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

$$A \vee \neg A \qquad \neg\neg A \supset A \qquad ((A \supset B) \supset A) \supset A$$

Konstruktiivne loogika

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

  "Kuidas antud väide saab tõeseks?"

Loomulik tuletus

Tuletusreeglite üldkuju:

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

- P_i on otsused, millest $P_1, \ldots, P_n$ on eeldused ja P_0 on järeldus.
- Kui $n = 0$ (eeldused puuduvad), siis vastav tuletusreegel on aksioom.

Iga konnektiiviga ($\wedge$, $\vee$, $\ldots$) 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 väidet?"*

Loomulik tuletus (Gentzen-i stiilis)

Gentzen-i stiilis kasutatakse otsusteks sekventse on kujul: $\Gamma \vdash P$

- P on valem,
- Γ on kontekst, ehk (kohalike) hüpoteeside hulk

Sõltumata valemist kehtib hüpoteesi aksioom:

$$\frac{}{\Gamma, P \vdash P}\ Hyp$$

- Kui kontekstis leidub P, siis P kehtib (ilma lisatingimusteta).

Tihti algab arutelu küsimusega, kas valem P kehtib ilma hüpoteesideta ehk tühjas kontekstis. S.t. $\vdash P$.

Lausearvutus

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

Implikatsiooni tuletusreeglid:

- Sissetoomine:

$$\frac{\Gamma, P_1 \vdash P_2}{\Gamma \vdash P_1 \supset P_2} \;\supset\mathsf{I}$$

- Väljaviimine:

$$\frac{\Gamma \vdash P_1 \supset P_2 \quad \Gamma \vdash P_1}{\Gamma \vdash P_2} \;\supset\mathsf{E}$$

Konjunktsiooni tuletusreeglid:

- Sissetoomine:

$$\frac{\Gamma \vdash P_1 \quad \Gamma \vdash P_2}{\Gamma \vdash P_1 \wedge P_2} \;\wedge\mathsf{I}$$

- Väljaviimine:

$$\frac{\Gamma \vdash P_1 \wedge P_2}{\Gamma \vdash P_1} \;\wedge\mathsf{E}_L \qquad \frac{\Gamma \vdash P_1 \wedge P_2}{\Gamma \vdash P_2} \;\wedge\mathsf{E}_R$$

Lausearvutus

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

Disjunktsiooni tuletusreeglid:

- Sissetoomine:

$$\frac{\Gamma \vdash P_1}{\Gamma \vdash P_1 \vee P_2}\ \vee\mathsf{I}_L \qquad\qquad \frac{\Gamma \vdash P_2}{\Gamma \vdash P_1 \vee P_2}\ \vee\mathsf{I}_R$$

- Väljaviimine:

$$\frac{\Gamma \vdash P_1 \vee P_2 \quad \Gamma, P_1 \vdash P_0 \quad \Gamma, P_2 \vdash P_0}{\Gamma \vdash P_0}\ \vee\mathsf{E}$$

Tõeväärtuste tuletusreeglid:

- Sissetoomine:

$$\frac{}{\Gamma \vdash \top}\ \top\mathsf{I}$$

- Väljaviimine:

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash P}\ \bot\mathsf{E}$$

Lausearvutus

- Eituse defineerime *"süntaktilise suhkruna"*:

$$\neg P \quad \equiv \quad P \supset \bot$$

- Esitatud reeglid annavad intuitsionistliku lausearvutuse IPC.
- Klassikalise lausearvutuse saame lisades kahekordse eituse elimineerimise reegli:

$$\frac{\Gamma \vdash \neg\neg P}{\Gamma \vdash P}$$

Lausearvutus

Näide(1)

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

Lausearvutus

Näide(1)

$$\frac{A \wedge B \vdash B \wedge A}{\vdash A \wedge B \supset B \wedge A} \supset \mathrm{I}$$

Lausearvutus

Näide(1)

$$\dfrac{\dfrac{A \wedge B \vdash B \qquad A \wedge B \vdash A}{A \wedge B \vdash B \wedge A}\ \wedge\mathsf{I}}{\vdash A \wedge B \supset B \wedge A}\ \supset\mathsf{I}$$

