לוגיקה למדעי המחשב - הרצאה 4

משפט השלמות של HPC

אם $T\vdash_{CPL}\varphi$ אז $T\vdash_{HPC}\varphi$. נראה במקום זאת שאם $T\nvdash_{HPC}\varphi$ אז $T\nvdash_{CPL}\varphi$, כלומר שאם $T\nvdash_{HPC}\varphi$ אז קיים מודל v של T שאינו מודל של φ.

<u>רעיון ההוכחה:</u>

נגדיר:

$$v_T(A) = \begin{cases} t & A\in T \\ f & A\notin T \end{cases}$$

ברור אבל כי ישנן תורות T עבורן v_T אינה השמה, אבל אם T מקיימת את התכונות הבאות, אז v_T תהיה השמה:

- $\neg A\in T \Leftrightarrow A\notin T$
- $(A\wedge B)\in T \Leftrightarrow (A\in T \text{ and } B\in T)$
- $(A\vee B)\in T \Leftrightarrow (A\in T \text{ or } B\in T)$
- $(A\to B)\in T \Leftrightarrow (A\notin T \text{ or } B\in T)$

בהינתן תורה T, אם כן, נרחיב אותה לתורה שמקיימת את הדרישות הנ"ל כך ש-φ עדיין לא יכיח ממנה.

<u>תמצית ההוכחה:</u>

1. נרחיב את T לתורה מקסימלית T^* כך ש-φ $T^*\nvdash_{HPC}\varphi$.
2. נראה שאם T^* מקסימלית כנ"ל אז v_{T^*} היא השמה חוקית המהווה מודל של T^* ואינה מודל של φ.

<u>הוכחה:</u>

שלב א'

תהי T תורה ו-φ פסוק כך ש-$T\nvdash_{HPC}\varphi$. נסדר את כל הפסוקים בשפה בסדרה: $A_1,A_2,A_3,\ldots$ (אפשרי כי זו קבוצה בת מניה). נגדרי סדרת תורות T_n $\lambda n.$ באופן הבא:

$$T_0=T \qquad T_{n+1}=\begin{cases} T_n\cup\{A_{n+1}\} & T_n\cup\{A_{n+1}\}\nvdash_{HPC}\varphi \\ T_n & T_n\cup\{A_{n+1}\}\vdash_{HPC}\varphi \end{cases}$$

כעת $T^*=\bigcup\limits_{n=0}^{\infty}T_n$.

<u>תכונות של T_n:</u>

א. $T_n\nvdash_{HPC}\varphi$ לכל $n\geq 0$.

ב. או ש-$T_n\vdash_{HPC}A_n$ או ש-$T_n\vdash_{HPC}A_n\to\varphi$ (עבור $n\geq 1$).

הוכחת התכונה הראשונה באינדוקציה על n הינה טריביאלית מהגדרת T_{n+1} והעובדה ש- $T_0\nvdash_{HPC}\varphi$ (כי $T_0=T$).

הוכחת התכונה השניה: נניח $n>0$. אם $T_n=T_{n-1}\cup\{A_n\}$ אז ברור כי $T_n\vdash_{HPC}A_n$ (כי $A_n\in T_n$).
אם $T_n=T_{n-1}$ אז $T_{n-1}\cup\{A_n\}\vdash_{HPC}\varphi$ ולפי משפט הדדוקציה, $T_{n-1}\vdash_{HPC}A_n\to\varphi$, כלומר $T_n\vdash_{HPC}A_n\to\varphi$.

מזה נקבל את התכונות הבאות של T^*:

1. $T^* \nvdash_{HPC} \varphi$
2. לכל פסוק ψ, או ש-$T^* \vdash_{HPC} \psi$ או ש-$T^* \vdash_{HPC} \psi \to \varphi$.
3. לכל פסוק ψ, אם $T^* \vdash_{HPC} \psi$ אז $\psi \in T^*$.

<u>הוכחת 1</u>:

נניח בשלילה כי $T^* \vdash_{HPC} \varphi$. אזי יש קבוצה סופית $\Gamma \subseteq T^*$ כך ש- $\Gamma \vdash_{HPC} \varphi$. כעת, $\Gamma \subseteq \bigcup_{n=0}^{\infty} T_n$ (כזכור $T^* = \bigcup_{n=0}^{\infty}$), אבל Γ סופית ולכן קיים N_0 כך ש- $\Gamma \subseteq \bigcup_{n=0}^{N_0} T_n$, כלומר $\Gamma \subseteq T_{N_0}$ (זאת מכיוון ש- $T_0 \subseteq T_1 \subseteq \ldots \subseteq T_{N_0}$ מהגדרת הסדרה $\lambda n.\ T_n$).
לכן נקבל $T_{N_0} \vdash_{HPC} \varphi$ בסתירה לתכונה א' של T_{N_0}.

