# Logica per l'Informatica

## Soluzioni commentate del laboratorio del:

## 12/12/2023

Come sempre, i commenti sono in blu.

**Esercizio 1: Riscaldamento booleano.**

1)

Definiamo la funzione $\texttt{and} : \texttt{Bool} \to \texttt{Bool} \to \texttt{Bool}$ per ricorsione strutturale:

$$\begin{array}{lcl} \texttt{and}\ \texttt{true}\ b & := & b \\ \texttt{and}\ \texttt{false}\ b & := & \texttt{false}, \end{array}$$

con $b : \texttt{Bool}$.

Definiamo la funzione $\texttt{or} : \texttt{Bool} \to \texttt{Bool} \to \texttt{Bool}$ per ricorsione strutturale:

$$\begin{array}{lcl} \texttt{or}\ \texttt{true}\ b & := & \texttt{true} \\ \texttt{or}\ \texttt{false}\ b & := & b, \end{array}$$

con $b : \texttt{Bool}$.

2)

**Theorem 1** (Versione semantica di una delle leggi di de Morgan)**.**

$$\forall b_1 : \textit{Bool}.\, \forall b_2 : \textit{Bool}. \qquad \textit{not}\,(\texttt{and}\, b_1\, b_2) = \textit{or}\,(\textit{not}\, b_1)\,(\textit{not}\, b_2).$$

*Dimostrazione.* Per dimostrare il teorema possiamo andare per induzione strutturale su $b : \texttt{Bool}$ per dimostrare la formula[1]:

$$\forall b_2 : \texttt{Bool}. \qquad \texttt{not}\,(\texttt{and}\, b\, b_2) = \texttt{or}\,(\texttt{not}\, b)\,(\texttt{not}\, b_2).$$

Per definizione di $\texttt{Bool}$, questo significa che, affinché questa dimostrazione per induzione sia corretta, dobbiamo risolvere esattamente i due casi seguenti:

[1] Nota che qui è sparito il primo quantificatore, quello su cui vado per induzione!

- Caso $\texttt{true}$.

  Dobbiamo dimostrare la formula:

  $$\forall b_2 : \texttt{Bool}. \qquad \texttt{not}\,(\texttt{and}\,\texttt{true}\,b_2) = \texttt{or}\,(\texttt{not}\,\texttt{true})\,(\texttt{not}\,b_2).$$

  Sia $b : \texttt{Bool}$. Dobbiamo dimostrare $\texttt{not}\,(\texttt{and}\,\texttt{true}\,b) = \texttt{or}\,(\texttt{not}\,\texttt{true})\,(\texttt{not}\,b)$. Ma questo è un semplice calcolo:

  Sviluppando il membro di sinistra ottengo: $\texttt{not}\,(\texttt{and}\,\texttt{true}\,b) = \texttt{not}\,b$ per definizione di $\texttt{and}$ .

  Sviluppando il membro di destra ottengo: $\texttt{or}\,(\texttt{not}\,\texttt{true})\,(\texttt{not}\,b) = \texttt{or}\,\texttt{false}(\texttt{not}\,b) = \texttt{not}\,b$ per definizione di $\texttt{not}$ , per definizione di $\texttt{or}$ (e per la transitività di $=$ il membro a sinistra di questa catena di uguaglianze è uguale a quello di destra).

  Dunque ci siamo ridotti a dover dimostrare $\texttt{not}\,b = \texttt{not}\,b$, che è triviale per la riflessività di $=$.

- Caso $\texttt{false}$.

  Dobbiamo dimostrare la formula:

  $$\forall b_2 : \texttt{Bool}. \qquad \texttt{not}\,(\texttt{and}\,\texttt{false}\,b_2) = \texttt{or}\,(\texttt{not}\,\texttt{false})\,(\texttt{not}\,b_2).$$

  Sia $b : \texttt{Bool}$. Dobbiamo dimostrare $\texttt{not}\,(\texttt{and}\,\texttt{false}\,b) = \texttt{or}\,(\texttt{not}\,\texttt{false})\,(\texttt{not}\,b)$. Ma questo è un semplice calcolo:

  Sviluppando il membro di sinistra ottengo: $\texttt{not}\,(\texttt{and}\,\texttt{false}\,b) = \texttt{not}\,\texttt{false} = \texttt{true}$ per definizione di $\texttt{and}$ , per definizione di $\texttt{not}$ (e per la transitività di $=$ il membro a sinistra di questa catena di uguaglianze è uguale a quello di destra).

  Sviluppando il membro di destra ottengo: $\texttt{or}\,(\texttt{not}\,\texttt{false})\,(\texttt{not}\,b) = \texttt{or}\,\texttt{true}(\texttt{not}\,b) = \texttt{true}$ per definizione di $\texttt{not}$ , per definizione di $\texttt{or}$ (e per la transitività di $=$ il membro a sinistra di questa catena di uguaglianze è uguale a quello di destra).

  Dunque ci siamo ridotti a dover dimostrare $\texttt{true} = \texttt{true}$, che è triviale per la riflessività di $=$.

$\square$

Commento: Osserva che nella dimostrazione di prima non c'era nessun "passo induttivo" nella dimostrazione, e questo perché il tipo induttivo dei booleani ha solo due forme base e nessuna forma definita in maniera ricorsiva.

**Esercizio 2: Riscaldamento aritmetico.**

1).

Definiamo la funzione $\texttt{isZero} : \texttt{Nat} \to \texttt{Bool}$ per ricorsione strutturale:

$$\begin{aligned} \texttt{isZero}\,\texttt{0} &:= \texttt{true} \\ \texttt{isZero}\,\texttt{S}\,n &:= \texttt{false}, \end{aligned}$$

con $n : \texttt{Nat}$.

Commento:

Nel testo non è specificato, ma dalla definizione del tipo $\texttt{Nat}$ si intende che prendiamo come assioma la formula: $\forall n : \texttt{Nat}.\ \ \texttt{S}\,n \neq \texttt{0}$. Lo useremo nella dimostrazione seguente.

**Theorem 2.**

$$\forall n : \texttt{Nat}. \qquad (n \neq \texttt{0}) \leftrightarrow (\texttt{isZero}\,n = \texttt{false}).$$

*Dimostrazione.* Per dimostrare il teorema, possiamo andare per induzione strutturale su $n : \texttt{Nat}$ per dimostrare la formula[2]: $(n \neq \texttt{0}) \leftrightarrow (\texttt{isZero}\,n = \texttt{false})$.

Per definizione di $\texttt{Nat}$, questo significa che, affinché questa dimostrazione per induzione sia corretta, dobbiamo risolvere esattamente i seguenti due casi:

- Caso $\texttt{0}$.

