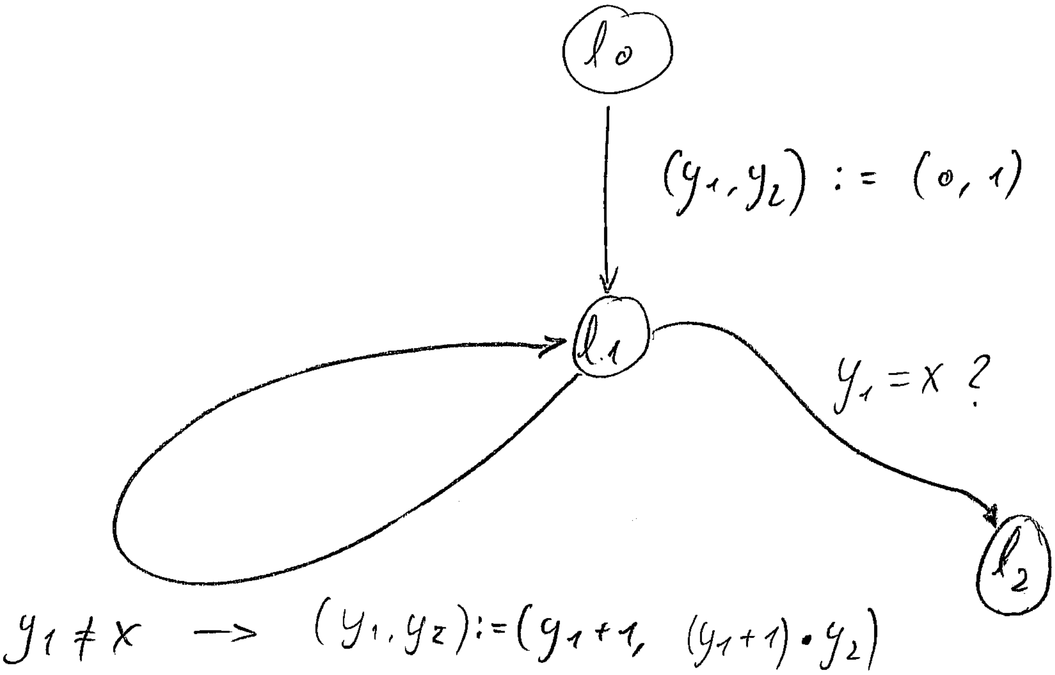
(1)

ex-1

תרגיל 1 - פתרון

I) 1. הסבה לגרף מסגרים:



2. נק' חיתוך: $C = \{l_0, l_1, l_2\}$

3. מסלולי אימות: $P = \{\pi_{01}, \pi_{11}, \pi_{12}\}$

4. מכיוון שכל מסלולי האימות הם במקרה זה קשתות בגרף

$G_{01}: (y_1, y_2) := (0, 1)$

$G_{11}: y_1 \neq x \rightarrow (y_1, y_2) := (y_1+1, (y_1+1) \cdot y_2)$

$G_{12}: y_1 = x\ ?$

---

5. הטענות לנק' החיתוך:

$\phi_0: \quad x \geqslant 0$

$\phi_1: \quad y_1 \leq x \wedge y_2 = y_1!$

$\phi_2: \quad y_1 = x \wedge y_2 = x!$

(2)

ex1

6. לכל מסלול אימות π שמחבר בין נק' חיתוך l_i לנק' חיתוך l_j צריך לבנות תנאי אימות:

$$VC_\pi : \varphi_i(V) \wedge C_\pi \rightarrow \varphi_j(f_\pi(V))$$

assertion לנק' חיתוך l_i

מצב כל המשתנים במסלול π

תנאי כניסה למסלול

assertion לנק' חיתוך l_j

מצב כל המשתנים בסוף π

לפי האימות:

$$VC_{01} : x \geq 0 \rightarrow 0 \leq x \wedge 1 = 0!$$

$$VC_{11} : y_1 \leq x \wedge y_2 = y_1! \wedge y_1 \neq x \rightarrow (y_1+1) \leq x \wedge ((y_1+1)\cdot y_2) = (y_1+1)!$$