<u>הוכחת 2</u>:

יהי ψ פסוק. אז קיים n כך ש- $\psi = A_n$. לפי תכונה ב' של T_n, או ש- $T_n \vdash_{HPC} \psi$ או ש- $T_n \vdash_{HPC} \psi \to \varphi$, לכן $T^* \vdash_{HPC} \psi$ או $T^* \vdash_{HPC} \psi \to \varphi$.

<u>הוכחת 3</u>:

נניח $T^* \vdash_{HPC} \psi$ אך $\psi \notin T^*$. נניח $\psi = A_n$. מכיוון ש- $\psi \notin T^*$, אז $\psi \notin T_n$. זה אפשרי רק אם $T_{n-1} \cup \{A_n\} \vdash_{HPC} \varphi$, כלומר $T_{n-1} \cup \{\psi\} \vdash_{HPC} \varphi$. ממילא נקבל אז ש- $T^* \cup \{\psi\} \vdash_{HPC} \varphi$. מזה ומ- $T^* \vdash_{HPC} \psi$ נקבל $T^* \vdash_{HPC} \varphi$ בסתירה לתכונה 1.

שלב ב'

נגדיר v ע"י:

$$v(\psi) \quad = \quad \begin{cases} t & \psi \in T^* \\ f & \psi \notin T^* \end{cases}$$

ברור ש- $v(\psi) = t$ לכל $\psi \in T$ (כי $T \subseteq T^*$) וש- $v(\varphi) = f$ (כי $\varphi \notin T^*$, שהרי $T^* \nvdash_{HPC} \varphi$).
נראה עתה כי v השמה חוקית (כלומר מכבדת את טבלאות האמת) ואז v תהיה מודל של T שאינה מודל של φ, כמבוקש.
עלינו להראות:

1. $v(\psi_1 \wedge \psi_2) = v(\psi_1) \wedge v(\psi_2)$
2. $v(\psi_1 \vee \psi_2) = v(\psi_1) \vee v(\psi_2)$
3. $v(\neg\psi) = \neg v(\psi)$
4. $v(\psi_1 \to \psi_2) = v(\psi_1) \to v(\psi_2)$

(כאשר $\wedge, \vee, \neg, \to$ בצד הימני של השוויונים הן פונקציות האמת כמובן).

<u>הוכחת 1</u>

- נניח $v(\psi_1) = t$ ו- $v(\psi_2) = t$. אז $\psi_1 \in T^*$ ו- $\psi_2 \in T^*$. מכיוון ש- $\psi_1, \psi_2 \vdash_{HPC} \psi_1 \wedge \psi_2$ (בעזרת אקסיומה C3) אז $T^* \vdash_{HPC} \psi_1 \wedge \psi_2$ ולכן $v(\psi_1 \wedge \psi_2) = t$.
- נניח $v(\psi_1) = f$ אז $\psi_1 \notin T^*$ ולכן $T^* \nvdash_{HPC} \psi_1$. מכיוון ש- $\psi_1 \wedge \psi_2 \vdash_{HPC} \psi_1$ (מ-C1) אז לא ייתכן כי $\psi_1 \wedge \psi_2 \in T^*$ ולכן $v(\psi_1 \wedge \psi_2) = f$.
- $v(\psi_2) = f$ - ההוכחה דומה למקרה בו $v(\psi_1) = f$, רק צריך את C2 במקום C1.

הוכחת 2

- נניח $v(\psi_1)=t$. אז $\psi_1\in T^*$. כיוון ש- $\psi_1\vdash_{HPC}\psi_1\vee\psi_2$ (לפי D1) אז נובע מזה ש- $T^*\vdash_{HPC}\psi_1\vee\psi_2$ ולכן $\psi_1\vee\psi_2\in T^*$ ו- $v(\psi_1\vee\psi_2)=t$.
- אם $v(\psi_2)=t$ מראים באופן דומה ש- $v(\psi_1\vee\psi_2)=t$, תוך שימוש ב-D2.
- נניח $v(\psi_1)=f$ וגם $v(\psi_2)=f$. אז $\psi_1\notin T^*$ ו- $\psi_2\notin T^*$, לכן $\psi_1\to\varphi\in T^*$ ו- $\psi_2\to\varphi\in T^*$. כיוון ש- $\psi_1\to\varphi,\psi_2\to\varphi,\psi_1\vee\psi_2\vdash_{HPC}\varphi$ (בעזרת D3) ו- $T^*\nvdash_{HPC}\varphi$, פירוש הדבר ש- $\psi_1\vee\psi_2\notin T^*$, ולכן $v(\psi_1\vee\psi_2)=f$.