Lausearvutus

Näide(1)

$$\dfrac{\dfrac{A \land B \vdash A \land B}{A \land B \vdash B}\,\land\mathbf{E}_R \qquad A \land B \vdash A}{\dfrac{A \land B \vdash B \land A}{\vdash A \land B \supset B \land A}\,\supset\mathbf{I}}\,\land\mathbf{I}$$

Lausearvutus

Näide(1)

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \wedge B \vdash A \wedge B}}{A \wedge B \vdash B}\;\wedge\mathsf{E}_R \qquad A \wedge B \vdash A}{A \wedge B \vdash B \wedge A}\;\wedge\mathsf{I}}{\vdash A \wedge B \supset B \wedge A}\;\supset\mathsf{I}$$

Lausearvutus

Näide(1)

$$
\dfrac{\dfrac{\dfrac{}{A \land B \vdash A \land B}}{A \land B \vdash B}\,\land\mathbf{E}_R \qquad \dfrac{A \land B \vdash A \land B}{A \land B \vdash A}\,\land\mathbf{E}_L}{\dfrac{A \land B \vdash B \land A}{\vdash A \land B \supset B \land A}\,\supset\mathbf{I}}\,\land\mathbf{I}
$$

Lausearvutus

Näide(1)

$$
\dfrac{\dfrac{\dfrac{}{A \wedge B \vdash A \wedge B}}{A \wedge B \vdash B}\,\wedge\mathbf{E}_R \qquad \dfrac{\dfrac{}{A \wedge B \vdash A \wedge B}}{A \wedge B \vdash A}\,\wedge\mathbf{E}_L}{\dfrac{A \wedge B \vdash B \wedge A}{\vdash A \wedge B \supset B \wedge A}\,\supset\mathbf{I}}\,\wedge\mathbf{I}
$$

Lausearvutus

Näide (2)

$$\dfrac{}{\vdash (A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)}\ \supset\mathsf{I}$$

Lausearvutus

Näide (2)

$$\dfrac{\dfrac{}{(A \supset B) \wedge (A \supset C) \vdash A \supset (B \wedge C)}\ {\supset}\mathsf{I}}{\vdash (A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)}\ {\supset}\mathsf{I}$$

Lausearvutus

Näide (2)

$$\dfrac{\dfrac{\dfrac{}{\Gamma = (A \supset B) \wedge (A \supset C), A \vdash B \wedge C}\,\wedge\mathrm{I}}{(A \supset B) \wedge (A \supset C) \vdash A \supset (B \wedge C)}\,\supset\mathrm{I}}{\vdash (A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)}\,\supset\mathrm{I}$$

Lausearvutus

Näide (2)

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash B}\,{\supset}\mathsf{E}}{\Gamma = (A \supset B) \wedge (A \supset C), A \vdash B \wedge C}\,{\wedge}\mathsf{I}}{(A \supset B) \wedge (A \supset C) \vdash A \supset (B \wedge C)}\,{\supset}\mathsf{I}}{\vdash (A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)}\,{\supset}\mathsf{I}
$$

Lausearvutus

Näide (2)

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash B}\,\supset\mathsf{E} \qquad \dfrac{}{\Gamma \vdash C}\,\supset\mathsf{E}}{\Gamma = (A \supset B) \wedge (A \supset C), A \vdash B \wedge C}\,\wedge\mathsf{I}}{(A \supset B) \wedge (A \supset C) \vdash A \supset (B \wedge C)}\,\supset\mathsf{I}}{\vdash (A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)}\,\supset\mathsf{I}$$

Lausearvutus

Näide (2)

$$
\dfrac{\dfrac{\dfrac{}{\Gamma \vdash A}\,Hyp \qquad \qquad}{\Gamma \vdash B}\,\supset\!E \qquad \dfrac{}{\Gamma \vdash C}\,\supset\!E}{\dfrac{\Gamma = (A \supset B) \wedge (A \supset C), A \vdash B \wedge C}{\dfrac{(A \supset B) \wedge (A \supset C) \vdash A \supset (B \wedge C)}{\vdash (A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)}\,\supset\!I}\,\supset\!I}\,\wedge I
$$

Lausearvutus

Näide (2)