  Dobbiamo dimostrare la formula: $(\texttt{0} \neq \texttt{0}) \leftrightarrow (\texttt{isZero}\,\texttt{0} = \texttt{false})$.

  Siccome $\leftrightarrow$ è zucchero sintattico per la congiunzione delle due implicazioni opposte, per la regola di introduzione di $\wedge$ dobbiamo dimostrare le due implicazioni, ovvero dobbiamo dimostrare le seguenti due implicazioni:

  - Dimostriamo $(\texttt{0} \neq \texttt{0}) \to (\texttt{isZero}\,\texttt{0} = \texttt{false})$, ovvero dimostriamo $\texttt{isZero}\,\texttt{0} = \texttt{false}$ sotto l'ipotesi $\texttt{0} \neq \texttt{0}$.

    Ma la nostra ipotesi è contraddittoria[3], perché la riflessività di $=$[4] ci dice che $\texttt{0} = \texttt{0}$ (e dunque, per la regola di eliminazione di $\neg$ otteniamo $\bot$). Siccome abbiamo trovato una contraddizione, per la regola di eliminazione del $\bot$ abbiamo finito[5].

[2] Nota che qui è sparito il primo quantificatore, quello su cui vado per induzione!

[3] Ovvero, usandola come ipotesi dimostriamo $\bot$ in DN. Ricorda che questo è ciò che si intende quando nel gergo matematico si dice che una formula "è assurda".

[4] Non lo specifichiamo mai nel testo, ma la prendiamo sempre come un assioma, ovvero: $\forall x.\, x = x$.

[5] Perché con la regola di eliminazione di $\bot$ dimostriamo una qualsiasi formula, in particolare $\texttt{isZero}\,\texttt{0} = \texttt{false}$, che era proprio quella che volevamo. Nota che questa formula è a sua volta contraddittoria con la definizione di $\texttt{isZero}$, ma non ci interessa!

- Dimostriamo $(\mathtt{isZero}\,\mathtt{0} = \mathtt{false}) \to (\mathtt{0} \neq \mathtt{0})$, ovvero dimostriamo $\mathtt{0} \neq \mathtt{0}$ sotto l'ipotesi $\mathtt{isZero}\,\mathtt{0} = \mathtt{false}$. Ma la nostra ipotesi è contraddittoria, perché la definizione di $\mathtt{isZero}$ ci dice che $\mathtt{isZero}\,\mathtt{0} = \mathtt{true}$ e sappiamo che invece $\mathtt{true} \neq \mathtt{false}$ come assioma. Dunque, abbiamo finito.

- Caso $\mathtt{S}\,n$, con $n : \mathtt{Nat}$.

  L'Ipotesi Induttiva è la formula: $(n \neq \mathtt{0}) \leftrightarrow (\mathtt{isZero}\,n = \mathtt{false})$.

  Avendo a disposizione l'Ipotesi Induttiva, dobbiamo dimostrare la formula: $(\mathtt{S}\,n \neq \mathtt{0}) \leftrightarrow (\mathtt{isZero}\,(\mathtt{S}\,n) = \mathtt{false})$.

  Ovvero, dobbiamo dimostrare le seguenti due implicazioni:

  - Dimostriamo $(\mathtt{S}\,n \neq \mathtt{0}) \to (\mathtt{isZero}\,(\mathtt{S}\,n) = \mathtt{false})$, ovvero dimostriamo $\mathtt{isZero}\,(\mathtt{S}\,n) = \mathtt{false}$ sotto l'ipotesi $\mathtt{S}\,n \neq \mathtt{0}$.

    Ma questa è proprio la definizione di $\mathtt{isZero}$.

  - Dimostriamo $(\mathtt{isZero}\,(\mathtt{S}\,n) = \mathtt{false}) \to (\mathtt{S}\,n \neq \mathtt{0})$, ovvero dimostriamo $\mathtt{S}\,n \neq \mathtt{0}$ sotto l'ipotesi $\mathtt{isZero}\,(\mathtt{S}\,n) = \mathtt{false}$.

    Ma questo è proprio uno dei nostri assiomi.

$\square$

Commento: Osserva che nel caso $\mathtt{S}\,n$ della dimostrazione precedente non abbiamo usato l'Ipotesi Induttiva (e non abbiamo neanche usato le ipotesi locali delle varie implicazioni)... nessun problema, vuol semplicemente dire che questo esercizio era particolarmente semplice!

2)

Definiamo la funzione $\cdot : \mathtt{Nat} \to \mathtt{Nat} \to \mathtt{Nat}$ per ricorsione strutturale:

Dalla definizione di funzione ricorsiva strutturale che avete dato in aula, dobbiamo andare per ricorsione strutturale sul primo argomento della funzione:

$$\begin{array}{lcl} \mathtt{0} \cdot m & := & \mathtt{0} \\ \mathtt{S}\,n \cdot m & := & (n \cdot m) + m, \end{array}$$

con $n : \mathtt{Nat}$ e $m : \mathtt{Nat}$.

**Theorem 3.**

$$\forall n : \mathtt{Nat}. \qquad n \cdot \mathtt{0} = \mathtt{0}.$$

*Dimostrazione.* Per dimostrare il teorema, possiamo andare per induzione strutturale su $n : \mathtt{Nat}$ per dimostrare la formula $n \cdot \mathtt{0} = \mathtt{0}$[6].

Per definizione di $\mathtt{Nat}$, questo significa che, affinché questa dimostrazione per induzione sia corretta, dobbiamo risolvere esattamente i seguenti due casi:

[6] Nota che qui è sparito il primo quantificatore, quello su cui vado per induzione!

- Caso $\mathtt{0}$.

  Dobbiamo dimostrare la formula $\mathtt{0} \cdot \mathtt{0} = \mathtt{0}$.

  Ma questa è proprio la definizione di $\cdot$.

- Caso $\mathtt{S}\, n$, con $n : \mathtt{Nat}$.

  L'Ipotesi Induttiva è: $n \cdot \mathtt{0} = \mathtt{0}$.

  Avendo a disposizione l'Ipotesi Induttiva, dobbiamo dimostrare la formula: $(\mathtt{S}\, n) \cdot \mathtt{0} = \mathtt{0}$.

  Per definizione di $\cdot$ ci riduciamo a dover dimostrare $(n \cdot \mathtt{0}) + \mathtt{0} = \mathtt{0}$; per definizione di $+$ ci riduciamo a dover dimostrare $n \cdot \mathtt{0} = \mathtt{0}$; ma questa è proprio l'Ipotesi Induttiva, quindi abbiamo finito.

$\square$

**Esercizio 3: Il tipo delle formule.**
1)

Definiamo la funzione $\mathtt{truth} : \mathtt{Formula} \to \mathtt{Bool} \to \mathtt{Bool} \to \mathtt{Bool} \to \mathtt{Bool}$ per ricorsione strutturale.