הוכחת 3

- נניח $v(\psi)=t$. אז $\psi\in T^*$. כיוון ש- $\psi,\neg\psi\vdash_{HPC}\varphi$ (לפי למה שהוכחה בכיתה), לא ייתכן שגם $\neg\psi\in T^*$ ולכן $\neg\psi\notin T^*$ ו- $v(\neg\psi)=f$.
- נניח $v(\psi)=f$. אז $\psi\notin T^*$ ולכן $\psi\to\varphi\in T^*$. נניח בשלילה ש- $\neg\psi\notin T^*$, כלומר $\neg\psi\to\varphi\in T^*$. לפי למה שהוכחה בתירגול, $\psi\to\varphi,\ \neg\psi\to\varphi\vdash_{HPC}\varphi$ לכן נקבל ש- $T^*\vdash_{HPC}\varphi$ וזו סתירה. לכן $\neg\psi\in T^*$ ו- $v(\neg\psi)=t$ כדרוש.

הוכחת 4

- נניח $v(\psi_1)=t$ ו- $v(\psi_2)=f$ אז $\psi_1\in T^*$ ו- $\psi_2\notin T^*$, לכן $T^*\nvdash_{HPC}\psi_2$. כיוון ש- $\psi_1,\psi_1\to\psi_2\vdash_{HPC}\psi_2$, נובע מכל זאת ש- $\psi_1\to\psi_2\notin T^*$ ולכן $v(\psi_1\to\psi_2)=f$.
- נניח $v(\psi_2)=t$, כלומר $\psi_2\in T^*$. כיוון ש- $\psi_2\vdash_{HPC}\psi_1\to\psi_2$ (בעזרת I1) אז $T^*\vdash_{HPC}\psi_1\to\psi_2$, ולכן $\psi_1\to\psi_2\in T^*$ ו- $v(\psi_1\to\psi_2)=t$.
- נניח $v(\psi_1)=f$. אז $\psi_1\in T$. לכן, לפי מה שהראנו לגבי $\neg$, $v(\neg\psi_1)=t$ ו- $\neg\psi_1\in T^*$. אבל $\neg\psi_1\vdash_{HPC}\psi_1\to\psi_2$ (בעזרת משפט הדדוקציה, כי $\neg\psi_1,\psi_1\vdash_{HPC}\psi_2$). לכן $T^*\vdash_{HPC}\psi_1\to\psi_2$ ולכן $\psi_1\to\psi_2\in T^*$ ו- $v(\psi_1\to\psi_2)=t$ כנדרש.

הערה: הוכחת 4 שונה מההוכחות האחרות בכך שהיא משתמשת בתכונות של $\neg$, כלומר באקסיומות שקשורות ב-$\neg$. על כן, ב-HPI, למשל, בו $\neg\neg A\to A$ אינה אקסיומה, $((A\to B)\to A)\to A$ אינו פסוק יכיח.

מסקנה: משפט הקומפקטיות:

אם $T\vdash_{CPL}\varphi$ אז קיימת $\Gamma\subseteq T$ סופית כך ש-$\Gamma\vdash_{CPL}\varphi$.

הוכחה: נובע מ- $\vdash_{CPL}=\vdash_{HPC}$ ומשפט הקומפקטיות של HPC.

תזכורת (מתירגול): T קונסיסטנטית ב-HPC אם אין פסוק φ כך שגם $T\vdash_{HPC}\varphi$ וגם $T\vdash_{HPC}\neg\varphi$.

משפט השלמות נוסח ב':

T היא תורה ספיקה אמ"ם T היא קונסיסטנטית ב-HPC.