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{Hyp}
\UnaryInfC{$\Gamma \vdash A$}
\AxiomC{}
\RightLabel{$\wedge\mathsf{E}_L$}
\UnaryInfC{$\Gamma \vdash A \supset B$}
\RightLabel{$\supset\mathsf{E}$}
\BinaryInfC{$\Gamma \vdash B$}
\AxiomC{}
\RightLabel{$\supset\mathsf{E}$}
\UnaryInfC{$\Gamma \vdash C$}
\RightLabel{$\wedge\mathsf{I}$}
\BinaryInfC{$\Gamma = (A \supset B) \wedge (A \supset C), A \vdash B \wedge C$}
\RightLabel{$\supset\mathsf{I}$}
\UnaryInfC{$(A \supset B) \wedge (A \supset C) \vdash A \supset (B \wedge C)$}
\RightLabel{$\supset\mathsf{I}$}
\UnaryInfC{$\vdash (A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)$}
\end{prooftree}
$$

Lausearvutus

Näide (2)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash A}\,Hyp \qquad \dfrac{\dfrac{}{\Gamma \vdash (A \supset B) \wedge (A \supset C)}\,Hyp}{\Gamma \vdash A \supset B}\,\wedge\mathsf{E}_L}{\Gamma \vdash B}\,\supset\mathsf{E} \qquad \dfrac{\qquad\qquad\qquad\qquad}{\Gamma \vdash C}\,\supset\mathsf{E}}{\Gamma = (A \supset B) \wedge (A \supset C), A \vdash B \wedge C}\,\wedge\mathsf{I}}{(A \supset B) \wedge (A \supset C) \vdash A \supset (B \wedge C)}\,\supset\mathsf{I}}{\vdash (A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)}\,\supset\mathsf{I}$$

Lausearvutus

Näide (2)

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{Hyp}
\UnaryInfC{$\Gamma \vdash A$}
\AxiomC{}
\RightLabel{Hyp}
\UnaryInfC{$\Gamma \vdash (A \supset B) \wedge (A \supset C)$}
\RightLabel{$\wedge\mathsf{E}_L$}
\UnaryInfC{$\Gamma \vdash A \supset B$}
\RightLabel{$\supset\mathsf{E}$}
\BinaryInfC{$\Gamma \vdash B$}
\AxiomC{}
\RightLabel{Hyp}
\UnaryInfC{$\Gamma \vdash A$}
\RightLabel{$\supset\mathsf{E}$}
\UnaryInfC{$\Gamma \vdash C$}
\RightLabel{$\wedge\mathsf{I}$}
\BinaryInfC{$\Gamma = (A \supset B) \wedge (A \supset C), A \vdash B \wedge C$}
\RightLabel{$\supset\mathsf{I}$}
\UnaryInfC{$(A \supset B) \wedge (A \supset C) \vdash A \supset (B \wedge C)$}
\RightLabel{$\supset\mathsf{I}$}
\UnaryInfC{$\vdash (A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)$}
\end{prooftree}
$$

Lausearvutus

Näide (2)

$$
\dfrac{
  \dfrac{
    \dfrac{}{\Gamma \vdash A}\,\mathit{Hyp}
    \qquad
    \dfrac{\dfrac{}{\Gamma \vdash (A \supset B) \wedge (A \supset C)}\,\mathit{Hyp}}{\Gamma \vdash A \supset B}\,\wedge\mathsf{E}_L
  }{\Gamma \vdash B}\,\supset\mathsf{E}
  \qquad
  \dfrac{
    \dfrac{}{\Gamma \vdash A}\,\mathit{Hyp}
    \qquad
    \dfrac{}{\Gamma \vdash A \supset C}\,\wedge\mathsf{E}_R
  }{\Gamma \vdash C}\,\supset\mathsf{E}
}{
  \dfrac{\Gamma = (A \supset B) \wedge (A \supset C), A \vdash B \wedge C}{
    \dfrac{(A \supset B) \wedge (A \supset C) \vdash A \supset (B \wedge C)}{\vdash (A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)}\,\supset\mathsf{I}
  }\,\supset\mathsf{I}
}\,\wedge\mathsf{I}
$$

Lausearvutus

Näide (2)