Dalla definizione di funzione ricorsiva strutturale che avete dato in aula, dobbiamo andare per ricorsione strutturale sul primo argomento della funzione:

$$
\begin{array}{llllll}
\mathtt{truth} & x_1 & b_1 & b_2 & b_3 & := & b_1 \\
\mathtt{truth} & x_2 & b_1 & b_2 & b_3 & := & b_2 \\
\mathtt{truth} & x_3 & b_1 & b_2 & b_3 & := & b_3 \\
\mathtt{truth} & (\neg\varphi_1) & b_1 & b_2 & b_3 & := & \mathtt{not}\,(\mathtt{truth}\,\varphi_1\, b_1\, b_2\, b_3) \\
\mathtt{truth} & (\varphi_1 \wedge \varphi_2) & b_1 & b_2 & b_3 & := & \mathtt{and}\,(\mathtt{truth}\,\varphi_1\, b_1\, b_2\, b_3)\,(\mathtt{truth}\,\varphi_2\, b_1\, b_2\, b_3) \\
\mathtt{truth} & (\varphi_1 \vee \varphi_2) & b_1 & b_2 & b_3 & := & \mathtt{or}\,(\mathtt{truth}\,\varphi_1\, b_1\, b_2\, b_3)\,(\mathtt{truth}\,\varphi_2\, b_1\, b_2\, b_3),
\end{array}
$$

con $\varphi_1 : \mathtt{Formula}$, $\varphi_2 : \mathtt{Formula}$, $b_1 : \mathtt{Bool}$, $b_2 : \mathtt{Bool}$, $b_3 : \mathtt{Bool}$.
2)

Dalla definizione di $\mathtt{GG}$ si ha:

$$
\begin{array}{rcl}
\mathtt{GG}\,(x_1 \vee \neg x_1) & = & \neg(\neg(\mathtt{GG}\, x_1) \wedge \neg(\mathtt{GG}\,(\neg x_2))) \\
& := & \neg(\neg x_1 \wedge \neg(\mathtt{GG}\,(\neg x_2))) \\
& := & \neg(\neg x_1 \wedge \neg(\neg(\mathtt{GG}\, x_2))) \\
& := & \neg(\neg x_1 \wedge \neg\neg x_2).
\end{array}
$$

**Theorem 4.**

$\forall \varphi : \mathtt{Formula}. \forall b_1 : \mathtt{Bool}. \forall b_2 : \mathtt{Bool}. \forall b_3 : \mathtt{Bool}. \quad \mathtt{truth}\,(\mathtt{GG}\,\varphi)\, b_1\, b_2\, b_3 = \mathtt{truth}\,\varphi\, b_1\, b_2\, b_3.$

*Dimostrazione.* Per dimostrare il teorema, possiamo andare per induzione strutturale su $\varphi : \texttt{Formula}$ per dimostrare la formula[7]:

$$\forall b_1 : \texttt{Bool}.\, \forall b_2 : \texttt{Bool}.\, \forall b_3 : \texttt{Bool}. \quad \texttt{truth}\,(\texttt{GG}\,\varphi)\, b_1\, b_2\, b_3 = \texttt{truth}\,\varphi\, b_1\, b_2\, b_3.$$

Per definizione di **Formula**, questo significa che, affinché questa dimostrazione per induzione sia corretta, dobbiamo risolvere esattamente i seguenti sei casi[8]:

- Caso $x_1$.

  Dobbiamo dimostrare la formula:

  $$\forall b_1 : \texttt{Bool}.\, \forall b_2 : \texttt{Bool}.\, \forall b_3 : \texttt{Bool}. \quad \texttt{truth}\,(\texttt{GG}\,x_1)\, b_1\, b_2\, b_3 = \texttt{truth}\,x_1\, b_1\, b_2\, b_3.$$

  Dati[9] $b_1 : \texttt{Bool}$, $b_2 : \texttt{Bool}$ e $b_3 : \texttt{Bool}$, dimostriamo: $\texttt{truth}\,(\texttt{GG}\,x_1)\, b_1\, b_2\, b_3 = \texttt{truth}\,x_1\, b_1\, b_2\, b_3$.

  Ma questa uguaglianza segue immediatamente dalla definizione di **GG** .

- Caso $x_2$.

  Analogo a quello sopra.

- Caso $x_3$.

  Analogo a quello sopra.

- Caso $\neg\varphi$, con $\varphi : \texttt{Formula}$.

  L'Ipotesi Induttiva è la formula:

  $$\forall b_1 : \texttt{Bool}.\, \forall b_2 : \texttt{Bool}.\, \forall b_3 : \texttt{Bool}. \quad \texttt{truth}\,(\texttt{GG}\,\varphi)\, b_1\, b_2\, b_3 = \texttt{truth}\,\varphi\, b_1\, b_2\, b_3.$$

  Avendo a disposizione l'Ipotesi Induttiva, dobbiamo dimostrare la formula:

  $$\forall b_1 : \texttt{Bool}.\, \forall b_2 : \texttt{Bool}.\, \forall b_3 : \texttt{Bool}. \quad \texttt{truth}\,(\texttt{GG}\,(\neg\varphi))\, b_1\, b_2\, b_3 = \texttt{truth}\,(\neg\varphi)\, b_1\, b_2\, b_3.$$

---

[7] Nota che qui è sparito il primo quantificatore, quello su cui vado per induzione!

[8] Osservazione: Guardando la definizione di **GG** , vediamo che per i casi base (le $x_i$), la funzione **GG** non fa nulla (si dice che "agisce come l'identità"); sui casi ricorsivi **Formula** ∧ **Formula** e ¬**Formula**, la sua azione è semplicemente quella di propagarsi ricorsivamente, lasciando intatta la "struttura" dell'input (si dice che "agisce come un omomorfismo"); l'unico caso nel quale la funzione **GG** fa qualcosa di diverso è il caso **Formula** ∨ **Formula**. Ancora prima di fare la dimostrazione dei vari casi, ci aspettiamo dunque che: nei casi base la formula da dimostrare sia triviale per definizione di **GG** ; nei casi **Formula** ∧ **Formula** e ¬**Formula** la formula da dimostrare si dimostri semplicemente con una chiamata ricorsiva alle ipotesi induttive; l'unico caso non immediato sarà il caso **Formula** ∨ **Formula**. Se tutto va bene, vedremo nelle prossime righe che infatti la nostra previsione è corretta.

[9] Che regole di DN stiamo usando qui?

Dati $b_1 : \texttt{Bool}$, $b_2 : \texttt{Bool}$ e $b_3 : \texttt{Bool}$, dimostriamo: $\texttt{truth}\,(\texttt{GG}\,(\neg\varphi))\,b_1\,b_2\,b_3 = \texttt{truth}\,(\neg\varphi)\,b_1\,b_2\,b_3$.