$$VC_{12} : y_1 \leq x \wedge y_2 = y_1! \wedge y_1 = x \rightarrow y_2 = x!$$

נפשט:

$$VC_{01} : x \geq 0 \rightarrow x \geq 0 \wedge true \iff true$$

$$VC_{11} : y_1 < x \wedge y_2 = y_1! \rightarrow (y_1+1) \leq x \wedge (y_1+1)\cdot y_2 = (y_1+1)!$$

$$\iff true$$

מכיוון ש:

$$y_1 < x \rightarrow (y_1+1) \leq x$$

$$y_2 = y_1! \rightarrow (y_1+1) y_2 = (y_1+1) y_1! = (y_1+1)!$$

$$VC_{12} : y_2 = y_1! \wedge y_1 = x \rightarrow y_2 = x! \iff true$$

3

ex1

הראינו כי $N = \{\phi_0, \phi_1, \phi_2\}$ הינו רשת טענות אינדוקטיבית, לפיכך התוכנית נכונה חלקית ביחס לספציפיקציה: $(\phi_0, \phi_2) = (\phi, \psi) = (x \geq 0, y_2 = x!)$

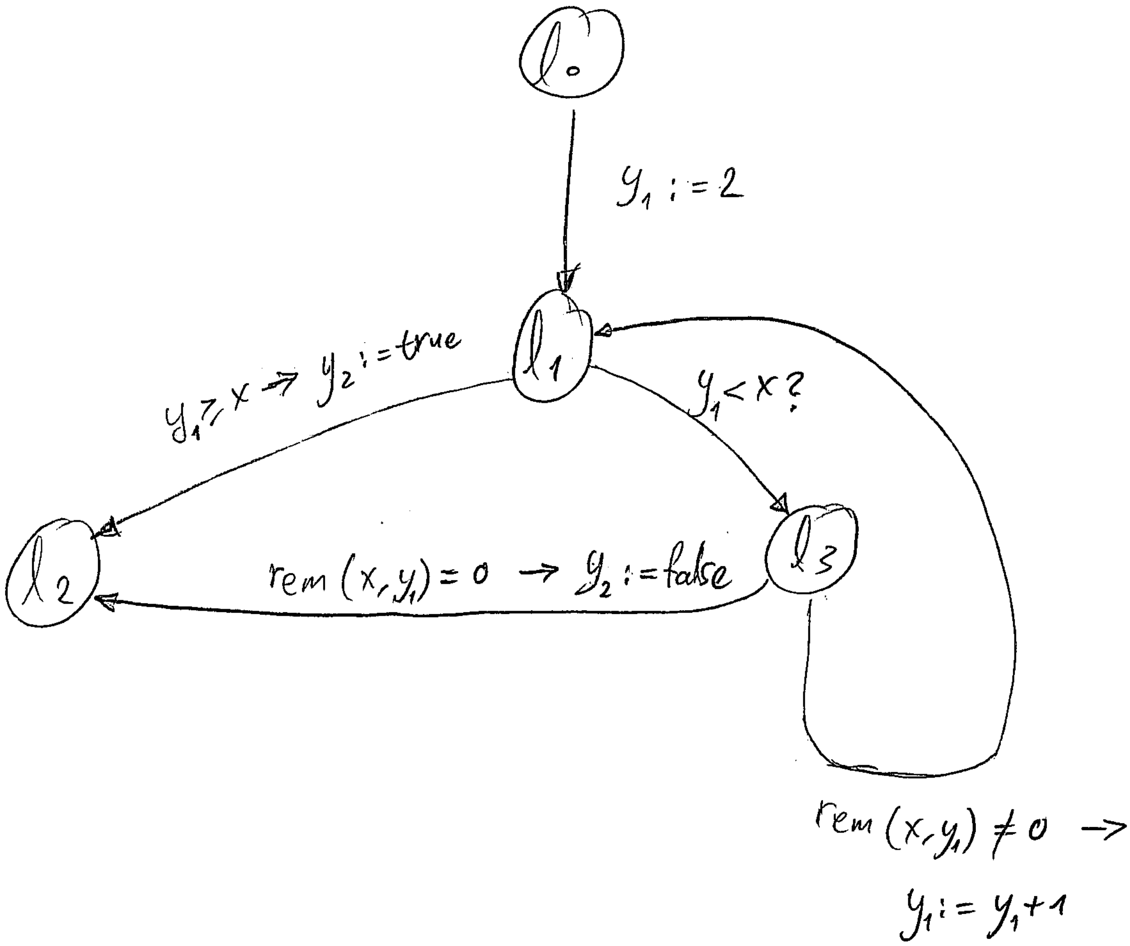
$\blacksquare$

(4)

ex1

(II

1.



