LTAT.03.019 Funktsionaalprogrammeerimine

Curry-Howard'i vastavus

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:

  "Kas antud väide on tõene või väär?"

Klassikalised tautoloogiad, mis konstruktiivselt ei kehti

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

Ko

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

  "Kuidas antud väide saab tõeseks?"

Loomulik tuletus

- Tueltusreeglite üldkuju:

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

Loomulik tuletus

- Tueltusreeglite 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

- Tueltusreeglite 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

- Tueltusreeglite üldkuju:

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

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:

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

Lausearvutus

- Süntaks:

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

- Implikatsiooni tuletusreeglid:
  - Sissetoomine:

$$\dfrac{\begin{array}{c}\overline{P_1}^{\,x}\\ \vdots \\ P_2\end{array}}{P_1 \supset P_2}\ \supset\mathrm{I}^x$$

  - Väljaviimine:

$$\dfrac{P_1 \supset P_2 \quad P_1}{P_2}\ \supset\mathrm{E}$$

Lausearvutus

- Süntaks:

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

- Konjunktsiooni tuletusreeglid:
  - Sissetoomine:

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

  - Väljaviimine:

$$\frac{P_1 \wedge P_2}{P_1} \wedge\mathrm{E}_L \qquad \frac{P_1 \wedge P_2}{P_2} \wedge\mathrm{E}_R$$

Lausearvutus

- Süntaks:

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

- Disjunktsiooni tuletusreeglid:
  - Sissetoomine:

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

  - Väljaviimine:

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

Lausearvutus

- Süntaks:

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

- Tõeväärtuste tuletusreeglid:
  - Sissetoomine:

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

  - Väljaviimine:

$$\frac{\bot}{P}\ \bot\mathrm{E}$$

Lausearvutus

- Süntaks:

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

- T

Tõesuskonstandi saab defineerida *"süntaktilise suhkruna"*:

$$\top \quad \equiv \quad \bot \supset \bot$$

P

Lausearvutus

- Süntaks:

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

- Eituse tuletusreeglid:
  - Sissetoomine:

$$\dfrac{\begin{array}{c}\overline{P}^{\,x}\\ \vdots\\ \bot\end{array}}{\neg P}\ \neg\mathrm{I}^{x}$$

  - Väljaviimine:

$$\dfrac{\neg P \quad P}{\bot}\ \neg\mathrm{E}$$

Lausearvutus

- Süntaks:

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

- Ei

Eituse saab defineerida *"süntaktilise suhkruna"*:

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

- Väljaviimine:

$$\frac{\neg P \quad P}{\bot}\ \neg\mathrm{E}$$

Lausearvutus

- Süntaks:

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

- 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)

$$\dfrac{\begin{array}{c}\dfrac{}{A \wedge B}\,x\\ \vdots\\ B \wedge A\end{array}}{A \wedge B \supset B \wedge A}\;{\supset}\mathrm{I}^{x}$$

Lausearvutus

Näide (1)

$$\cfrac{\cfrac{\begin{array}{c}\overline{A \wedge B}^{\;x}\\ \vdots\\ B\end{array} \qquad \begin{array}{c}\overline{A \wedge B}^{\;x}\\ \vdots\\ A\end{array}}{B \wedge A}\,\wedge\mathrm{I}}{A \wedge B \supset B \wedge A}\,\supset\mathrm{I}^{x}$$

Lausearvutus

Näide (1)

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \wedge B}\,x}{B}\,\wedge\mathrm{E}_R \qquad \dfrac{\dfrac{}{A \wedge B}\,x}{A}\,\wedge\mathrm{E}_L}{B \wedge A}\,\wedge\mathrm{I}}{A \wedge B \supset B \wedge A}\,\supset\mathrm{I}^x$$

Lausearvutus

Näide (2)

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

Lausearvutus

Näide (2)

$$\dfrac{\begin{array}{c}\dfrac{}{(A \supset B) \wedge (A \supset C)}\, x \\ \vdots \\ A \supset (B \wedge C)\end{array}}{(A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)}\, \supset\mathrm{I}^{x}$$

Lausearvutus

Näide (2)

$$\dfrac{\dfrac{\begin{array}{c}\overline{A}^{\,y} \qquad \overline{(A \supset B) \wedge (A \supset C)}^{\,x} \\ \vdots \\ B \wedge C\end{array}}{A \supset (B \wedge C)}\supset\mathrm{I}^{y}}{(A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)}\supset\mathrm{I}^{x}$$