Sviluppando il membro sinistro abbiamo:

$$
\begin{array}{rcll}
\texttt{truth}\,(\texttt{GG}\,(\neg\varphi))\,b_1\,b_2\,b_3 & = & \texttt{truth}\,(\neg(\texttt{GG}\,\varphi))\,b_1\,b_2\,b_3 & \textit{per def. di } \texttt{GG} \\
 & = & \texttt{not}\,(\texttt{truth}\,(\texttt{GG}\,\varphi)\,b_1\,b_2\,b_3) & \textit{per def. di } \texttt{truth} \\
 & = & \texttt{not}\,(\texttt{truth}\,\varphi\,b_1\,b_2\,b_3) & \textit{per l'Ipotesi Induttiva.}
\end{array}
$$

Per la tranisitività di =, ci siamo dunque ricondotti a dover dimostrare:

$$\texttt{not}\,(\texttt{truth}\,\varphi\,b_1\,b_2\,b_3) \quad = \quad \texttt{truth}\,(\neg\varphi)\,b_1\,b_2\,b_3$$

che è proprio la definizione di **truth** .

- Caso $\varphi_1 \wedge \varphi_2$, con $\varphi_1 : \texttt{Formula}$, $\varphi_2 : \texttt{Formula}$.

  Abbiamo due Ipotesi Induttive, che sono le formule:

  $$\forall b_1 : \texttt{Bool}.\,\forall b_2 : \texttt{Bool}.\,\forall b_3 : \texttt{Bool}. \quad \texttt{truth}\,(\texttt{GG}\,\varphi_1)\,b_1\,b_2\,b_3 = \texttt{truth}\,\varphi_1\,b_1\,b_2\,b_3.$$

  $$\forall b_1 : \texttt{Bool}.\,\forall b_2 : \texttt{Bool}.\,\forall b_3 : \texttt{Bool}. \quad \texttt{truth}\,(\texttt{GG}\,\varphi_2)\,b_1\,b_2\,b_3 = \texttt{truth}\,\varphi_2\,b_1\,b_2\,b_3.$$

  Avendo a disposizione le Ipotesi Induttive, dobbiamo dimostrare la formula:

  $$\forall b_1 : \texttt{Bool}.\,\forall b_2 : \texttt{Bool}.\,\forall b_3 : \texttt{Bool}. \quad \texttt{truth}\,(\texttt{GG}\,(\varphi_1{\wedge}\varphi_2))\,b_1\,b_2\,b_3 = \texttt{truth}\,(\varphi_1{\wedge}\varphi_2)\,b_1\,b_2\,b_3.$$

  Dati $b_1 : \texttt{Bool}$, $b_2 : \texttt{Bool}$ e $b_3 : \texttt{Bool}$, dimostriamo: $\texttt{truth}\,(\texttt{GG}\,(\varphi_1{\wedge}\varphi_2))\,b_1\,b_2\,b_3 = \texttt{truth}\,(\varphi_1 \wedge \varphi_2)\,b_1\,b_2\,b_3$.

  Sviluppando il membro sinistro abbiamo:

  $$
  \begin{array}{rcl}
  \texttt{truth}\,(\texttt{GG}\,(\varphi_1 \wedge \varphi_2))\,b_1\,b_2\,b_3 & = & \texttt{truth}\,((\texttt{GG}\,\varphi_1) \wedge (\texttt{GG}\,\varphi_2)))\,b_1\,b_2\,b_3 \\
   & & \hfill \textit{per def. di } \texttt{GG} \\
   & = & \texttt{and}\,(\texttt{truth}\,(\texttt{GG}\,\varphi_1)\,b_1\,b_2\,b_3)\,(\texttt{truth}\,(\texttt{GG}\,\varphi_2)\,b_1\,b_2\,b_3) \\
   & & \hfill \textit{per def. di } \texttt{truth} \\
   & = & \texttt{and}\,(\texttt{truth}\,\varphi_1\,b_1\,b_2\,b_3)\,(\texttt{truth}\,\varphi_2\,b_1\,b_2\,b_3) \\
   & & \hfill \textit{per le II.}
  \end{array}
  $$

  Per la tranisitività di =, ci siamo dunque ricondotti a dover dimostrare:

  $$\texttt{and}\,(\texttt{truth}\,\varphi_1\,b_1\,b_2\,b_3)\,(\texttt{truth}\,\varphi_2\,b_1\,b_2\,b_3) \quad = \quad \texttt{truth}\,(\varphi_1 \wedge \varphi_2)\,b_1\,b_2\,b_3$$

  che è proprio la definizione di **truth** .

- Caso $\varphi_1 \vee \varphi_2$, con $\varphi_1 : \texttt{Formula}$, $\varphi_2 : \texttt{Formula}$.

  Abbiamo due Ipotesi Induttive, che sono le formule:

  $$\forall b_1 : \texttt{Bool}. \forall b_2 : \texttt{Bool}. \forall b_3 : \texttt{Bool}. \quad \texttt{truth}\,(\texttt{GG}\,\varphi_1)\,b_1\,b_2\,b_3 = \texttt{truth}\,\varphi_1\,b_1\,b_2\,b_3.$$

  $$\forall b_1 : \texttt{Bool}. \forall b_2 : \texttt{Bool}. \forall b_3 : \texttt{Bool}. \quad \texttt{truth}\,(\texttt{GG}\,\varphi_2)\,b_1\,b_2\,b_3 = \texttt{truth}\,\varphi_2\,b_1\,b_2\,b_3.$$

  Avendo a disposizione le Ipotesi Induttive, dobbiamo dimostrare la formula:

  $$\forall b_1 : \texttt{Bool}. \forall b_2 : \texttt{Bool}. \forall b_3 : \texttt{Bool}. \quad \texttt{truth}\,(\texttt{GG}\,(\varphi_1 \vee \varphi_2))\,b_1\,b_2\,b_3 = \texttt{truth}\,(\varphi_1 \vee \varphi_2)\,b_1\,b_2\,b_3.$$

  Dati $b_1 : \texttt{Bool}$, $b_2 : \texttt{Bool}$ e $b_3 : \texttt{Bool}$, dimostriamo: $\texttt{truth}\,(\texttt{GG}\,(\varphi_1 \vee \varphi_2))\,b_1\,b_2\,b_3 = \texttt{truth}\,(\varphi_1 \vee \varphi_2)\,b_1\,b_2\,b_3$.