הוכחה:

1. נניח T ספיקה ו-v מודל של T. יהי φ פסוק כלשהו. אז או ש-$v(\varphi)=f$ או ש-$v(\neg\varphi)=f$. במקרה הראשון, $T\nvdash_{HPC}\varphi$ בגלל משפט הנאותות. במקרה השני, $T\nvdash_{HPC}\neg\varphi$ מאותו שיקול. זה נכון לכל φ ולכן T קונסיסטנטית ב-HPC.
2. נניח T קונסיסטנטית ב-HPC. אז יש פסוק φ כך ש-$T\nvdash_{HPC}\varphi$ (בתרגיל הוכח כי הגדרה זו של קונסיסטנטיות שקולה). לפי משפט השלמות שהוכחנו, $T\nvdash_{CPL}\varphi$, כלומר יש מודל של T שאינו מודל של φ ולכן יש ל-T מודל, כלומר T ספיקה.

מסקנה נוספת ממשפט השלמות:

שלמות חלשה של HPC: φ הינה טאוטולוגיה של תחשיב הפסוקים אמ"ם $\vdash_{HPC}\varphi$.

הוכחה: φ טאוטולוגיה אמ"ם $\emptyset\vdash_{CPL}\varphi$ אמ"ם $\emptyset\vdash_{HPC}\varphi$ (שלמות ונאותות של HPC).

דדוקציה טבעית - Natural Deduction

קישור wikipedia: http://en.wikipedia.org/wiki/Natural_deduction

הוכחה בדדוקציה טבעית מדמה את הדרך הטבעית בה אנשים מוכיחים טענות. נראה אם כן, דוגמא להוכחה בדרך טבעית ואיך דדוקציה טבעית מייצגת הוכחה כזו.

דוגמא:

נוכיח $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$, כלומר $x \in A \wedge (x \in B \vee x \in C) \to (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$.

נניח $x \in A \wedge (x \in B \vee x \in C)$ אז $x \in A$ ו-$x \in B \vee x \in C$.
אם $x \in B$ אז כיוון ש-$x \in A$, מתקיים $x \in A \wedge x \in B$ ולכן $(x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$.
ואם $x \in C$ אז כיוון ש-$x \in A$, מתקיים $x \in A \wedge c \in C$ ולכן $(x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$.
בשני המקרים קיבלנו $(x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$ ולכן
$x \in A \wedge (x \in B \vee x \in C) \to (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$

נשים לב כי למרות שמדובר כאן בהוכחה של טאוטולוגיה, לא כל הנוסחאות המופיעות בהוכחה הן בעצמן טאוטולוגיות (בניגוד למה שקורה בהוכחות ב-HPC). כך למשל $x \in A \wedge x \in B$ אינה טאוטולוגיה. כל נוסחא נכונה כאן רק אם ההנחות הנמצאות ברקע במקום בו היא נכתבת מתקיימות. הוכחות בדדוקציה טבעית פועלות אכן בדרך של הכנסת הנחות רקע, הסקת מסקנות וסילוק ההנחות כדי להגיע לנוסחא אותה רוצים להוכיח.

דרך אחת להגדיר תחשיב לצורה כזו היא לכתוב בכל שורה את הנחות הרקע שמהן הוסקה השורה. כל שורה כזו נקראת סקוונט (Sequent) וצורתה היא הסימן $\Rightarrow$ שמשמאלו קבוצת הנחות הרקע ומימינו הנוסחא שטוענים כי היא מתקיימת בהינתן הנחות הרקע. כל סקוונט מוסק מקודמיו בעזרת כללי ההיסק של NDC.

כללי היסק בדדוקציה טבעית (NDC)

