

Teoreemitõestuse keel Idris

- Curry-Howardi vastavus ütleb: saame teha tõestusi prog. keelega. Aluseks on funktsioonitüübile vastavad reeglid.

- Funktsiooni sissetoomise reegel:

$$\frac{\Gamma, x : a \vdash e : b[y \rightarrow x]}{\Gamma \vdash (\lambda x \Rightarrow e) : (y : a) \rightarrow b} I^{\rightarrow}$$

- Funktsiooni väljaviimise reegel:

$$\frac{\Gamma \vdash f : (x : a) \rightarrow b \quad \Gamma \vdash e : a}{\Gamma \vdash f e : b[x \rightarrow e]} E^{\rightarrow}$$

- Edasi läheb lihtsamaks. :)

Aga ülejäänud reeglid?

Loogikareegel:

$$\frac{A \quad B \quad C}{D} \text{ nimi}$$

Loogikareegel Idrises:

```
nimi : a → b → c
      -----
      →      c
```

- Sissetoomise reegel: konstruktor
- Väljaviimise reegel: mustrisobitus, abifunktsioonid
- Töötab, kuna Idrises on puhtad ja täielikud funktsioonid.
- Täielikuse jaoks võtmesõna **total** või kogu failile **%default total**

Näide: konjunktsioon

$$\frac{A \quad B}{A \wedge B} \text{conj}_i$$

Idrises:

```
infixl 10 /\
data (/\) : Type → Type → Type where
  ConI : a → b
          -----
          → a /\ b
```

$$\frac{A \wedge B}{A} \text{ conj}_{el}$$

$$\frac{A \wedge B}{B} \text{ conj}_{er}$$

Loogikareegel Idrises:

conEl : a ∧ b

→ a

conEl = ?conEl_v

conEr : a ∧ b

→ b

conEr = ?conEr_v

$$\frac{A \wedge B}{A} \text{ conj}_{el}$$

$$\frac{A \wedge B}{B} \text{ conj}_{er}$$

koos tõestustega:

conEl : a $\wedge$ b

→ a
 conEl (ConI x y) = x

conEr : a $\wedge$ b

→ b
 conEr (ConI x y) = y

Ülesanded

- $A \wedge B \supset B \wedge A$
- $A \supset B \supset B$
- $A \vee B \supset A \wedge B$
- $\perp \supset A$
- $(A \vee B) \wedge C \supset (A \wedge C) \vee (B \wedge C)$
- $(\forall A. \neg \neg A \supset A) \supset (\forall B. B \vee \neg B)$
- $(\forall B. B \vee \neg B) \supset (\forall A. \neg \neg A \supset A)$

Võrdused

```
-- defineeritud standardteegis
data (≡) : a → b → Type where
  Refl :
    -----
    a = a
```

- Miks on `Refl` piisav?
- Kas võrdus on transitiivne ja sümmeetriline?
- Kas kehib substituutsiooni omadus?
- Filosoofia (Leibniz): asjad on võrdsed, kui me *ei saa* neil vahet teha.

Ülesanded

- $0 + x = x$
- $x + 0 = x$
- $1 * x = x$
- $x * 1 = x$
- $x + y = y + x$

Kokkuvõtteks

- Tüübiteooria on hea alus tõestussüsteemile!
- Idris sobib õppimiseks kuid pole piisavalt küps suurte tõestuste jaoks.
- Soovitame kasutada muid vahendeid. Näiteks Agda, Lean4 või Rocq.