  Sviluppando il membro sinistro abbiamo:

  $$\begin{array}{rll} & \texttt{truth}\,(\texttt{GG}\,(\varphi_1 \vee \varphi_2))\,b_1\,b_2\,b_3 & \\ = & \texttt{truth}\,(\neg(\neg(\texttt{GG}\,\varphi_1) \wedge \neg(\texttt{GG}\,\varphi_2)))\,b_1\,b_2\,b_3 & \textit{per def. di } \texttt{GG} \\ = & \texttt{not}\,(\texttt{truth}\,(\neg(\texttt{GG}\,\varphi_1) \wedge \neg(\texttt{GG}\,\varphi_2))\,b_1\,b_2\,b_3) & \textit{per def. di } \texttt{truth} \\ = & \texttt{not}\,(\texttt{and}\,(\texttt{truth}\,(\neg(\texttt{GG}\,\varphi_1))\,b_1\,b_2\,b_3))\,(\texttt{truth}\,(\neg(\texttt{GG}\,\varphi_2))\,b_1\,b_2\,b_3)) & \textit{per def. di } \texttt{truth} \\ = & \texttt{not}\,(\texttt{and}\,(\texttt{not}\,(\texttt{truth}\,(\texttt{GG}\,\varphi_1)\,b_1\,b_2\,b_3))\,(\texttt{not}\,(\texttt{truth}\,(\texttt{GG}\,\varphi_2)\,b_1\,b_2\,b_3))) & \textit{per def. di } \texttt{truth} \\ = & \texttt{not}\,(\texttt{and}\,(\texttt{not}\,(\texttt{truth}\,\varphi_1\,b_1\,b_2\,b_3))\,(\texttt{not}\,(\texttt{truth}\,\varphi_2\,b_1\,b_2\,b_3))) & \textit{per le due Ip. Ind.} \\ = & \texttt{or}\,(\texttt{not}\,(\texttt{not}\,(\texttt{truth}\,\varphi_1\,b_1\,b_2\,b_3)))\,(\texttt{not}\,(\texttt{not}\,(\texttt{truth}\,\varphi_2\,b_1\,b_2\,b_3))) & \textit{per il Teorema 1}^{10} \\ = & \texttt{or}\,(\texttt{truth}\,\varphi_1\,b_1\,b_2\,b_3)\,(\texttt{truth}\,\varphi_2\,b_1\,b_2\,b_3), & \end{array}$$

  dove l'ultima uguaglianza segue dal teorema $\forall b : \texttt{Bool}.\texttt{not}\,(\texttt{not}\,b) = b$, che il testo ci diceva poter usare (e che si può dimostrare immediatamente).

  Per la tranisitività di $=$, ci siamo dunque ricondotti a dover dimostrare:

  $$\texttt{or}\,(\texttt{truth}\,\varphi_1\,b_1\,b_2\,b_3)\,(\texttt{truth}\,\varphi_2\,b_1\,b_2\,b_3) \quad = \quad \texttt{truth}\,(\varphi_1 \vee \varphi_2)\,b_1\,b_2\,b_3.$$

  Ma questa è proprio la definizione di $\texttt{GG}$.

$\square$

**Esercizio 4: Il tipo delle esepressioni aritmetiche.**

1)

Definiamo la funzione $\texttt{eval} : \texttt{Expr} \to \texttt{Nat}$ per ricorsione strutturale:

$$\begin{array}{lcl} \texttt{eval}\,(\texttt{num}\,n) & := & n \\ \texttt{eval}\,(\texttt{add}\,e_1\,e_2) & := & \texttt{eval}\,e_1 + \texttt{eval}\,e_2 \\ \texttt{eval}\,(\texttt{mult}\,e_1\,e_2) & := & \texttt{eval}\,e_1 \cdot \texttt{eval}\,e_2, \end{array}$$

[10] Stiamo usando tale teorema sui booleani $\texttt{not}\,(\texttt{truth}\,\varphi_1\,b_1\,b_2\,b_3) : \texttt{Bool}$ e $\texttt{not}\,(\texttt{truth}\,\varphi_2\,b_1\,b_2\,b_3) : \texttt{Bool}$.

con $n : \texttt{Nat}$, $e_1 : \texttt{Expr}$, $e_2 : \texttt{Expr}$.

Definiamo la funzione $\texttt{if} : \texttt{Bool} \to \texttt{Expr} \to \texttt{Expr} \to \texttt{Expr}$ per ricorsione strutturale.

Dalla definizione di funzione ricorsiva strutturale che avete dato in aula, dobbiamo andare per ricorsione strutturale sul *primo* argomento della funzione:

$$\begin{aligned} \texttt{if}\,\texttt{true}\,e_1\,e_2 &:= e_1 \\ \texttt{if}\,\texttt{false}\,e_1\,e_2 &:= e_2, \end{aligned}$$

con $e_1 : \texttt{Expr}$, $e_2 : \texttt{Expr}$.

2)

Definiamo la funzione $\texttt{occZ} : \texttt{Expr} \to \texttt{Bool}$ per ricorsione strutturale:

$$\begin{aligned} \texttt{occZ}\,(\texttt{num}\,n) &:= \texttt{isZero}\,n \\ \texttt{occZ}\,(\texttt{add}\,e_1\,e_2) &:= \texttt{or}\,(\texttt{occZ}\,e_1)\,(\texttt{occZ}\,e_2) \\ \texttt{occZ}\,(\texttt{mult}\,e_1\,e_2) &:= \texttt{or}\,(\texttt{occZ}\,e_1)\,(\texttt{occZ}\,e_2), \end{aligned}$$

con $n : \texttt{Nat}$, $e_1 : \texttt{Expr}$, $e_3 : \texttt{Expr}$.

3)

Ricorda che il testo ci dice che per dimostrare il prossimo teorema, possiamo usare la seguente formula come assioma:

$$\forall e : \texttt{Expr}. \qquad (\texttt{eval}\,e = \texttt{0}) \vee (\texttt{eval}\,e \neq \texttt{0}). \tag{$H_1$}$$

**Theorem 5.**

$$\forall e : \texttt{Expr}. \qquad (\texttt{eval}\,e \neq \texttt{0}) \to (\texttt{occZ}\,(\texttt{semp}\,e) = \texttt{false}).$$

*Dimostrazione.* Per dimostrare il teorema, possiamo andare per induzione strutturale su $e : \texttt{Expr}$ per dimostrare la formula[11]:

$$(\texttt{eval}\,e \neq \texttt{0}) \to (\texttt{occZ}\,(\texttt{semp}\,e) = \texttt{false}).$$

Per definizione di $\texttt{Expr}$, questo significa che, affinché questa dimostrazione per infuzione sia corretta, dobbiamo risolvere esattamente i seguenti tre casi:

- Caso $\texttt{num}\,n$, con $n : \texttt{Nat}$.