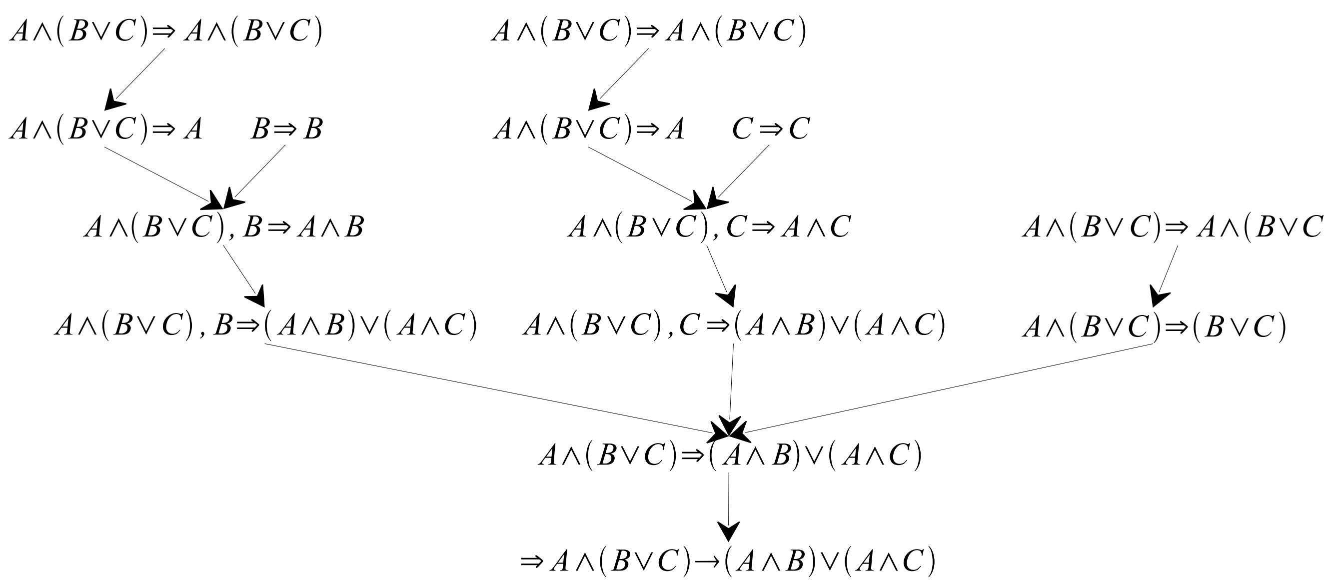
כללי הכנסה של קשר, שבעזרתם ניתן לקבל פסוק עם הקשר, מסומנים ב-$\circ I$ (Introduction), כאשר $\circ$ הוא הקשר.
כללי סילוק של קשר, שבעזרתם ניתן להיפטר מקשר בפסוק מסויים, מסומנים ב-$\circ E$ (Elimination), כאשר $\circ$ הוא הקשר.
בתיאור כל כלל הסקוונטים שמהם מסיקים (ההקדמות של הכלל) מופיעים מעל הקו והסקוונט אותו מסיקים (המסקנה) מופיע מתחת לקו.

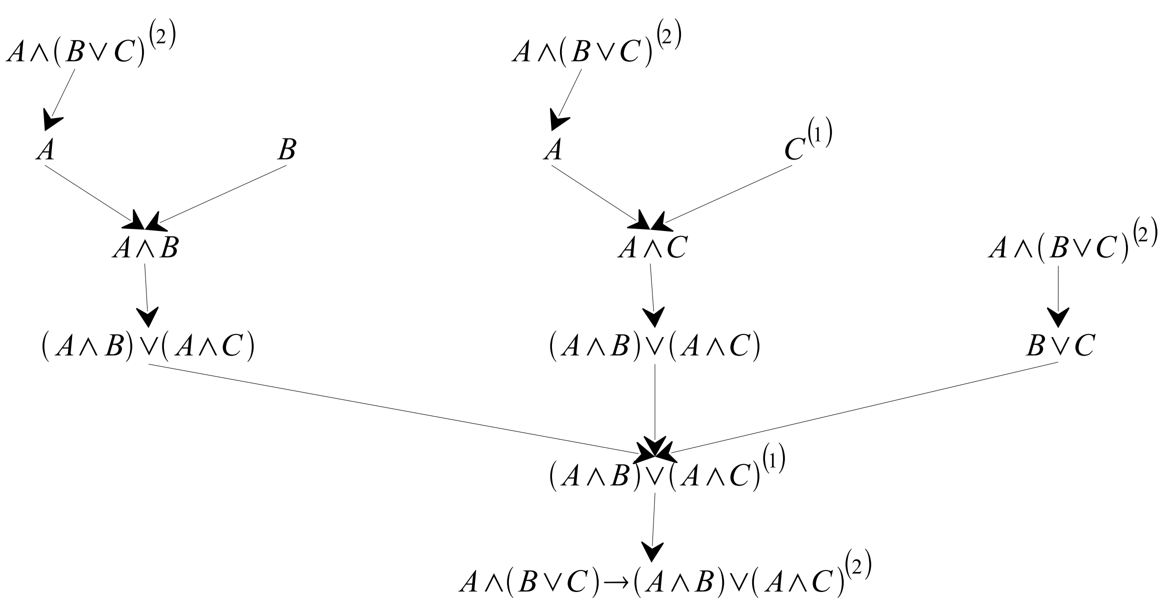
- אקסיומה: $\{A\} \cup \Gamma \Rightarrow A$
- $\wedge I$: $\frac{\Gamma_1 \Rightarrow A \qquad \Gamma_2 \Rightarrow B}{\Gamma_1 \cup \Gamma_2 \Rightarrow A \wedge B}$
- $\wedge E$: $\frac{\Gamma \Rightarrow A \wedge B}{\Gamma \Rightarrow A} \qquad \frac{\Gamma \Rightarrow A \wedge B}{\Gamma \Rightarrow B}$
- $\to I$: $\frac{\Gamma \cup \{A\} \Rightarrow B}{\Gamma \Rightarrow A \to B}$
- $\to E$: $\frac{\Gamma_1 \Rightarrow A \qquad \Gamma_2 \Rightarrow A \to B}{\Gamma_1 \cup \Gamma_2 \Rightarrow B}$
- $\vee I$: $\frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B} \qquad \frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B}$
- $\vee E$: $\frac{\Gamma_1 \Rightarrow A \vee B \qquad \{A\} \cup \Gamma_2 \Rightarrow C \qquad \{B\} \cup \Gamma_3 \Rightarrow C}{\Gamma_1 \cup \Gamma_2 \cup \Gamma_3 \Rightarrow C}$
- $\neg I$: $\frac{\{A\} \cup \Gamma_1 \Rightarrow B \qquad \{A\} \cup \Gamma_2 \Rightarrow \neg B}{\Gamma_1 \cup \Gamma_2 \Rightarrow \neg A}$
- $\neg E$: $\frac{\Gamma \Rightarrow \neg\neg A}{\Gamma \Rightarrow A}$

