

Curry-Howard'i vastavus

Curry-Howard correspondence (*en.wikipedia.org*)

The **Curry–Howard correspondence** is the direct relationship between computer programs and proofs in constructive mathematics. Also known as **Curry–Howard isomorphism**, **proofs-as-programs correspondence** and **formulae-as-types correspondence**, it refers to the generalization of a syntactic analogy between systems of formal logic and computational calculi that was first discovered by the American mathematician Haskell Curry and logician William Alvin Howard.

Klassikaline vs. konstruktiivne loogika

Klassikaline loogika

- Iga väide on kas tõene või vale.
- Põhiküsimus:

"Kas antud väide on tõene või väär?"

Klassikaline vs. konstruktiivne loogika

Klassikaline loogika

- Iga väide on kas tõene või vale.
- Põhiküsimus:

"Kas antud väide on tõene või väär?"

Konstruktiivne loogika

- Väide on tõene vaid siis, kui suudame selle tõesust tõestada.
- Põhiküsimus:

"Kuidas antud väide saab tõeseks?"

Klassikaline vs. konstruktiivne loogika

Klassikaline loogika

- Iga väide on kas tõene või vale.
- Põhiküsimus:

Klassikalised tautoloogiad, mis konstruktiivselt ei kehti

$$A \vee \neg A$$

$$\neg\neg A \supset A$$

$$((A \supset B) \supset A) \supset A$$

Ko

- Väide on tõene vaid siis, kui suudame selle tõesust tõestada.
- Põhiküsimus:

"Kuidas antud väide saab tõeseks?"

Loomulik tuletus

- Tuletusreeglite üldkuju:

$$\frac{P_1 P_2 \dots P_n}{P_0}$$

Loomulik tuletus

- Tuletusreeglite üldkuju:

$$\frac{P_1 \quad P_2 \quad \dots \quad P_n}{P_0}$$

- P_1, \dots, P_n on eeldused, P_0 is a järeldus.
- Kui $n = 0$ (eeldused puuduvad), siis vastav tuletusreegel on aksioom.

Loomulik tuletus

- Tuletusreeglite üldkuju:

$$\frac{P_1 \quad P_2 \quad \dots \quad P_n}{P_0}$$

- Iga konnektiiviga (\wedge , \vee , ...) on seotud kaht liiki reegleid.
- **Sissetoomise reeglid:**
 - Konnektiiv esineb järelduses P_0 .
 - "Kuidas näidata konnektiiviga väite tõesust?"
- **Väljaviimise reeglid:**
 - Konnektiiv esineb eelduses P_i .
 - "Kuidas kasutada konnektiiviga väite olemasolevat tõestust?"

Loomulik tuletus

- T **NB!**

Tavaliselt on konnektiivil üks sissetoomise ja üks väljaviimise reegel, kuid võib olla ka mitu või siis üldse mitte ühtegi antud liiki reeglit.

Lausearvutus

- Süntaks:

$$P ::= A \mid P \supset P \mid P \wedge P \mid P \vee P \mid \top \mid \perp \mid \neg P$$

Lausearvutus

- Süntaks:

$$P ::= A \mid P \supset P \mid P \wedge P \mid P \vee P \mid \top \mid \perp \mid \neg P$$

- Implikatsiooni tuletusreeglid:

- Sissetoomine:

$$\frac{\overline{P_1}^x \quad \vdots \quad P_2}{P_1 \supset P_2} \supset I^x$$

- Väljaviimine:

$$\frac{P_1 \supset P_2 \quad P_1}{P_2} \supset E$$

Lausearvutus

- Süntaks:

$$P ::= A \mid P \supset P \mid P \wedge P \mid P \vee P \mid \top \mid \perp \mid \neg P$$

- Konjunktsiooni** tuletusreeglid:

- Sissetoomine:

$$\frac{P_1 \quad P_2}{P_1 \wedge P_2} \wedge I$$

- Väljaviimine:

$$\frac{P_1 \wedge P_2}{P_1} \wedge E_L$$

$$\frac{P_1 \wedge P_2}{P_2} \wedge E_R$$

Lausearvutus

- Süntaks:

$$P ::= A \mid P \supset P \mid P \wedge P \mid P \vee P \mid \top \mid \perp \mid \neg P$$

- Disjunktsiooni tuletusreeglid:

- Sissetoomine:

$$\frac{P_1}{P_1 \vee P_2} \vee I_L$$

$$\frac{P_2}{P_1 \vee P_2} \vee I_R$$

- Väljaviimine:

$$\frac{\begin{array}{c} \overline{P_1} \quad x \\ \vdots \\ P_1 \vee P_2 \quad P_0 \end{array} \quad \begin{array}{c} \overline{P_2} \quad y \\ \vdots \\ P_0 \end{array}}{P_0} \vee E^{x,y}$$