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{Hyp}
\UnaryInfC{$\Gamma \vdash A$}
\AxiomC{}
\RightLabel{Hyp}
\UnaryInfC{$\Gamma \vdash (A \supset B) \wedge (A \supset C)$}
\RightLabel{$\wedge\mathsf{E}_L$}
\UnaryInfC{$\Gamma \vdash A \supset B$}
\RightLabel{$\supset\mathsf{E}$}
\BinaryInfC{$\Gamma \vdash B$}
\AxiomC{}
\RightLabel{Hyp}
\UnaryInfC{$\Gamma \vdash A$}
\AxiomC{}
\RightLabel{Hyp}
\UnaryInfC{$\Gamma \vdash (A \supset B) \wedge (A \supset C)$}
\RightLabel{$\wedge\mathsf{E}_R$}
\UnaryInfC{$\Gamma \vdash A \supset C$}
\RightLabel{$\supset\mathsf{E}$}
\BinaryInfC{$\Gamma \vdash C$}
\RightLabel{$\wedge\mathsf{I}$}
\BinaryInfC{$\Gamma = (A \supset B) \wedge (A \supset C), A \vdash B \wedge C$}
\RightLabel{$\supset\mathsf{I}$}
\UnaryInfC{$(A \supset B) \wedge (A \supset C) \vdash A \supset (B \wedge C)$}
\RightLabel{$\supset\mathsf{I}$}
\UnaryInfC{$\vdash (A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)$}
\end{prooftree}
$$

Lausearvutus

Näide (3)

$$\dfrac{}{\vdash A \vee B \supset A \wedge B}\ \supset\!\mathsf{I}$$

Lausearvutus

Näide (3)

$$\dfrac{\dfrac{}{A \vee B \vdash A \wedge B}\ \wedge\mathrm{I}}{\vdash A \vee B \supset A \wedge B}\ \supset\mathrm{I}$$

Lausearvutus

Näide (3)

$$\dfrac{\dfrac{\dfrac{}{A \vee B \vdash A} \quad \dfrac{}{A \vee B \vdash B}}{A \vee B \vdash A \wedge B}\ \wedge\mathrm{I}}{\vdash A \vee B \supset A \wedge B}\ \supset\mathrm{I}$$

Lausearvutus

Näide (3)

$$
\dfrac{\dfrac{\dfrac{???}{A \vee B \vdash A} \quad \dfrac{???}{A \vee B \vdash B}}{A \vee B \vdash A \wedge B}\ \wedge\mathrm{I}}{\vdash A \vee B \supset A \wedge B}\ \supset\mathrm{I}
$$

Pole võimalik!

Lausearvutus

Näide (4)

$$\dfrac{}{\vdash A \supset B \supset B}\ {\supset}\mathsf{E}$$

Lausearvutus

Näide (4)

$$\dfrac{\dfrac{}{\vdash (B \supset B) \supset A \supset B \supset B}\,{\supset}\mathsf{I} \qquad \dfrac{}{\vdash B \supset B}\,{\supset}\mathsf{I}}{\vdash A \supset B \supset B}\,{\supset}\mathsf{E}$$

Lausearvutus

Näide (4)

$$
\dfrac{\dfrac{\dfrac{}{B \supset B \vdash A \supset B \supset B}\,\supset\mathsf{I}}{\vdash (B \supset B) \supset A \supset B \supset B}\,\supset\mathsf{I} \qquad \dfrac{}{\vdash B \supset B}\,\supset\mathsf{I}}{\vdash A \supset B \supset B}\,\supset\mathsf{E}
$$

Lausearvutus

Näide (4)

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{B \supset B, A \vdash B \supset B}\,Hyp}{B \supset B \vdash A \supset B \supset B}\supset\mathsf{I}}{\vdash (B \supset B) \supset A \supset B \supset B}\supset\mathsf{I} \qquad \dfrac{}{\vdash B \supset B}\supset\mathsf{I}}{\vdash A \supset B \supset B}\supset\mathsf{E}
$$

Lausearvutus

Näide (4)

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{Hyp}
\UnaryInfC{$B \supset B, A \vdash B \supset B$}
\RightLabel{$\supset$I}
\UnaryInfC{$B \supset B \vdash A \supset B \supset B$}
\RightLabel{$\supset$I}
\UnaryInfC{$\vdash (B \supset B) \supset A \supset B \supset B$}
\AxiomC{}
\RightLabel{Hyp}
\UnaryInfC{$B \vdash B$}
\RightLabel{$\supset$I}
\UnaryInfC{$\vdash B \supset B$}
\RightLabel{$\supset$E}
\BinaryInfC{$\vdash A \supset B \supset B$}
\end{prooftree}
$$