ההוכחה שבדוגמא תראה כך (כאשר משמיטים, כמקובל כאן, את הסוגריים המסולסלים בצד שמאל של $\Rightarrow$):

1.	$A \wedge (B \vee C) \Rightarrow A \wedge (B \vee C)$	אקסיומה
2.	$A \wedge (B \vee C) \Rightarrow A$	מ–1 ע"י הכלל $\wedge E$
3.	$A \wedge (B \vee C) \Rightarrow B \vee C$	מ–1 ע"י הכלל $\wedge E$
4.	$B \Rightarrow B$	אקסיומה
5.	$A \wedge (B \vee C), B \Rightarrow A \wedge B$	מ–2,4 ע"י הכלל $\wedge I$
6.	$A \wedge (B \vee C), B \Rightarrow (A \wedge B) \vee (A \wedge C)$	מ–5 ע"י הכלל $\vee I$
7.	$C \Rightarrow C$	אקסיומה
8.	$A \wedge (B \vee C), C \Rightarrow A \wedge C$	מ–2,7 ע"י הכלל $\wedge I$
9.	$A \wedge (B \vee C), C \Rightarrow (A \wedge B) \vee (A \wedge C)$	מ–8 ע"י הכלל $\vee I$
10.	$A \wedge (B \vee C) \Rightarrow (A \wedge B) \vee (A \wedge C)$	מ–3,6,9 ע"י הכלל $\vee E$
11.	$\Rightarrow A \wedge (B \vee C) \rightarrow (A \wedge B) \vee (A \wedge C)$	מ–10 ע"י הכלל $\rightarrow I$

מקובל לכתוב את ההוכחה גם בצורת עץ, עם או בלי ההנחות. כשלא כותבים את ההנחות, יש לציין את המקומות בהם הן מוכנסות ומסולקות (המספרים הקטנים בסוגריים):





ואפשר גם בצורה סדרתית (רשימה):

	נוסחא	הוסק מ:	הנחות רקע
1	$A \wedge (B \vee C)$	הנחה	$\{1\}$
2	A	1 ע"י $\wedge E$	$\{1\}$
3	$B \vee C$	1 ע"י $\wedge E$	$\{1\}$
4	B	הנחה	$\{4\}$
5	$A \wedge B$	4,2 ע"י $\wedge I$	$\{1, 4\}$
6	$(A \wedge B) \vee (A \wedge C)$	5 ע"י $\vee I$	$\{1, 4\}$
7	C	הנחה	$\{7\}$
8	$A \wedge C$	7,2 ע"י $\wedge I$	$\{1, 7\}$
9	$(A \wedge B) \vee (A \wedge C)$	8 ע"י $\vee I$	$\{1, 7\}$
10	$(A \wedge B) \vee (A \wedge C)$	9,6,3 ע"י $\vee E$	$\{1\}$
11	$A \wedge (B \vee C) \rightarrow (A \wedge B) \vee (A \wedge C)$	10 ע"י $\rightarrow I$	$\emptyset$