Lausearvutus

Näide (2)

$$
\dfrac{\dfrac{\dfrac{\begin{array}{c}\overline{A}^{\,y}\qquad \overline{(A\supset B)\wedge(A\supset C)}^{\,x}\\ \vdots \\ B\end{array} \qquad \begin{array}{c}\overline{A}^{\,y}\qquad \overline{(A\supset B)\wedge(A\supset C)}^{\,x}\\ \vdots \\ C\end{array}}{B \wedge C}\,\wedge\mathrm{I}}{A \supset (B\wedge C)}\,\supset\mathrm{I}^{y}}{(A\supset B)\wedge(A\supset C)\supset A\supset(B\wedge C)}\,\supset\mathrm{I}^{x}
$$

Lausearvutus

Näide (2)

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A}\,y \qquad \begin{array}{c}\dfrac{}{(A \supset B) \wedge (A \supset C)}\,x \\ \vdots \\ A \supset B\end{array}}{B}\supset\mathrm{E} \qquad \dfrac{\dfrac{}{A}\,y \qquad \begin{array}{c}\dfrac{}{(A \supset B) \wedge (A \supset C)}\,x \\ \vdots \\ A \supset C\end{array}}{C}\supset\mathrm{E}}{B \wedge C}\wedge\mathrm{I}}{A \supset (B \wedge C)}\supset\mathrm{I}^{y}}{(A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)}\supset\mathrm{I}^{x}}{}
$$

Lausearvutus

Näide (2)

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{\dfrac{}{A}\,y \qquad \dfrac{\dfrac{}{(A \supset B) \wedge (A \supset C)}\,x}{A \supset B}\,\wedge \mathrm{E}_L}{B}\,\supset \mathrm{E}
\qquad
\dfrac{\dfrac{}{A}\,y \qquad \dfrac{\dfrac{}{(A \supset B) \wedge (A \supset C)}\,x}{A \supset C}\,\wedge \mathrm{E}_R}{C}\,\supset \mathrm{E}
}{B \wedge C}\,\wedge \mathrm{I}
}{A \supset (B \wedge C)}\,\supset \mathrm{I}^y
}{(A \supset B) \wedge (A \supset C) \supset A \supset (B \wedge C)}\,\supset \mathrm{I}^x
$$

Lausearvutus

Näide (3)

$$A \supset B \supset B$$

Lausearvutus

Näide (3)

$$\dfrac{B \supset B \qquad (B \supset B) \supset A \supset B \supset B}{A \supset B \supset B} \supset E$$

Lausearvutus

Näide (3)

$$\dfrac{\dfrac{\begin{array}{c}\dfrac{}{B}\,x\\ \vdots \\ B\end{array}}{B \supset B}\,{\supset}\mathrm{I}^{x} \qquad (B \supset B) \supset A \supset B \supset B}{A \supset B \supset B}\,{\supset}\mathrm{E}$$

Lausearvutus

Näide (3)

$$\dfrac{\dfrac{\dfrac{}{B}\,{}^{x}}{B \supset B}\,\supset\mathrm{I}^{x} \qquad (B \supset B) \supset A \supset B \supset B}{A \supset B \supset B}\,\supset\mathrm{E}$$

Lausearvutus

Näide (3)

$$\dfrac{\dfrac{\overline{B}^{\,x}}{B \supset B}\,{\supset}\mathrm{I}^{x} \qquad \dfrac{\begin{array}{c}\overline{B \supset B}^{\,y}\\ \vdots \\ A \supset B \supset B\end{array}}{(B \supset B) \supset A \supset B \supset B}\,{\supset}\mathrm{I}^{y}}{A \supset B \supset B}\,{\supset}\mathrm{E}$$

Lausearvutus

Näide (3)

$$\dfrac{\dfrac{\overline{B}^{\,x}}{B \supset B}\supset\mathrm{I}^{x} \qquad \dfrac{\dfrac{\begin{array}{c}\overline{B \supset B}^{\,y} \qquad \overline{A}^{\,z}\\ \vdots \\ B \supset B\end{array}}{A \supset B \supset B}\supset\mathrm{I}^{z}}{(B \supset B) \supset A \supset B \supset B}\supset\mathrm{I}^{y}}{A \supset B \supset B}\supset\mathrm{E}$$