Lausearvutus

Näide (4) — alternatiivne tõestus

$$\dfrac{}{\vdash A \supset B \supset B}\ {\color{green}\supset\mathsf{I}}$$

Lausearvutus

Näide (4) — alternatiivne tõestus

$$\dfrac{\dfrac{}{A \vdash B \supset B}\,\supset\mathrm{I}}{\vdash A \supset B \supset B}\,\supset\mathrm{I}$$

Lausearvutus

Näide (4) — alternatiivne tõestus

$$\dfrac{\dfrac{\overline{A, B \vdash B}\,Hyp}{A \vdash B \supset B}\,{\supset}\mathsf{I}}{\vdash A \supset B \supset B}\,{\supset}\mathsf{I}$$

Tõestuste normaliseerimine

Teoreem:

Igal tõesel väitel on normaalkujuline tõestus.

Tõestuste normaliseerimine

Teoreem:

Igal tõesel väitel on normaalkujuline tõestus.

Normaliseerimisreeglid — implikatsioon:

$$
\dfrac{\dfrac{\begin{array}{c}\overline{\Gamma, S, \Gamma' \vdash S}\\ \vdots\ \Pi \\ \Gamma, S \vdash P\end{array}}{\Gamma \vdash S \supset P} \qquad \begin{array}{c}\vdots\ \Sigma \\ \Gamma \vdash S\end{array}}{\Gamma \vdash P}
\quad \to \quad
\begin{array}{c}\vdots\ \Sigma \\ \Gamma, \Gamma' \vdash S \\ \vdots\ \Pi \\ \Gamma \vdash P\end{array}
$$

Tõestuste normaliseerimine

Teoreem:

Igal tõesel väitel on normaalkujuline tõestus.

Normaliseerimisreeglid — konjunktsioon:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ \Sigma\\ \Gamma \vdash P_1\end{array} \quad \begin{array}{c}\vdots\ \Pi\\ \Gamma \vdash P_2\end{array}}{\Gamma \vdash P_1 \land P_2}}{\Gamma \vdash P_1} \quad \rightarrow \quad \begin{array}{c}\vdots\ \Sigma\\ P_1\end{array}$$

Tõestuste normaliseerimine

Teoreem:

Igal tõesel väitel on normaalkujuline tõestus.

Normaliseerimisreeglid — disjunktsioon:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\ \Theta\\ \Gamma \vdash P_1\end{array}}{\Gamma \vdash P_1 \lor P_2} \quad \begin{array}{c}\overline{\Gamma, P_1, \Gamma' \vdash P_1}\\ \vdots\ \Sigma \\ \Gamma, P_1 \vdash S\end{array} \quad \begin{array}{c}\overline{\Gamma, P_2, \Gamma'' \vdash P_2}\\ \vdots\ \Pi\\ \Gamma, P_2 \vdash S\end{array}}{\Gamma \vdash S} \quad \to \quad \begin{array}{c}\vdots\ \Theta\\ \Gamma, \Gamma' \vdash P_1\\ \vdots\ \Sigma\\ \Gamma \vdash S\end{array}$$

Curry-Howard'i isomorfism

Teoreem:

(i) Kui λ-termi M jaoks $\lambda(\rightarrow, \times, +)$-s on tõestatav $\Gamma \vdash M : \varphi$, siis $\{\varphi \mid (x : \varphi) \in \Gamma\} \vdash \varphi$ on tõestatav $ND(\supset, \wedge, \vee)$-s.

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

Curry-Howard'i isomorfism

Teoree

(i) K

$\{\varphi$

(ii) K $)$

lei

Curry-Howard'i vastavus

Propositsioon	Tüüp
$\bot$	Void
$\top$	Unit
$A \supset B$	$A \to B$
$A \wedge B$	$A \times B$
$A \vee B$	$A + B$

Curry-Howard'i isomorfism

Teoree

(i) K
{φ

(ii) K)
lei

Curry-Howard'i vastavus

Intuitsionistlik loogika	Tüüpidega λ-arvutus
Väide	Tüüp
Väite muutuja	Tüübimuutuja
Tõestus	Term
Hüpotees	Termi muutuja
Konnektiiv	Tüübikonstruktor
Tõestatavus	*Type inhabitation*
Tõestuse normaliseerimine	Reduktsioon