Lausearvutus

- Süntaks:

$$P ::= A \mid P \supset P \mid P \wedge P \mid P \vee P \mid \top \mid \perp \mid \neg P$$

- Tõeväärtuste tuletusreeglid:

- Sissetoomine:

$$\frac{}{\top} \top I$$

- Väljaviimine:

$$\frac{\perp}{P} \perp E$$

Lausearvutus

- Süntaks:

$$P ::= A \mid P \supset P \mid P \wedge P \mid P \vee P \mid \top \mid \perp \mid \neg P$$

- Tõesuskonstandi saab defineerida "süntaktilise suhkruna":

$$\top \equiv \perp \supset \perp$$

$$\frac{\perp}{P} \perp E$$

Lausearvutus

- Süntaks:

$$P ::= A \mid P \supset P \mid P \wedge P \mid P \vee P \mid \top \mid \perp \mid \neg P$$

- Eituse tuletusreeglid:

- Sissetoomine:

$$\frac{\overline{P} \quad \dots \quad \perp}{\neg P} \neg\text{-I}^x$$

- Väljaviimine:

$$\frac{\neg P \quad P}{\perp} \neg\text{-E}$$

Lausearvutus

- Süntaks:

$$P ::= A \mid P \supset P \mid P \wedge P \mid P \vee P \mid \top \mid \perp \mid \neg P$$

- Eituse tuletusreeglid:

Eituse saab defineerida "süntaktilise suhkruna":

$$\neg P \equiv P \supset \perp$$

- Väljaviimine:

$$\frac{\neg P \quad P}{\perp} \neg\text{-E}$$

Lausearvutus

- Süntaks:

$$P ::= A \mid P \supset P \mid P \wedge P \mid P \vee P \mid \top \mid \perp \mid \neg P$$

- Esitatud reeglid annavad **intuitsionistliku** lausearvutuse IPC.
- Mõnikord kasutame väiksemaid fragmente.
- **Klassikalise** lausearvutuse saame lisades **kahekordse eituse elimineerimise** reegli:

$$\frac{\neg\neg P}{P}$$

Lausearvutus

Näide (1)

$$A \wedge B \supset B \wedge A$$

Lausearvutus

Näide (1)

$$\frac{\overline{A \wedge B} \quad x}{\vdots} \quad \frac{\vdots \quad B \wedge A}{\overline{A \wedge B \supset B \wedge A} \quad \supset I^F}$$

Lausearvutus

Näide (1)

$$\begin{array}{c}
 \frac{}{A \wedge B} \quad \text{⊗} \qquad \qquad \frac{}{A \wedge B} \quad \text{⊗} \\
 \vdots \qquad \qquad \qquad \vdots \\
 B \qquad \qquad \qquad A \\
 \hline
 \qquad \qquad \qquad B \wedge A \qquad \qquad \text{⊗} \\
 \hline
 \qquad \qquad \qquad \qquad \qquad \qquad \text{⊃I} \\
 \qquad \qquad \qquad \qquad \qquad \qquad A \wedge B \supset B \wedge A
 \end{array}$$

Lausearvutus

Näide (1)

$$\begin{array}{c}
 \frac{}{A \wedge B} \quad \text{⊗} \qquad \qquad \frac{}{A \wedge B} \quad \text{⊗} \\
 \hline
 B \qquad \qquad \qquad A \quad \wedge E_R \qquad \wedge E_L \\
 \hline
 B \wedge A \quad \wedge I \\
 \hline
 A \wedge B \supset B \wedge A \quad \supset I^{\text{F}}
 \end{array}$$

Lausearvutus

Näide (2)

$$(A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)$$

Lausearvutus

Näide (2)

$$\frac{\frac{}{(A \supset B) \wedge (A \supset C)} \quad x}{A \supset (B \wedge C)}}{(A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)} \supset I^{\#}$$

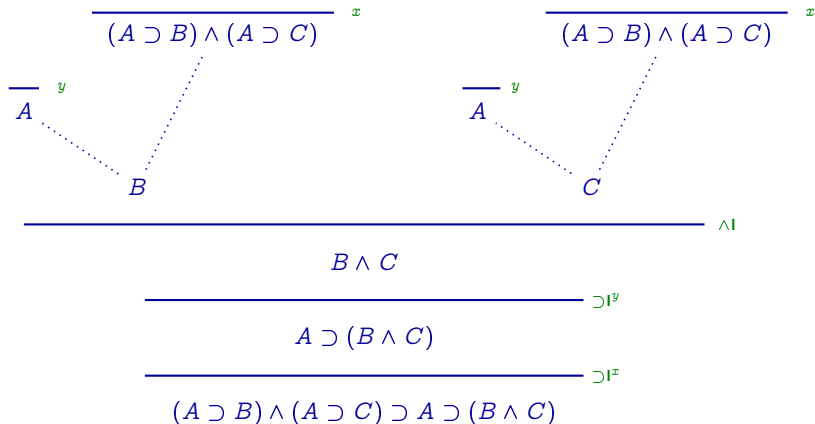
Lausearvutus

Näide (2)