  Dobbiamo dimostrare la formula:

  $$(\texttt{eval}\,(\texttt{num}\,n) \neq \texttt{0}) \to (\texttt{occZ}\,(\texttt{semp}\,(\texttt{num}\,n)) = \texttt{false}),$$

  ovvero dimostriamo $\texttt{occZ}\,(\texttt{semp}\,(\texttt{num}\,n)) = \texttt{false}$ sotto l'ipotesi $\texttt{eval}\,(\texttt{num}\,n) \neq \texttt{0}$.

[11] Nota che qui è sparito il primo quantificatore, quello su cui vado per induzione!

Siccome abbiamo:

$$\begin{array}{rcll} \texttt{occZ}\,(\texttt{semp}\,(\texttt{num}\,n)) & = & \texttt{occZ}\,(\texttt{num}\,n) & \textit{per def. di } \texttt{semp} \\ & = & \texttt{isZero}\,n & \textit{per def. di } \texttt{occZ}\,, \end{array}$$

dobbiamo dimostrare che $\texttt{isZero}\,n = \texttt{false}$.

Ma siccome abbiamo $\texttt{eval}\,(\texttt{num}\,n) = n$ per definizione di $\texttt{eval}$, la nostra ipotesi ci dice che $n \neq \texttt{0}$.

Ma allora possiamo concludere grazie al Teorema[12] 2.

- Caso $\texttt{add}\,e_1\,e_2$, con $e_1 : \texttt{Expr}$, $e_2 : \texttt{Expr}$.

  Le Ipotesi Induttive sono le formule:

  $$(\texttt{eval}\,e_1 \neq \texttt{0}) \to (\texttt{occZ}\,(\texttt{semp}\,e_1) = \texttt{false}) \qquad (II_1)$$

  $$(\texttt{eval}\,e_2 \neq \texttt{0}) \to (\texttt{occZ}\,(\texttt{semp}\,e_2) = \texttt{false}). \qquad (II_2)$$

  Avendo a disposizione le Ipotesi Induttive, dobbiamo dimostrare la formula:

  $$(\texttt{eval}\,(\texttt{add}\,e_1\,e_2) \neq \texttt{0}) \to (\texttt{occZ}\,(\texttt{semp}\,(\texttt{add}\,e_1\,e_2)) = \texttt{false}),$$

  ovvero, dimostriamo:

  $$\texttt{occZ}\,(\texttt{semp}\,(\texttt{add}\,e_1\,e_2)) = \texttt{false} \qquad (\star)$$

  sotto l'ipotesi:

  $$\texttt{eval}\,(\texttt{add}\,e_1\,e_2) \neq \texttt{0}. \qquad (H_2)$$

  Guardando la definizione di $\texttt{semp}\,(\texttt{add}\,e_1\,e_2)$, vediamo che il suo risultato dipende dal risultato di $\texttt{isZero}\,(\texttt{eval}\,e_1)$, ovvero, guardando la definizione di $\texttt{isZero}$ (o, più precisamente, il Teorema 2), dipende dal risultato di $\texttt{eval}\,e_1$. Decidiamo allora di andare per casi su questo risultato. Fortunatamente l'assioma $(H_1)$ ci permette proprio di farlo!

  Usando l'ipotesi $(H_1)$ su $e_1 : \texttt{Expr}$ otteniamo: $\texttt{eval}\,e_1 = \texttt{0} \vee \texttt{eval}\,e_1 \neq \texttt{0}$ e dunque, per la regola di eliminazione della disgiunzione, ci riduciamo a dover fornire le seguenti due dimostrazioni di $(\star)$:

  - Dimostriamo la formula $(\star)$ sotto l'ulteriore ipotesi $\texttt{eval}\,e_1 = \texttt{0}$.

    Da questa ipotesi, e dalla definizione di $\texttt{isZero}$, abbiamo $\texttt{isZero}\,(\texttt{eval}\,e_1) = \texttt{true}$ e dunque, dalla definizione di $\texttt{semp}$ abbiamo $\texttt{semp}\,(\texttt{add}\,e_1\,e_2) = \texttt{semp}\,e_2$.

[12] Lo stiamo applicando sul nostro $n : \texttt{Nat}$ e stiamo usando l'implicazione $\to$ del $\leftrightarrow$.

Dunque per dimostrare $(\star)$ ci basta dimostrare: $\texttt{occZ}\,(\texttt{semp}\,e_2) = \texttt{false}$.
Notiamo che questa è proprio la conclusione dell'Ipotesi Induttiva $(II_2)$! Dunque per finire ci basta dimostrare la premessa di $(II_2)$.

Usando l'Ipotesi Induttiva $(II_2)$, per dimostrare $\texttt{occZ}\,(\texttt{semp}\,e_2) = \texttt{false}$, grazie alla regola di eliminazione di $\rightarrow$, ci basta dimostrare $\texttt{eval}\,e_2 \neq \texttt{0}$.

Supponiamo dunque $\texttt{eval}\,e_2 = \texttt{0}$ e cerchiamo una contraddizione.

Ma siccome siamo sotto le ipotesi $\texttt{eval}\,e_1 = \texttt{0}$ e $\texttt{eval}\,e_2 = \texttt{0}$, dalla definizione di $\texttt{eval}$ otteniamo $\texttt{eval}\,(\texttt{add}\,e_1\,e_2) = \texttt{0} + \texttt{0} = \texttt{0}$[13] (usando la definizione di $+$), e questo contraddice l'ipotesi $(H_2)$.

– Dimostriamo la formula $(\star)$ sotto l'ulteriore ipotesi $\texttt{eval}\,e_1 \neq \texttt{0}$.
Da questa ipotesi, e dalla definizione di $\texttt{isZero}$, abbiamo $\texttt{isZero}\,(\texttt{eval}\,e_1) = \texttt{false}$ e dunque, dalla definizione di $\texttt{semp}$ abbiamo:

$$\texttt{semp}\,(\texttt{add}\,e_1\,e_2) = \texttt{if}\,(\texttt{isZero}\,(\texttt{eval}\,e_2))\,(\texttt{semp}\,e_1)\,(\texttt{add}\,(\texttt{semp}\,e_1)\,(\texttt{semp}\,e_2)).$$

Analogamente a prima, ora vediamo che il risultato di $\texttt{semp}\,(\texttt{add}\,e_1\,e_2)$ dipende dal risultato di $\texttt{isZero}\,(\texttt{eval}\,e_2)$, ovvero, guardando la definizione di $\texttt{isZero}$ (o, più precisamente, il Teorema 2), dipende dal risultato di $\texttt{eval}\,e_2$. Decidiamo allora di andare per casi su questo risultato. Fortunatamente l'assioma $(H_1)$ ci permette proprio di farlo!