2. ק' חיתוך:

$$C = \{l_0, l_1, l_2\}$$

3. מסלולי אימות:

$$P = \{\pi_{01}, \pi_{12}, \pi'_{12}, \pi_{11}\}$$

π_{01} : l_0, l_1

π_{12} : l_1, l_2

π'_{12} : l_1, l_3, l_2

π_{11} : l_1, l_3, l_1

4. Summary Guarded Cmds:

G_{01} : $y_1 := 2$

G_{12} : $y_1 \geq x \to y_2 := true$

G'_{12} : $y_1 < x \wedge rem(x, y_1) = 0 \to y_2 := false$

G_{11} : $y_1 < x \wedge rem(x, y_1) \neq 0 \to y_1 := y_1 + 1$

(5)

ex1

5. הצעה לנק' החתך:

$\phi_0: \quad x \geq 2$

$\phi_1: \quad \forall k_{2 \leq k < y_1} (rem(x,k) \neq 0) \wedge 2 \leq y_1 \leq X$

$\phi_2: \quad y_2 = \underbrace{\forall k_{2 \leq k < X} (rem(x,k) \neq 0)}_{\text{המשמעות של להיות ראשוני}}$

6. נוכיח נכונות חלקית - נבדוק את כל תנאי האימות ונראה כי מתקיימים.

$$VC_{01}: X \geq 2 \rightarrow \underbrace{\forall k_{2 \leq k < 2} (rem(x,k) \neq 0)}_{\text{מתקיים באופן ריק}} \wedge \underbrace{2 \leq 2 \leq X}_{\text{מתקיים}}$$

$$\Updownarrow$$

$$true$$

לכן תנאי האימות מתקיים למסלול π_{01}

$$VC_{12}: \forall k_{2 \leq k < y_1} (rem(x,k) \neq 0) \wedge \overbrace{2 \leq y_1 \leq X \wedge y_1 \geq X}^{y_1 = X} \rightarrow$$

$$\forall k_{2 \leq k < X} (rem(x,k) \neq 0) = true$$

$$\Updownarrow$$

$$\forall k_{2 \leq k < X} (rem(x,k) \neq 0) \rightarrow \forall k_{2 \leq k < X} (rem(x,k) \neq 0)$$

$$\Updownarrow$$

$$true$$

לכן תנאי האימות למסלול π_{12} מתקיים.

(6)
ex1

$$VC'_{12}: \forall k_{2\le k<y_1}(rem(x,k)\neq 0) \wedge 2\le y_1\le x \wedge y_1<x \wedge$$

$$rem(x,y_1)=0 \rightarrow$$

$$\forall k_{2\le k<x}(rem(x,k)\neq 0) = false$$

$$\Updownarrow$$

$$\forall k_{2\le k<y_1}(rem(x,k)\neq 0) \wedge 2\le y_1<x \wedge rem(x,y_1)=0 \rightarrow$$

$$\exists k_{2\le k<x}(rem(x,k)=0)$$

$$\Updownarrow$$

true

לכן תנאי האימות מתקיימים למסלול π'_{12}.

$$VC_{11}: \forall k_{2\le k<y_1}(rem(x,k)\neq 0) \wedge 2\le y_1\le x \wedge y_1<x \wedge$$

$$rem(x,y_1)\neq 0 \rightarrow$$

$$\forall k_{2\le k<y_1+1}(rem(x,k)\neq 0) \wedge 2\le y_1+1\le x$$

$$\Updownarrow$$

$$\forall k_{2\le k<y_1+1}(rem(x,k)\neq 0) \wedge 2\le y_1<x \rightarrow$$

$$\forall k_{2\le k<y_1+1}(rem(x,k)\neq 0) \wedge 2\le y_1+1\le x$$

$$\Updownarrow$$

true

לכן תנאי האימות מתקיימים למסלול π_{11}.