$$\begin{array}{c}
 \frac{}{A} \quad y \qquad \frac{}{(A \supset B) \wedge (A \supset C)} \quad x \\
 \begin{array}{c} \text{.....} \\ \text{.....} \end{array} \\
 B \wedge C \\
 \hline
 A \supset (B \wedge C) \quad \supset I^y \\
 \hline
 (A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C) \quad \supset I^x
 \end{array}$$

Lausearvutus

Näide (2)



Lausearvutus

Näide (2)

$$\begin{array}{c}
 \frac{\frac{\frac{\frac{A}{y}}{A} \quad \frac{(A \supset B) \wedge (A \supset C)}{x}}{A \supset B} \quad \supset E}{B} \\
 \frac{\frac{\frac{\frac{A}{y}}{A} \quad \frac{(A \supset B) \wedge (A \supset C)}{x}}{A \supset C} \quad \supset E}{C} \\
 \frac{B \quad C}{B \wedge C} \wedge I \\
 \frac{\quad B \wedge C}{A \supset (B \wedge C)} \supset I^y \\
 \frac{A \supset (B \wedge C)}{(A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)} \supset I^x
 \end{array}$$

Lausearvutus

Näide (2)

$$\begin{array}{c}
 \frac{\frac{\frac{A}{y}}{A \supset B} \quad \frac{\frac{\frac{(A \supset B) \wedge (A \supset C)}{x}}{\wedge E_L}}{A \supset B}}{B} \supset E}{B \wedge C} \wedge I \\
 \frac{\frac{\frac{A}{y}}{A \supset C} \quad \frac{\frac{\frac{(A \supset B) \wedge (A \supset C)}{x}}{\wedge E_R}}{A \supset C}}{C} \supset E}{B \wedge C} \wedge I \\
 \frac{A \supset (B \wedge C)}{A \supset (B \wedge C)} \supset I^y \\
 \frac{A \supset (B \wedge C)}{(A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)} \supset I^x
 \end{array}$$

Lausearvutus

Näide (3)

$$A \supset B \supset B$$

Lausearvutus

Näide (3)

 $B \supset B$ $(B \supset B) \supset A \supset B \supset B$

 $\supset E$ $A \supset B \supset B$

Lausearvutus

Näide (3)

$$\begin{array}{c}
 \text{---} \quad x \\
 B \\
 \vdots \\
 B \\
 \text{---} \quad \supset I^x \\
 B \supset B \qquad (B \supset B) \supset A \supset B \supset B \\
 \hline
 A \supset B \supset B \quad \supset E
 \end{array}$$

Lausearvutus

Näide (3)

$$\begin{array}{c} \frac{}{B} \quad x \\ \hline B \supset B \quad \supset I^x \\ \quad (B \supset B) \supset A \supset B \supset B \\ \hline A \supset B \supset B \quad \supset E \end{array}$$

Lausearvutus

Näide (3)

$$\begin{array}{c}
 \frac{}{B} \quad x \\
 \hline
 B \supset B \quad \supset I^x \\
 \\
 \frac{}{B \supset B} \quad y \\
 \hline
 B \supset B \\
 \vdots \\
 A \supset B \supset B \\
 \hline
 (B \supset B) \supset A \supset B \supset B \quad \supset I^y \\
 \\
 \frac{}{A \supset B \supset B} \quad \supset E
 \end{array}$$

Lausearvutus

Näide (3)

$$\begin{array}{c}
 \frac{}{B} \quad x \\
 \hline
 B \supset B \quad \supset I^x \\
 \\
 \frac{}{B \supset B} \quad y \qquad \frac{}{A} \quad z \\
 \vdots \qquad \qquad \qquad \diagdown \\
 B \supset B \qquad \qquad \qquad A \\
 \hline
 A \supset B \supset B \quad \supset I^z \\
 \\
 \frac{}{B \supset B} \quad \supset I^x \qquad \frac{}{A \supset B \supset B} \quad \supset I^z \\
 \hline
 (B \supset B) \supset A \supset B \supset B \quad \supset I^y \\
 \\
 \frac{}{(B \supset B) \supset A \supset B \supset B} \quad \supset E \\
 \hline
 A \supset B \supset B
 \end{array}$$