Usando l'assioma $(H_1)$ su $e_2 : \texttt{Expr}$ otteniamo: $\texttt{eval}\,e_2 = \texttt{0} \vee \texttt{eval}\,e_2 \neq \texttt{0}$ e dunque, per la regola di eliminazione della disgiunzione, ci riduciamo a dover fornire le seguenti due dimostrazioni di $(\star)$:

* Dimostriamo la formula $(\star)$ sotto l'ulteriore ipotesi $\texttt{eval}\,e_2 = \texttt{0}$.
Da questa ipotesi, e dalla definizione di $\texttt{isZero}$, abbiamo $\texttt{isZero}\,(\texttt{eval}\,e_2) = \texttt{true}$ e dunque, dalla definizione di $\texttt{semp}$ abbiamo $\texttt{semp}\,(\texttt{add}\,e_1\,e_2) = \texttt{semp}\,e_1$.
Dunque per dimostrare $(\star)$ ci basta dimostrare: $\texttt{occZ}\,(\texttt{semp}\,e_1) = \texttt{false}$.
Analogamente a prima, notiamo che questa è proprio la conclusione dell'Ipotesi Induttiva $(II_1)$! Dunque per finire ci basta dimostrare la premessa di $(II_1)$.
Usando l'Ipotesi Induttiva $(II_1)$, per dimostrare $\texttt{occZ}\,(\texttt{semp}\,e_1) = \texttt{false}$, grazie alla regola di eliminazione di $\rightarrow$, ci basta dimostrare $\texttt{eval}\,e_1 \neq \texttt{0}$.

[13] Per essere pedanti, quando scriviamo due uguaglianze in questo modo, intendiamo che abbiamo due uguaglianze: quella tra il membro a sinistra e quello al centro, e quella tra il membro al centro e quello a destra. Dopodiché, per la transitività di $=$, deduciamo l'uguaglianza tra il membro di sinistra e quello di destra, che è l'uguaglianza che intendiamo davvero considerare.

Ma questa è proprio una delle nostre ipotesi correnti[14], dunque abbiamo finito.

∗ Dimostriamo la formula $(\star)$ sotto l'ulteriore ipotesi $\texttt{eval}\, e_2 \neq \texttt{0}$.
Da questa ipotesi, e dalla definizione di $\texttt{isZero}$, abbiamo $\texttt{isZero}\,(\texttt{eval}\, e_2) = \texttt{false}$ e dunque, dalla definizione di $\texttt{semp}$ abbiamo $\texttt{semp}\,(\texttt{add}\, e_1\, e_2) = \texttt{add}\,(\texttt{semp}\, e_1)\,(\texttt{semp}\, e_2)$ ed infine, dalla definizione di $\texttt{occZ}$, abbiamo $\texttt{occZ}\,(\texttt{semp}\,(\texttt{add}\, e_1\, e_2)) = \texttt{or}\,(\texttt{occZ}\,(\texttt{semp}\, e_1))\,(\texttt{occZ}\,(\texttt{semp}\, e_2))$.
Ricordando che il nostro obiettivo è dimostrare $(\star)$, ci siamo dunque ricondotti a dover dimostrare:

$$\texttt{or}\,(\texttt{occZ}\,(\texttt{semp}\, e_1))\,(\texttt{occZ}\,(\texttt{semp}\, e_2)) = \texttt{false}.$$

Ma siccome siamo sotto entrmbe le ipotesi $\texttt{eval}\, e_1 \neq \texttt{0}$ e $\texttt{eval}\, e_2 \neq \texttt{0}$, possiamo usare le Ipotesi induttive $(II_1)$ e $(II_2)$ per ottenere (grazie alla regola di eliminazione di $\to$), le formule $\texttt{occZ}\,(\texttt{semp}\, e_1) = \texttt{false}$ e $\texttt{occZ}\,(\texttt{semp}\, e_2) = \texttt{false}$. Ma allora otteniamo:

$$\begin{array}{rcll} \texttt{or}\,(\texttt{occZ}\,(\texttt{semp}\, e_1))\,(\texttt{occZ}\,(\texttt{semp}\, e_2)) & = & \texttt{or false false} & \textit{per quanto appena detto} \\ & = & \texttt{false} & \textit{per def. di } \texttt{or}, \end{array}$$

e grazie alla transitività di $=$, abbiamo proprio dimostrato $(\star)$.

- Caso $\texttt{mult}\, e_1\, e_2$, con $e_1 : \texttt{Expr}$, $e_2 : \texttt{Expr}$.
  Le Ipotesi Induttive sono le formule:

$$(\texttt{eval}\, e_1 \neq \texttt{0}) \to (\texttt{occZ}\,(\texttt{semp}\, e_1) = \texttt{false}) \qquad (II_1)$$

$$(\texttt{eval}\, e_2 \neq \texttt{0}) \to (\texttt{occZ}\,(\texttt{semp}\, e_2) = \texttt{false}). \qquad (II_2)$$

  Avendo a disposizione le Ipotesi Induttive, dobbiamo dimostrare la formula:

$$(\texttt{eval}\,(\texttt{mult}\, e_1\, e_2) \neq \texttt{0}) \to (\texttt{occZ}\,(\texttt{semp}\,(\texttt{mult}\, e_1\, e_2)) = \texttt{false}),$$

  ovvero, dimostriamo:

$$\texttt{occZ}\,(\texttt{semp}\,(\texttt{mult}\, e_1\, e_2)) = \texttt{false} \qquad (\star)$$

[14] Notate come stiamo esattamente usando la gestione delle ipotesi che facevamo in DN o Matita, sotto la terminologia di ipotesi vive/morte, attive/scaricate ecc? In questo punto della dimostrazione, per esempio, l'ipotesi $\texttt{eval}\, e_1 \neq \texttt{0}$ è viva, così come l'ipotesi $\texttt{eval}\, e_2 \neq \texttt{0}$, ma mentre la seconda sarà scaricata appena finito questo sotto-sotto-caso, la prima rimane viva per tutto il sotto-caso (per esempio, infatti, la useremo anche nel prossimo sotto-sotto-caso). Se avete pazienza, e volete divertirvi, potete addirittura provare a riscrivervi tutta questa dimostrazione col formalismo degli alberi di DN, è solo un modo di scrivere ancora più pedante ed esplicito, ma tutto torna! Con formalismi nettamente più potenti della DN che avete visto voi in aula, un giorno forse vedrete che addirittura "tutta" la matematica può, in principio, essere scritta in questo modo!

sotto l'ipotesi:

$$\texttt{eval}\,(\texttt{mult}\,e_1\,e_2) \neq \texttt{0}. \tag{$H_2$}$$

Guardando la definizione di $\texttt{semp}\,(\texttt{mult}\,e_1\,e_2)$, vediamo che il suo risultato dipende dal risultato di $\texttt{isZero}\,(\texttt{eval}\,e_1)$, ovvero, guardando la definizione di $\texttt{isZero}$ (o, più precisamente, il Teorema 2), dipende dal risultato di $\texttt{eval}\,e_1$. Decidiamo allora di andare per casi su questo risultato. Fortunatamente l'assioma $(H_1)$ ci permette proprio di farlo!