(7)

ex1

הראינו כי $N=\{\phi_0,\phi_1,\phi_2\}$ היא רשת טענות אינדוקטיביות

ולכן התוכנית נכונה חלקית ביחס למפרט: $(\phi_0,\phi_2)=(\phi,\psi)$.

III)

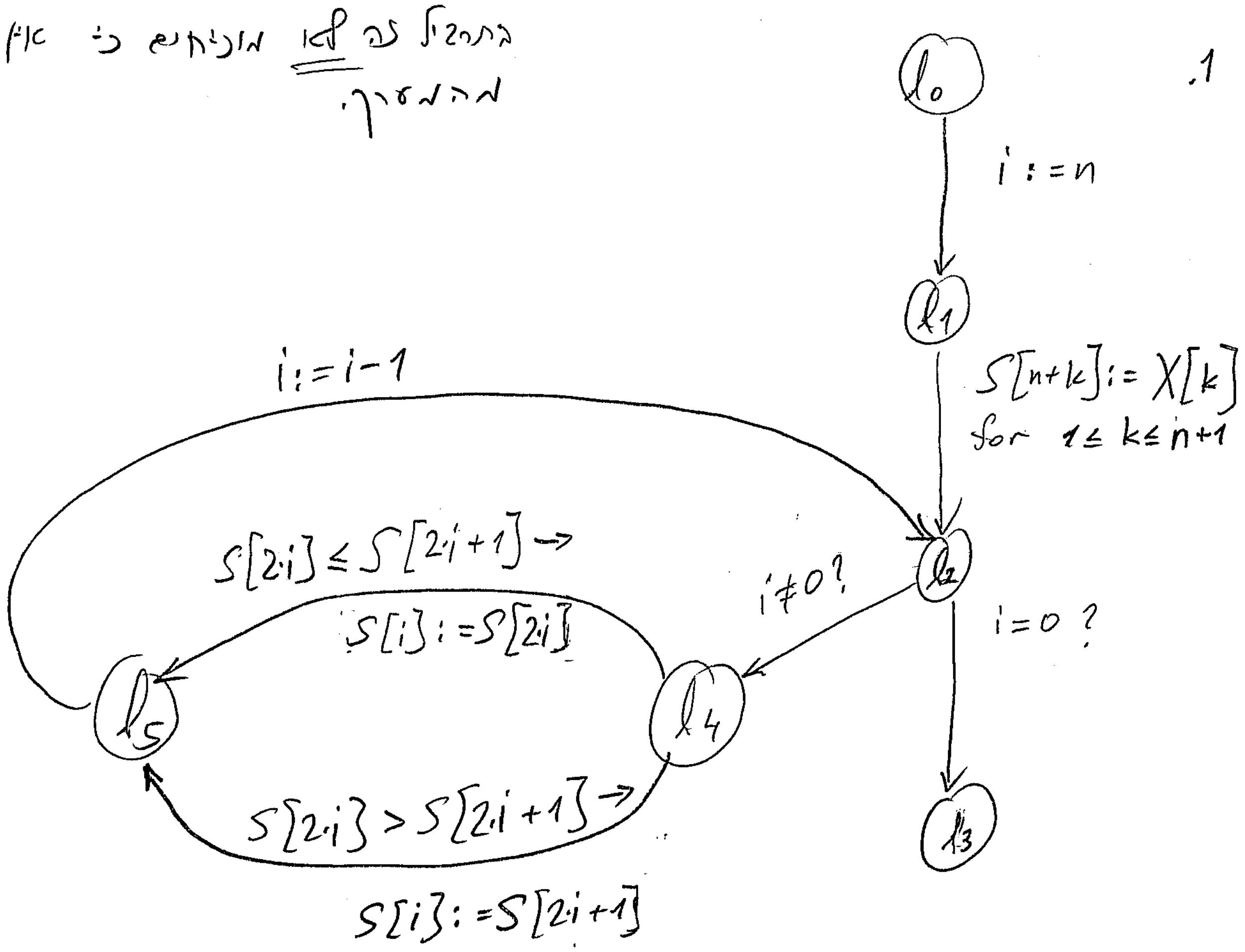
הפקודה: $\boxed{\begin{array}{l} S[n+k] \leftarrow X[k] \\ \text{for } 1\le k\le n+1 \end{array}}$ מבצעת רצף של

