(A)$ ויחס הכלה. $A_1 \subset A_2 \subset A_3 \ldots$ - סדרה מבוססת היטב, כי תמיד נעצור אחרי שנגיע ל $P(A)$. לכל היותר יש $|A|+1$ איברים בסדרה.

כלל F^* להוכחת עצירה: $\langle q_1 \rangle P \langle True \rangle$
1. בחר קבוצה מבוססת היטב עם סדר חלקי או מלא $(W,<)$. (למשל מספרים טבעיים)
2. בחר נקודות חתך כמו (כמו ב F)
3. לכל נקודת חתך, התאם טענה אינדוקטיבית, $I(\bar{y},w)$ כאשר w משתנה שתחומו W.
4. הוכח את תנאי הנכונות הבאים:
   א. $\forall \bar{x}(q_1(\bar{x})) \to \exists_w I_{Start}(\bar{x},w) \qquad (Init)$
   ב. עבור כל מסלול $\alpha = (l,l')$ ללא נקודות חתך באמצע:
$$(Dec) \qquad \forall \bar{x} \forall w I_l(\bar{x},w) \wedge R_\alpha(\bar{x},w) \to \exists \underbrace{w'}_{\in W} w' < w \wedge I_{l'}(T_a(\bar{x}),w')$$

בצורה כזאת נוכיח $\langle q_1 \rangle P \langle True \rangle$ - אם תנאי ההתחלה מתקיים, אז התוכנית עוצרת.
אם היינו רוצים גם להוכיח נכונות "באותה הזדמנות" היינו צריכים להוכיח:
$\forall \bar{x} \forall w I_{halt}(\bar{x},w) \to q_2(\bar{x})$ (האינווריאנטה של נקודת העצירה מספקת את תנאי הסיום)

דוגמה:



תוכנית שמבצעת חילוק (מההרצאה הקודמת).

ננסה קודם כל $I_{l_2} : (w = r)$. $(W = \mathbb{N})$

מסלול מ l_2 לעצמו, נסמנו ב α:

צ"ל: $$\forall \bar{x} \forall w \left(\underbrace{(w = r)}_{I_{l_2}} \wedge \underbrace{r \geq x_2}_{R_\alpha} \right) \rightarrow \left(\exists w' : w' < w \wedge \underbrace{\left(w' = r\left[(q,r) \leftarrow (q+1, r-x_2) \right] \right)}_{I_{l_2}\left(T_\alpha(\bar{x}), w'\right)} \right)$$

$$w = r \wedge r \geq x_2 \rightarrow \exists w' : w' < w \wedge w' = r - x_2$$

נבחר $w' = r - x_2$

$$w = r \wedge r \geq x_2 \rightarrow \underbrace{r - x_2 < w}_{*} \wedge \underbrace{r - x_2 = r - x_2}_{True}$$

* נכון רק אם ידוע ש $x_2 > 0$ ולכן אי אפשר להוכיח את הטענה.

ננסה במקום זאת לבחור אינווריאנטה: $I_{l_2} : (x_2 > 0 \wedge w = r)$

צ"ל:

$$\forall \bar{x} \forall w \left(\underbrace{(x_2 > 0 \wedge w = r)}_{I_{l_2}} \wedge \underbrace{r \geq x_2}_{R_\alpha} \right) \rightarrow \left(\exists w' : w' < w \wedge \underbrace{\left(x_2 > 0 \wedge w' = r\left[(q,r) \leftarrow (q+1, r-x_2) \right] \right)}_{I_{l_2}\left(T_\alpha(\bar{x}), w'\right)} \right)$$

$$x_2 > 0 \wedge w = r \wedge r \geq x_2 \rightarrow \exists w' : x_2 > 0 \wedge w' < w \wedge w' = r - x_2$$

נבחר $w' = r - x_2$

$$x_2 > 0 \wedge w = r \wedge r \geq x_2 \rightarrow \underbrace{x_2 > 0}_{True} \wedge \underbrace{r - x_2 < w}_{True} \wedge \underbrace{r - x_2 = r - x_2}_{True}$$ - נכון באופן טריויאלי!

נבחר כעת אינווריאנטה עבור START: $I_{Start} : (x_2 > 0 \wedge w = x_1 + 1)$

צ"ל: $$\forall \bar{x} \left(\underbrace{x_1 \geq 0 \wedge x_2 > 0}_{q_1(\bar{x})} \right) \rightarrow \exists w \left(x_2 > 0 \wedge w = x_1 + 1 \right) \qquad (Init)$$

נבחר $w = x_1 + 1$ וזה יתקיים באופן טריוויאלי.

נשאר להוכיח עבור המסלולים $\gamma = (l_2, l_4)$, $\beta = (l_0, l_2)$ (בבית)

נוכיח את נאותות הכלל F^*:
בהוכחת הכלל F השתמשנו בלמה שאומרת (באופן לא פורמאלי) שאם התחלנו עם מצב σ שמספק את I_{Start} אזי σ_k בנקודת חיתוך l_k מספק את I_{l_k}.

ניסוח הלמה עבור F^*:
אם $\vdash_{F^*} \langle q_1 \rangle P \langle True \rangle$ אזי לכל חישוב π של P שמתחיל מ $Start$ במצב σ כך ש $\sigma \models q_1(\overline{x})$,
אם החישוב מגיע לנקודה l' במצב σ' אז קיים w' כך ש $\sigma' \models I_{l'}(\overline{x}, w)$.
(זאת אומרת שאם ניתן להוכיח תחת F^* שהתוכנית עוצרת אם קיימה את תנאי ההתחלה, אז כל חישוב שמתחיל מההתחלה ומספק את תנאי ההתחלה, אם הוא מגיע לנקודה כלשהי, אז המצב החדש מספק את האינווריאנטה בנקודה).

הוכחה של הלמה: דומה מאוד להוכחה של הלמה עבור F.
נותר להוכיח: אם לנקודות חתך על החישוב π מותאמים ערכים $v_0, v_1, \ldots$ אזי מתקיים ש
$v_0 > v_1 > v_2 \ldots$
ההוכחה באינדוקציה על מספר נקודות החתך שבהן עבר π.
<u>בסיס:</u> נקודת חתך אחת l_0 בהנחה ש π בתחילתו מספק את $q_1(\overline{x})$. ניתן לבחור ערך כלשהו עבור w, ונקרא לערך הזה v_0.
<u>צעד האינדוקציה:</u> נניח $\sigma_i \models I_{l_i}(\overline{x} > v_i)$ והחישוב ממשיך ל l_{i+1}.
אזי: $\sigma_i \models R_{(l_i, l_{i+1})}(\overline{x})$ כי החישוב עביר. מכיוון שהוכחנו את DEC אזי
$$\sigma_i \models \exists w' \left[w' \in W \wedge I_{l_{i+1}}\left(T_\alpha(\overline{x}), w'\right) \right]$$