Usando l'assioma $(H_1)$ su $e_1 : \texttt{Expr}$ otteniamo: $\texttt{eval}\,e_1 = \texttt{0} \vee \texttt{eval}\,e_1 \neq \texttt{0}$ e dunque, per la regola di eliminazione della disgiunzione, ci riduciamo a dover fornire le seguenti due dimostrazioni di $(\star)$:

- Dimostriamo la formula $(\star)$ sotto l'ulteriore ipotesi $\texttt{eval}\,e_1 = \texttt{0}$.
  Ma questa ipotesi è assurda, ovvero usandola possiamo dedurre una contraddizione[15]: infatti da essa, e dalla definizione di $\texttt{isZero}$, abbiamo $\texttt{isZero}\,(\texttt{eval}\,e_1) = \texttt{true}$ e dunque, dalla definizione di $\texttt{eval}$ abbiamo $\texttt{eval}\,(\texttt{mult}\,e_1\,e_2) = \texttt{0} \cdot \texttt{eval}\,e_2 = \texttt{0}$ (usando la definizione di $\cdot$). Ma (usando la transitività di $=$) questo contraddice $(H_2)$. Siccome abbiamo trovato una contraddizione, abbiamo finito perché (grazie alla regola di eliminazione del $\bot$) possiamo dedurne qualsiasi formula, in particolare la nostra cara $(\star)$.
- Dimostriamo la formula $(\star)$ sotto l'ulteriore ipotesi $\texttt{eval}\,e_1 \neq \texttt{0}$.
  Da questa ipotesi, e dalla definizione di $\texttt{isZero}$, abbiamo $\texttt{isZero}\,(\texttt{eval}\,e_1) = \texttt{false}$ e dunque, dalla definizione di $\texttt{semp}$ abbiamo:

  $$\texttt{semp}\,(\texttt{mult}\,e_1\,e_2) = \texttt{if}\,(\texttt{isZero}\,(\texttt{eval}\,e_2))\,(\texttt{num}\,\texttt{0})\,(\texttt{mult}\,(\texttt{semp}\,e_1)\,(\texttt{semp}\,e_2)).$$

  Analogamente a prima, ora vediamo che il risultato di $\texttt{semp}\,(\texttt{mult}\,e_1\,e_2)$ dipende dal risultato di $\texttt{isZero}\,(\texttt{eval}\,e_2)$, ovvero, guardando la definizione di $\texttt{isZero}$ (o, più precisamente, il Teorema 2), dipende dal risultato di $\texttt{eval}\,e_2$. Decidiamo allora di andare per casi su questo risultato. Fortunatamente l'assioma $(H_1)$ ci permette proprio di farlo!
  Usando l'assioma $(H_1)$ su $e_2 : \texttt{Expr}$ otteniamo: $\texttt{eval}\,e_2 = \texttt{0} \vee \texttt{eval}\,e_2 \neq \texttt{0}$ e dunque, per la regola di eliminazione della disgiunzione, ci riduciamo a dover fornire le seguenti due dimostrazioni di $(\star)$:
  * Dimostriamo la formula $(\star)$ sotto l'ulteriore ipotesi $\texttt{eval}\,e_2 = \texttt{0}$.
    Ma questa ipotesi è assurda, ovvero usandola possiamo dedurre una contraddizione[16]: infatti da essa, e dalla definizione di $\texttt{isZero}$, abbiamo $\texttt{isZero}\,(\texttt{eval}\,e_2) = \texttt{true}$ e dunque, dalla definizione di $\texttt{eval}$

[15] Non è un ragionamento per assurdo!
[16] Non è un ragionamento per assurdo!

abbiamo $\texttt{eval}\,(\texttt{mult}\,e_1\,e_2) = \texttt{eval}\,e_1 \cdot \texttt{0} = \texttt{0}$ (usando il Teorem 3 su $\texttt{eval}\,e_1 : \texttt{Nat}$). Ma (usando la transitività di $=$) questo contraddice $(H_2)$. Siccome abbiamo trovato una contraddizione, abbiamo finito perché (grazie alla regola di eliminazione del $\perp$) possiamo dedurne qualsiasi formula, in particolare la nostra cara $(\star)$.

* Dimostriamo la formula $(\star)$ sotto l'ulteriore ipotesi $\texttt{eval}\,e_2 \neq \texttt{0}$.
Da questa ipotesi, e dalla definizione di $\texttt{isZero}$, abbiamo $\texttt{isZero}\,(\texttt{eval}\,e_2) = \texttt{false}$ e dunque, dalla definizione di $\texttt{semp}$ abbiamo $\texttt{semp}\,(\texttt{mult}\,e_1\,e_2) = \texttt{mult}\,(\texttt{semp}\,e_1)\,(\texttt{semp}\,e_2)$ ed infine, dalla definizione di $\texttt{occZ}$, abbiamo $\texttt{occZ}\,(\texttt{semp}\,(\texttt{mult}\,e_1\,e_2)) = \texttt{or}\,(\texttt{occZ}\,(\texttt{semp}\,e_1))\,(\texttt{occZ}\,(\texttt{semp}\,e_2))$.
Ricordando che il nostro obiettivo è dimostrare $(\star)$, ci siamo dunque ricondotti a dover dimostrare:

$$\texttt{or}\,(\texttt{occZ}\,(\texttt{semp}\,e_1))\,(\texttt{occZ}\,(\texttt{semp}\,e_2)) = \texttt{false}.$$

Ma siccome siamo sotto entrmbe le ipotesi $\texttt{eval}\,e_1 \neq \texttt{0}$ e $\texttt{eval}\,e_2 \neq \texttt{0}$, possiamo usare le Ipotesi induttive $(II_1)$ e $(II_2)$ per ottenere (grazie alla regola di eliminazione di $\to$), le formule $\texttt{occZ}\,(\texttt{semp}\,e_1) = \texttt{false}$ e $\texttt{occZ}\,(\texttt{semp}\,e_2) = \texttt{false}$. Ma allora otteniamo:

$$\begin{array}{rcll} \texttt{or}\,(\texttt{occZ}\,(\texttt{semp}\,e_1))\,(\texttt{occZ}\,(\texttt{semp}\,e_2)) & = & \texttt{or}\,\texttt{false}\,\texttt{false} & \textit{per quanto appena detto} \\ & = & \texttt{false} & \textit{per def. di } \texttt{or}, \end{array}$$

e grazie alla transitività di $=$, abbiamo proprio dimostrato $(\star)$.

$\square$