$k+1$ השמות. נמשיך להשתמש בקיצור זה. בנוסף, נשתמש

במערכים בצורה הרגילה למרות שלא הוגדרו פורמלית.

בתרגיל זה <u>לא</u> מניחים כי אין חריגה מהמערך.

1.



8

ex-1

2. קב' חתך :

$$C = \{l_0, l_2, l_3\}$$

3. מסלולי בסיס :

$$P = \{\pi_{02}, \pi_{22}, \pi_{22}', \pi_{23}\}$$

$\pi_{02} : l_0, l_2$

$\pi_{22} : l_2, l_4, l_5, l_2$ — בקשת העליונה בתרשים, עם תנאי ה- $\leq$.

$\pi_{22}' : l_2, l_4, l_5, l_2$ — בקשת התחתונה, עם תנאי ה- $>$

$\pi_{23} : l_2, l_3$

4. Summary Guarded Cmds :

G_{02} : $i := n$, $S[n+k] := X[k]$ for $1 \leq k \leq n+1$

G_{22} : $i \neq 0 \wedge S[2i] \leq S[2i+1] \rightarrow (S[i], i) := (S[2i], i-1)$

G_{22}' : $i \neq 0 \wedge S[2i] > S[2i+1] \rightarrow (S[i], i) := (S[2i+1], i-1)$

G_{23} : $i = 0$?

5. נשים לב כי התוכנית שומרת על האינווריאנטה הבאה ב-l_2:

$$\varphi_{21}: \quad \exists_{i<j\le 2i+1} j \quad \forall_{i<k\le 2n+1} k \quad S[j] \le S[k]$$

כלומר, האיבר המינימלי במערך תמיד נמצא בין $i+1$ ל- $2i+1$.
כאשר $i=0$, מתקבל כי $S[1]$ הוא המינימלי ב- S.

בנוסף, עלינו להראות כי S מכיל את כל איברי X ורק את איברי X, כלומר:

$$\varphi_{22}: \quad \forall_{i<j\le 2n+1} j \quad \exists_{1\le k\le n+1} k \quad S[j] = X[k]$$ רק איברי X:

$$\varphi_{23} \quad \forall_{1\le k\le n+1} k \quad \exists_{i<j\le 2n+1} j \quad S[j] = X[k]$$ כל איברי X:

עתה נצמיד את הטענות לפי החיתוך:

$\varphi_0: \quad n \ge 0$

$\varphi_2: \quad \varphi_{21} \wedge \varphi_{22} \wedge \varphi_{23}$

$\varphi_3: \quad \varphi_2 \wedge i = 0$

6. נוכיח נכונות חלקית ע"י כך שנראה כי כל טענות האימות מתקיימות.

VC_{02} : $n \geq 0 \rightarrow \phi_2(f_{\pi_{02}}(S,i))$

$$\Updownarrow$$

$$n \geq 0 \rightarrow \phi_2\Big(i=n,\ \underset{1 \leq k \leq n+1}{S[n+k] = X[k]}\Big) \quad (*)$$

$$\Updownarrow$$

$$n \geq 0 \rightarrow \Big(\overbrace{\underset{n<j\leq 2n+1}{\exists j} \ \underset{n<k\leq 2n+1}{\forall k} \ S[j] \leq S[k]}^{(\text{א})} \ \wedge$$

$$\overbrace{\underset{n<j\leq 2n+1}{\forall j} \ \underset{1\leq k\leq n+1}{\exists k} \ S[j] = X[k]}^{(\text{ב})} \ \wedge$$

$$\overbrace{\underset{1\leq k\leq n+1}{\forall k} \ \underset{n<j\leq 2n+1}{\exists j} \ S[j] = X[k]}^{(\text{ג})} \Big)$$

(א) בוודאי מתקיים כי למערך X המועתק ל- $S[n+1],\dots,S[2n+1]$ מוכרח להיות איבר מינימלי (אולי יותר מאחד).