Lausearvutus

Näide (3)

$$\begin{array}{c}
 \frac{}{B} \quad x \\
 \hline
 B \supset B \quad \supset I^x \\
 \\
 \frac{\frac{}{B \supset B} \quad y}{A \supset B \supset B} \quad \supset I^z \\
 \hline
 (B \supset B) \supset A \supset B \supset B \quad \supset I^y \\
 \hline
 A \supset B \supset B \quad \supset E
 \end{array}$$

Lausearvutus

Näide (3) — alternatiivne tõestus

$$A \supset B \supset B$$

Lausearvutus

Näide (3) — alternatiivne tõestus

$$\frac{\begin{array}{c} \text{--- } x \\ A \\ \vdots \\ B \supset B \end{array}}{\text{--- } \supset I^{\#}} \\ A \supset B \supset B$$

Lausearvutus

Näide (3) — alternatiivne tõestus

$$\begin{array}{c}
 \overline{A} \quad x \qquad \qquad \overline{B} \quad y \\
 \quad \quad \quad \cdot \quad \quad \quad \cdot \\
 \qquad \qquad \quad B \\
 \hline
 \qquad \qquad \qquad B \supset B \\
 \hline
 \qquad \qquad \qquad A \supset B \supset B
 \end{array}$$

Lausearvutus

Näide (3) — alternatiivne tõestus

$$\frac{\frac{\overline{\quad} \quad y}{B}}{\frac{\quad}{B \supset B} \supset I^y}}{\frac{\quad}{A \supset B \supset B} \supset I^x}$$

Tõestuste normaliseerimine

Teoreem:

Igal tõesel väitel on normaalkujuline tõestus.

Tõestuste normaliseerimine

Teoreem:

Igal tõesel väitel on normaalkujuline tõestus.

Normaliseerimisreeglid — implikatsioon:

$$\frac{\begin{array}{c} \vdots \Sigma \\ S \end{array} \quad \frac{\begin{array}{c} \overline{S} \\ \vdots \Pi \\ P \end{array}}{S \supset P}}{P} \rightarrow \begin{array}{c} \vdots \Sigma \\ S \\ \vdots \Pi \\ P \end{array}$$

Tõestuste normaliseerimine

Teoreem:

Igal tõesel väitel on normaalkujuline tõestus.

Normaliseerimisreeglid — **konjunktsioon**:

$$\frac{\frac{\begin{array}{c} \vdots \\ \Sigma \end{array} \quad \begin{array}{c} \vdots \\ \Pi \end{array}}{P_1 \quad P_2}}{P_1 \wedge P_2}}{P_1} \rightarrow \begin{array}{c} \vdots \\ \Sigma \end{array}$$

Tõestuste normaliseerimine

Teoreem:

Igal tõesel väitel on normaalkujuline tõestus.

Normaliseerimisreeglid — **disjunktsioon**:

$$\frac{\begin{array}{c} \vdots \ominus \\ P_1 \end{array}}{P_1 \vee P_2} \quad \frac{\begin{array}{c} \overline{P_1} \\ \vdots \Sigma \end{array}}{S} \quad \frac{\begin{array}{c} \overline{P_2} \\ \vdots \Pi \end{array}}{S}}{S} \rightarrow \frac{\begin{array}{c} \vdots \ominus \\ P_1 \\ \vdots \Sigma \end{array}}{S}$$

Curry-Howard'i isomorfism

Teoreem:

- (i) Kui $\Gamma \vdash M : \varphi$ in $\lambda(\rightarrow, \times, +)$, siis $|\Gamma| \vdash \varphi$ in $ND(\supset, \wedge, \vee)$, kus $|\Gamma| = \{\varphi \mid (x : \varphi) \in \Gamma\}$.
- (ii) Kui $\Gamma \vdash \varphi$ in $ND(\supset, \wedge, \vee)$, siis fragmendis $\lambda(\rightarrow, \times, +)$ leidub term M , selline et $\Delta \vdash M : \varphi$, kus $\Delta = \{x_\varphi : \varphi \mid \varphi \in \Gamma\}$.

Curry-Howard'i isomorfism

Curry-Howard'i vastavus

Teoree

- (i) K
| Γ
(ii) K
se

Proposition

Type

\perp

Void

\top

Unit

$A \supset B$

$A \rightarrow B$

$A \wedge B$

$A \times B$

$A \vee B$

$A + B$

in M ,

Curry-Howard'i isomorfism

Curry-Howard'i vastavus

Teoreem

- (i) K
| Γ
(ii) K
se

Intuitionistic logic

Proposition
Propositional variable
Proof
Hypothesis
Logical connective
Provability
Proof normalization

Typed λ -calculus

Type
Type variable
Term
Term variable
Type constructor
Type inhabitation
Reduction

n M ,