Lausearvutus

Näide (3)

$$
\dfrac{
  \dfrac{\dfrac{}{B}\,x}{B \supset B}\,{\supset}\mathrm{I}^x
  \qquad
  \dfrac{\dfrac{\dfrac{}{B \supset B}\,y}{A \supset B \supset B}\,{\supset}\mathrm{I}^z}{(B \supset B) \supset A \supset B \supset B}\,{\supset}\mathrm{I}^y
}{A \supset B \supset B}\,{\supset}\mathrm{E}
$$

Lausearvutus

Näide (3) — alternatiivne tõestus

$$A \supset B \supset B$$

Lausearvutus

Näide (3) — alternatiivne tõestus

$$\dfrac{\begin{array}{c}\overline{A}^{\;x}\\ \vdots \\ B \supset B\end{array}}{A \supset B \supset B}\;\supset\mathrm{I}^{x}$$

Lausearvutus

Näide (3) — alternatiivne tõestus

$$\dfrac{\dfrac{\begin{array}{c}\overline{A}^{\,x} \qquad\qquad \overline{B}^{\,y} \\ \ddots \qquad \therefore \\ B\end{array}}{B \supset B}\,\supset\mathrm{I}^{y}}{A \supset B \supset B}\,\supset\mathrm{I}^{x}$$

Lausearvutus

Näide (3) — alternatiivne tõestus

$$\dfrac{\dfrac{\overline{\;B\;}^{\,y}}{B \supset B}\,{\supset}\mathrm{I}^{y}}{A \supset B \supset B}\,{\supset}\mathrm{I}^{x}$$

Tõestuste normaliseerimine

Teoreem:

Igal tõesel väitel on normaalkujuline tõestus.

Tõestuste normaliseerimine

Teoreem:

Igal tõesel väitel on normaalkujuline tõestus.

Normaliseerimisreeglid — implikatsioon:

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

Tõestuste normaliseerimine

Teoreem:

Igal tõesel väitel on normaalkujuline tõestus.

Normaliseerimisreeglid — konjunktsioon:

$$\dfrac{\dfrac{\begin{matrix}\vdots\,\Sigma \\ P_1\end{matrix} \qquad \begin{matrix}\vdots\,\Pi \\ P_2\end{matrix}}{P_1 \wedge P_2}}{P_1} \quad \to \quad \begin{matrix}\vdots\,\Sigma \\ P_1\end{matrix}$$

Tõestuste normaliseerimine

Teoreem:

Igal tõesel väitel on normaalkujuline tõestus.

Normaliseerimisreeglid — disjunktsioon:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\;\Theta\\ P_1\end{array}}{P_1 \vee P_2} \qquad \begin{array}{c}\overline{P_1}\\ \vdots\;\Sigma\\ S\end{array} \qquad \begin{array}{c}\overline{P_2}\\ \vdots\;\Pi\\ S\end{array}}{S} \qquad \to \qquad \begin{array}{c}\vdots\;\Theta\\ P_1\\ \vdots\;\Sigma\\ S\end{array}$$

Curry-Howard'i isomorfism

Teoreem:

(i) Kui $\Gamma \vdash M : \varphi$ in $\lambda(\to, \times, +)$, 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 $\lambda(\to, \times, +)$ leidub term M, selline et $\Delta \vdash M : \varphi$, kus $\Delta = \{x_\varphi : \varphi \mid \varphi \in \Gamma\}$.

Curry-Howard'i isomorfism

Teoreem:

(i) K… kus

|Γ…

(ii) K… term

M…

Curry-Howard'i vastavus

Proposition	Type
$\bot$	Void
$\top$	Unit
$A \supset B$	$A \to B$
$A \land B$	$A \times B$
$A \lor B$	$A + B$

Curry-Howard'i isomorfism

Teoreem:

(i) K ... s

$|\Gamma$

(ii) K ... term

M

Curry-Howard'i vastavus

Intuitionistic logic	Typed λ-calculus
Proposition	Type
Propositional variable	Type variable
Proof	Term
Hypothesis	Term variable
Logical connective	Type constructor
Provability	Type inhabitation
Proof normalization	Reduction