(ב) ו-(ג) מתקיימים כי:

$$\underset{n<j\leq 2n+1}{\forall j} \ S[j] = X[j-n]$$

$$\Updownarrow$$

$$\underset{1\leq j\leq n+1}{\forall j} \ S[j+n] = X[j]$$

אשר מקיים לפי (*).

ex-1

$$VC_{22}: \quad \phi_2(S,i) \wedge C_{\pi_{22}}(S,i) \rightarrow \phi_2(f_{\pi_{22}}(S,i))$$

$$\Updownarrow$$

ⓐ $\exists_{i<j\leq 2i+1} j \ \forall_{i<k\leq 2n+1} k \quad S[j] \leq S[k] \quad \wedge$

ⓑ $\forall_{i<j\leq 2n+1} j \ \exists_{1\leq k\leq n+1} k \quad S[j] = X[k] \quad \wedge$

ⓒ $\forall_{1\leq k\leq n+1} k \ \exists_{i<j\leq 2n+1} j \quad S[j] = X[k] \quad \wedge$

$i \neq 0 \ \wedge \ S[2i] \leq S[2i+1] \longrightarrow$

ⓐ' $\exists_{i-1<j\leq 2(i-1)+1} j \ \forall_{(i-1)<k\leq 2n+1} k \quad S'[j] \leq S'[k] \quad \wedge$

ⓑ' $\forall_{(i-1)<j\leq 2n+1} j \ \exists_{1\leq k\leq n+1} k \quad S'[j] = X[k] \quad \wedge$

ⓒ' $\forall_{1\leq k\leq n+1} k \ \exists_{i-1<j\leq 2n+1} j \quad S'[j] = X[k]$

<u>S' הוא S לאחר ההשמה $S[i]:=S[2i]$</u>. טענה ⓐ מבטיחה שהאיבר המינימלי ב-S נמצא בין $i+1$ ל-$2i+1$, ו-$C_{\pi_{22}}$ מצמצמת את הטווח להיות בין $i+1$ ל-$2i$. מכיוון שההשמה מעתיקה את $S[2i]$ ל-$S[i]$ מתקבל כי האיבר המינימלי ב-S' הוא בין i ל-$2i-1$, כלומר טענה ⓐ'.

טענה b מבטיחה כי כל האיברים ב-S מ-$n+1$ עד $2n+1$ הם איברים מ-$X[1],\ldots,X[n+1]$. ההשמה בוצעה, קיבלנו אז S' מעתיקה אחד מאיברים אלו ל-$S[i]$ לכן כל האיברים ב-S' מ-i עד $2n+1$ הם איברים מ-X, וטענה b' מתקיימת.

טענה c מבטיחה כי כל איברי X מוצבים ב-S, בין $i+1$ ל-$2n+1$. מכיוון שהיא מתקיימת אז בוודאי כל איברי X מוצבים ב-S' בין i ל-$2n+1$.

קיבלנו כי תנאי האימות VC_{22} מתקיים.

את VC'_{22} מקבלים תוך שימוש בשיקולים דומים.

$$VC_{23}: \quad \phi_2(S,i) \wedge C_{\pi_{23}}(S,i) \to \phi_3(f_{\pi_{23}}(S,i))$$

מתקבל מיידית כי $f_{\pi_{23}}$ היא זהות, ו- $\phi_3 = \phi_2 \wedge C_{\pi_{23}}$.

הראינו כי כל תנאי האימות מתקיימים, לכן $N=\{\phi_1,\phi_2,\phi_3\}$ היא רשת טענות אינדוקטיבית. ניתן לראות כי $\phi_1=\phi$, $\phi_3 \to \psi$. כלומר N גוררת את קיום הספציפיקציה (ϕ,ψ), לפיכך P נכונה חלקית ביחס ל-(ϕ,ψ).